FIREWALL DIGITAL CONSCIENTE

EDICIÓN ACTUALIZADA · EDICIÓN ACTUALIZADA ·

GUÍA DE SEGURIDAD DE UN HACKER

Cómo proteger tus datos, tu familia y tu negocio de las amenazas digitales

CÉSAR CERRUDO

Guía de seguridad de un HACKER

Cómo proteger tus datos, tu familia
y tu negocio de las amenazas digitales

César Cerrudo

A mis padres, que me dieron la posibilidad de vivir y sus mejores esfuerzos

A mi esposa, que siempre me ha acompañado y dado dos hermosos hijos

A mis hijos, que espero puedan triunfar en todos los aspectos de la vida

Prólogo

Pon un hacker (o jáquer) en tu vida

Es cierto que el término «hacker» se toma por lo general con una connotación negativa, refiriéndose a alguien con capacidades avanzadas en tecnología que podría colarse en los sistemas informáticos de una empresa o en tus cuentas de redes sociales. Lo cierto es que los hackers, para nosotros, que nos dedicamos a la ciberseguridad, no son los malos. Son personas con capacidades especiales que llevan la tecnología más allá de los límites para los que esta se creó. Y sí, muchas veces son los especialistas en seguridad que demuestran que algo que se percibía como confiable no lo es.

Son esas personas con un punto de creatividad especial. Con una mirada distinta, capaz de ver la tecnología de forma íntegra; con lo bueno y con lo malo que esta tenga. Son investigadores, curiosos, retadores y brillantes. Personas con capacidades que van más allá de la media; que pueden trabajar y estudiar mucho para luego poder añadir una pizca de su conocimiento a una disciplina concreta. Son

los grandes hackers que tanto adoramos los que amamos el hacking.

Pero no son los malos. Son quienes aman el conocimiento, la innovación y la mejora constante de las cosas. Es cierto que los medios de comunicación, las películas de Hollywood y una confusión repetida a nivel de la sociedad en general llevó a pensar que alguien que utiliza una herramienta informática para hacer el mal a alguien es un hacker. Sí, entiendo que en los medios de comunicación han hecho que esto sea así para muchos, pero no es verdad. Los malos, los que hacen uso de las herramientas informáticas para hacer daño son los cibercriminales. Y créanme, la gran mayoría de quienes usan esas herramientas no serían capaces de crearlas y se basan en aprovecharse del trabajo de otros. Es comprensible que las personas asuman que un hacker es alguien con capacidad de hacer algún mal por medio de herramientas informáticas. Si bien no es lo que pensamos nosotros, lo entiendo.

De hecho, hace años yo comencé una campaña en pro de cambiar la definición de «hacker» en el Diccionario de la lengua española, para que no fuera negativa, sino positiva. Y aunque no lo conseguí, al final la Real Academia Española decidió añadir una segunda definición de «hacker»: persona con grandes conocimientos que ayuda a mejorar la tecnología.

---

jáquer

Del ingl. *hacker.*

1. *m. y f. Inform.* Pirata informático.

2. m. y f. Inform. Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.

Definición de «hacker» en la RAE (dle.rae.es/jaquer)

Y he de decir que me gusta mucho esa segunda acepción: «Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora». Y me gusta mucho porque eso es justo César Cerrudo para nosotros, uno de los grandes hackers de nuestra generación. No de los piratas informáticos, sino un hacker que ha ayudado a corregir fallos de seguridad en importantes empresas, en Microsoft, en Oracle, en grandes organizaciones.

César Cerrudo no tiene nada que ver con un cibercriminal o con un criminal que, sin saber nada de tecnología, hace un ataque burdo de robo de tarjetas de crédito, o mediante un spam hace una campaña de phishing para robar identidades de personas en la red. No, César Cerrudo ha puesto su nombre a técnicas de hacking que han avanzado en el conocimiento de la tecnología, de la seguridad informática y de la construcción de nuevos servicios digitales de forma más segura. Él es un hacker.

Así que, en este libro, está haciendo lo que nosotros entendemos por hacker, que es «avisar de los fallos y desarrollar técnicas de mejora». Esto es este libro, para ti y para la mayoría de la gente que quiere defenderse de los «hackers»: una guía escrita por un hacker para que aprendas de verdad a estar más seguro en tu vida.

No sé si conseguiré con este pequeño prólogo convencerte de que no utilices el término «hacker» de forma negativa, porque un tipo que no es capaz de llevar la tecnología un poco más allá de los límites para los que se creó para nosotros no es un hacker. No sé si conseguiré que entiendas la grandeza de lo que es para nosotros un hacker como César Cerrudo, pero si este libro consigue ayudarte a que estés un poco más protegido contra los malos, entonces habrá sido un éxito.

Así que tómate en serio las enseñanzas y recomendaciones de este libro y pon un hacker, como César Cerrudo, en tu vida.

Chema Alonso[1]

---

1 José María Alonso Cebrián, más conocido como Chema Alonso (Madrid,17 de junio de 1975), es un hacker español, exmiembro del Comité Ejecutivo de Telefónica, Vice President, Head of International Development en Cloudflare y experto en ciberseguridad.

Capítulo 1

Ciberseguridad en la vida actual

Al escuchar el término «ciberseguridad» (o seguridad informática) muchas personas no entienden exactamente de qué se trata, a menos que, de alguna manera, estén vinculadas a la profesión o lo tecnológico. Si bien esta expresión puede ser desconocida por la mayoría de la gente, cada vez se hace más necesario entender por qué es tan importante y tiene tanta influencia en diferentes aspectos de nuestra vida cotidiana.

Nuestra relación con la tecnología

Cuando nos referimos a la tecnología, usualmente hacemos referencia a modernos dispositivos con pantallas táctiles que procesan información, pero lo cierto es que el concepto de tecnología es mucho más amplio.

Por su definición, «tecnología» implica conocimientos técnicos científicamente ordenados que permiten diseñar y crear bienes y servicios que faciliten la adaptación al ambiente, debiendo satisfacer, además, necesidades esenciales y deseos de las personas.

Se considera que la primera tecnología del ser humano fue el fuego, cuyo dominio alcanzó el *Homo erectus* hace más de 300.000 años. Luego aparecieron elementos para cazar y cocinar que evolucionaron en los primeros dispositivos mecánicos, en máquinas electromecánicas y en equipos electrónicos hasta llegar a la actualidad, cuando prácticamente todo nuestro entorno está signado por la tecnología moderna, las computadoras y la obsolescencia programada.

Hace solo treinta años, aproximadamente, los dispositivos hogareños más modernos eran los televisores a color y, aunque poca gente entendía cómo funcionaban, posiblemente era más de la que hoy sabe cómo funciona un moderno televisor led.

Nuestra dependencia de los dispositivos alcanzó niveles incalculables y hoy sería imposible pensar la vida cotidiana sin heladera, computadora, teléfono celular, microondas, iluminación, autos y muchas cosas más. Asimismo, estos contienen cada vez más tecnología incorporada y elementos electrónicos como los microcontroladores (que funcionan como pequeñas computadoras). A su vez, se van integrando más componentes en espacios físicos

reducidos, por lo que la miniaturización es una constante en progreso, siendo los dispositivos cada vez más pequeños y potentes.

Los teléfonos móviles que hoy utilizamos y que caben en nuestros bolsillos tienen más poder y son mucho más pequeños que las computadoras de hace unos años. Pero, quizás, lo más interesante de la tecnología moderna es que se basa en un elemento clave: la información que los dispositivos electrónicos necesitan.

No es casualidad que se haya nombrado «sociedad de la información» al grupo humano que conformamos y en el que un conjunto de tecnologías facilita la creación, la modificación y la distribución de la información de manera tal que esta pasa a cumplir un rol fundamental en la sociedad.

Posteriormente apareció el concepto de «sociedad del conocimiento» como evolución de la anterior a partir de la masificación de las tecnologías de la información y la comunicación (TIC) y su uso como parte de las relaciones humanas cotidianas. Esta sociedad va más lejos que la anterior; apunta a transformaciones radicales, al desarrollo sustentable y está sostenida en la libertad de expresión y el acceso a la información.

Pero ¿qué tiene que ver todo lo anterior con la seguridad informática? Tiene mucho que ver. En sociedades en las que la información es un bien tan preciado y donde se busca conocimiento –que también marca la diferencia en el progreso de los países– es necesario que esté resguardada, protegida y asegurada en todo nivel.

Como nuestra información se transmite principalmente desde y hacia dispositivos electrónicos, es fundamental aprender a ser buenos usuarios de esa tecnología y hacer un manejo prudente de los datos que estos aparatos procesan para, de esta manera,

protegernos de posibles amenazas como programas dañinos o hackers maliciosos.

Hace unos años, en cada hogar había una sola computadora de escritorio, que habitualmente llamamos PC, que compartía toda la familia, y el acceso a internet se realizaba a través de una conexión muy lenta. Por esos tiempos, tanto las computadoras como la conexión a internet no eran económicas ni accesibles para todos. En cambio, en una vivienda actual es muy común encontrar varios equipos electrónicos que procesan datos, que guardan nuestra información y que se conectan a internet a altas velocidades: computadoras de escritorio, notebooks, tablets, teléfonos inteligentes (smartphones), televisores inteligentes (smart TV), consolas de juegos (PlayStation, Xbox, etc.), por mencionar los principales.

Cada vez poseemos más dispositivos que manejan nuestra información y que se conectan a internet. Los utilizamos constantemente para distintas actividades y nuestra dependencia es cada vez mayor, ya que se convierten en un aspecto esencial de nuestra vida cotidiana. ¿Qué ocurre, por ejemplo, si se rompe nuestra PC, la notebook o el teléfono inteligente? Además de las consecuencias económicas, sufrimos una pérdida de información que puede provocarnos diferentes problemas de no haber tomado el recaudo de respaldarla, por ejemplo, la desaparición de fotos, videos o documentos de trabajo o de estudio. Un pequeño incidente en alguno de los dispositivos que usamos regularmente podría tener un impacto más que significativo en nuestras vidas y hasta causarnos graves complicaciones si perdemos información de relevancia.

Todo indica que seguiremos incorporando nueva tecnología a nuestras vidas y que la dependencia seguirá creciendo, así como los posibles problemas, ya sean fortuitos o causados por ataques de

programas dañinos, hackers maliciosos o robos, entre otras razones posibles.

Es muy común que amigos, familiares y conocidos me llamen, generalmente muy preocupados, porque no pueden acceder a algún servicio como el correo electrónico o redes sociales, porque perdieron información debido a la rotura de un dispositivo o a causa de programas dañinos (comúnmente denominado malware), o porque hackearon su cuenta y necesitan ayuda para recuperar el acceso al servicio y, por lo tanto, a su información. Por lo general, esto les sucede a muchas personas que no han sabido tomar precauciones para prevenir problemas como estos.

Recuerdo un día en que un amigo me llamó; enseguida noté que estaba muy alterado y pensé que algo grave le había ocurrido. Rápidamente me explicó que el disco rígido o disco duro (dispositivo donde se guardan los datos) de su computadora había dejado de funcionar, se había roto y ahí tenía la tesis final de su carrera universitaria, en la que había estado trabajando por seis meses y que debía presentar en un par de semanas. Era entendible su preocupación, el fruto de un largo esfuerzo con el que finalizaría su carrera había desaparecido al romperse el dispositivo. Le hice una pregunta obvia: si tenía copia de respaldo (o backup), y me dijo que no, que no se había dado cuenta de hacerlo, nunca pensó que algo así podría pasarle y siempre le había funcionado todo bien. Lo tranquilicé un poco diciéndole que tal vez era posible recuperar todo o parte de lo que había perdido, pero que iba a llevar tiempo y le iba a costar seguramente bastante dinero, ya que es un servicio especializado que no es fácil de conseguir. Un poco aliviado me dijo que no importaba, que haría lo que fuese necesario con tal de recuperarlo. Finalmente, pudo rescatar gran parte de la información y con gran esfuerzo completar la tesis, tras largas noches sin dormir, para poder presentarla a tiempo.

Historias como estas son muy habituales y no tienen finales felices. Pero tales problemas pueden evitarse si se conoce la importancia de proteger de manera apropiada la información almacenada en dispositivos electrónicos para que, cuando la necesitemos, siempre esté disponible. De cada uno de nosotros

depende tomar las medidas y precauciones para no sufrir este tipo de situaciones indeseadas.

En definitiva, cada vez somos más dependientes de tecnologías cuyo funcionamiento interno desconocemos, y a medida que vayamos incorporando más dispositivos a nuestras rutinas –ya sea en el trabajo o en el hogar– y aumenten los inconvenientes que estos puedan tener en materia de seguridad informática, mayor será el impacto en nuestras vidas y la sociedad en general.

Por lo mencionado anteriormente, lo mejor es prepararnos para evitar los posibles perjuicios que la tecnología nos pueda causar. Es por ello que este libro ofrece al lector una serie de sugerencias sobre cómo manejarse y protegerse de los nuevos riesgos y peligros derivados del uso y la dependencia de la tecnología.

¿Hackers malos o buenos?

En el mundo de la seguridad informática, la palabra «hacker» se utiliza con mucho cuidado. Quizás por simplificar o llamar la atención, entiendo que hay una tendencia en los medios de comunicación a utilizar el término sin un criterio claro.

En el ámbito tecnológico, se considera hacker a aquella persona que hace uso de sus conocimientos de forma ingeniosa y creativa, que intenta llevar la tecnología más allá de los límites conocidos; alguien a quien le gustan los desafíos y la búsqueda de problemas de seguridad en la tecnología, independientemente de querer utilizarlos con un buen fin o no.

Hay quienes podrían ser considerados hackers que han hecho importantes contribuciones a la tecnología que utilizamos en la actualidad. Tales son los casos de Tim Berners Lee (creador de la World Wide Web), Vinton Cerf (creador del protocolo TCP/IP), Dennis Ritchie (cocreador del lenguaje C y el sistema operativo Unix), Linus Torvalds (creador del kernel del sistema Linux), Bill Gates (creador de Microsoft) y otros tantos que –mediante sus aportes– contribuyeron al avance tecnológico en varios aspectos.

En nuestros tiempos, comúnmente se denomina hacker a quien se dedica a algunos aspectos de la seguridad informática, fundamentalmente a la parte ofensiva que consiste en «romper» tecnologías sobrepasando protecciones, buscando problemas de seguridad y aprovechándolos para realizar distintas acciones que puedan estar restringidas. Cuando esto se lleva a cabo con buena intención, colabora a hacer tecnologías más seguras, ya que los problemas de seguridad encontrados por estos hackers pueden luego solucionarse.

Por eso, la labor de un hacker profesional es constructiva y muy importante en la sociedad actual, ya que ayuda a eliminar los problemas de seguridad en la tecnología y, por lo tanto, a hacer que nuestra vida cotidiana no se vea afectada en este aspecto.

¿Por qué entonces los ciudadanos y los medios masivos de comunicación asocian la palabra «hacker» con los delincuentes informáticos? No hay una sola respuesta para eso, pero es posible que ciertas figuras públicas que fueron reconocidas como especialistas en seguridad hayan sido vinculadas a casos de delincuencia y esa sea la razón por la que comenzó a asociarse al hacker con el perfil criminal.

Por su parte, desde el año 2014 la Real Academia Española (RAE) define «hacker» como «pirata informático», lo que ha sido desde entonces una mala reputación para los profesionales de la seguridad.

Esto nos lleva a plantear una especie de clasificación aceptada en el ámbito de la seguridad informática, que divide a los hackers en función de sus intenciones y de qué lado de la ley estén. Así aparecen, por un lado, los *white hat hackers* –«hackers de sombrero blanco»–, que son aquellos que utilizan sus habilidades para mejorar la seguridad de los sistemas, y, por el otro, los *black hat hackers* –«hackers de sombrero negro»–, que son los que utilizan su conocimiento para cometer delitos y realizar actividades ilegales.

En esta categorización existe, además, una categoría intermedia: los *gray hat hackers* –«hackers de sombrero gris»–, cuya línea puede variar hacia uno u otro lado según el momento o la conveniencia. En esta zona gris también se encuentran los hacktivistas, que son una combinación de hackers y activistas, en tanto realizan acciones de protesta por causas sociales e ideológicas, aunque muchas veces esas actividades se consideran ilegales.

Los *white hat hackers* –también llamados *ethical hackers*, hackers profesionales o hackers éticos– trabajan para proteger los sistemas de las empresas y organizaciones, además de abordar las distintas tecnologías que utilizamos frecuentemente, haciéndolas más seguras mediante la corrección de los problemas de seguridad que encuentran en ellas. Para esto, pueden utilizar técnicas especializadas, como la simulación de ciberataques, que permite ver cómo la organización y sus sistemas responden a ellos. Esta actividad se convirtió en una profesión muy especializada que requiere altos conocimientos en materia de seguridad y tecnología, entre otras habilidades.

En cuanto a los hacktivistas, muchas veces aparecen noticias en los medios de comunicación dando a conocer que se atacó un sitio web o servicio de internet; a veces es un cambio en su página de inicio (este ataque es llamado *defacement*), o hacen saturar el servicio para que nadie pueda utilizarlo («denegación de servicio»; *denial of service*, DoS).

Este tipo de ataques que describimos responden, frecuentemente, a cuestiones ideológicas, filosóficas o motivos religiosos o políticos, y, por lo tanto, mucha gente suele estar de acuerdo con ellos. Vale aclarar que el hecho de avalar la motivación de una acción ilegal no la convierte en legal ni en inocente a su autor.

Los *black hat hackers* –o hackers «malos»– se encuentran vinculados, ya sea directa o indirectamente, a actividades cibercriminales y están en pleno conocimiento de ello. Las motivaciones son, por lo general, fines económicos, ya que los negocios ilegales suelen pagar muy bien a quienes colaboran con delincuentes, lo que lo hace tentador para algunas personas.

Aunque en muchos casos las fuerzas de seguridad y la ley persiguen a estos hackers-delincuentes, ellos saben esconderse

muy bien, incluso sus identidades suelen desconocerse abiertamente.

Vale aclarar que quien escribe estas líneas es un hacker profesional que utiliza sus conocimientos para el bien, buscando mejorar la seguridad en las tecnologías que utilizamos comúnmente.

Privacidad y confidencialidad

Uno de los temas más discutidos en los últimos años ha sido la privacidad, que, en el ámbito de la seguridad de la información, se relaciona con la confidencialidad. Para quienes no estén familiarizados con este último concepto, podemos definirlo de forma simple como aquella característica de la información que permite que sea conocida solamente por quienes están autorizados a acceder a ella. Es decir, que algo solo pueda ser conocido por quien nosotros queramos y nadie más. La definición que tomamos refiere al manejo de la información en todo ámbito, ya que estamos habituados a escuchar que algo es confidencial en referencia a cosas que no pueden saberse fuera del contexto en el que se tratan. El concepto de confidencialidad es sumamente importante en ciberseguridad y es uno de sus tres pilares fundamentales, junto con la integridad y la disponibilidad.

La confidencialidad refiere a lo que en lo cotidiano llamamos privacidad, todo lo vinculado al terreno personal, ámbito en el que manejamos información que no es –o no pretendemos que sea– pública. Por ejemplo, hay ciertas fotos que nos tomamos que son privadas y otras que compartimos en redes sociales y por eso son públicas (o semipúblicas); algunas son de acceso para cualquier persona y otras solo para algunas, según la configuración que hayamos programado en la red social utilizada.

En las últimas dos décadas, la privacidad tuvo una enorme transformación que fue corriendo la línea de lo que consideramos privado y lo que no. Hasta fines de los años 90, dar una opinión en público o mostrar fotografías y videos personales a otros (sean conocidos o no) era algo bastante poco común; en parte porque la tecnología no facilitaba que fuera de otra manera. Para mostrar un

álbum de fotos de nuestras vacaciones, debíamos juntarnos en casas de amigos o familiares, mientras que hoy lo hacemos a través de las redes sociales por medio de álbumes compartidos con nuestros contactos. Es mucho más fácil y más rápido también.

Esta transformación de la privacidad se debe a dos factores fundamentales: por un lado, la tecnología, que permitió digitalizar la información, y, por otro, la aceptación social, que nos fue llevando a que hoy no esté mal visto hacer ciertas cosas que antes hubieran sido inaceptables socialmente o consideradas fuera de lo común. Claro que esto no sucedió de un día para el otro, sino que fue cambiando gradualmente en la medida en que más personas han ido haciendo uso de las nuevas tecnologías y cambiando sus comportamientos.

Es habitual escuchar en charlas sobre ciberseguridad que uno «paga» con su privacidad muchos servicios «gratuitos» de internet, debido a que proveemos una gran cantidad de datos personales y de terceros al hacer uso del servicio. Facebook, por ejemplo, es un servicio gratuito, pero al usarlo volcamos en él mucha información personal valiosa que luego esta red social utiliza con distintos fines de lucro como publicidad, ventas, etcétera.

Otro aspecto importante, aunque menos conocido que la privacidad, está relacionado con el espionaje –tanto local como internacional– llevado a cabo por gobiernos o empresas.

Posiblemente, al hablar por teléfono nos habremos preguntado si la llamada podría estar siendo escuchada por alguien más. Los más paranoicos quizás se lo cuestionan en reiteradas ocasiones; otros, jamás. Lo cierto es que, en la práctica, una empresa, gobierno u organización que disponga de suficientes recursos técnicos podría interceptar y escuchar una conversación. Algunas, de hecho, podrían hacerlo muy fácilmente si quisieran, como las empresas de telefonía o los proveedores de servicios de internet (ISP). Esto no

significa que todos los que pueden escucharnos lo harán, pero tampoco podemos ser demasiado inocentes en este sentido.

En definitiva, tanto en el aspecto de la aceptación social como por el hecho de que existe la posibilidad técnica de que ciertas organizaciones irrumpan en nuestras comunicaciones o que accedan a nuestra información, podemos decir que la privacidad es un terreno que poco a poco estamos perdiendo y que probablemente sea muy difícil de recuperar sin una concientización y educación continuas para lograrlo.

En estas páginas se brindarán también varios recursos para incrementar la privacidad, protegiendo nuestros datos de la mejor manera para que solo puedan acceder a ellos quienes nosotros dispongamos.

Importante recordar

- Como nuestra información está cada vez más relacionada con la tecnología, debemos tratar de conocerla lo mejor posible para saber cómo protegerla adecuadamente.
- En la actualidad, es muy difícil no depender de la tecnología; esto será cada vez mayor, por lo que debemos tomar medidas para saber cómo actuar y estar prevenidos en caso de que la tecnología falle o perdamos acceso por algún motivo.
- La confidencialidad de la información implica que algunas personas tienen acceso a ella y otras no, lo que suele estar definido por los dueños o responsables de ella. Por ejemplo, cuando subimos una foto a una red social elegimos quién puede verla y quién no; de esta forma limitamos el acceso.
- La privacidad es un terreno que se está perdiendo poco a poco, por lo que debemos considerar cómo vamos a manejarnos en el mundo virtual respecto a ella.
- Los hackers pueden ser buenos o malos, su nivel de conocimiento puede ser el mismo, pero hay quienes trabajan para mejorar la seguridad y quienes lo hacen para cometer delitos.
- Cuando se habla de hackers, se suele hacer un uso inadecuado del concepto, pues se da por sentado que se trata de delincuentes, y no siempre es así.

Capítulo 2

Convivir con hackers malos y peligros en internet

Diariamente estamos expuestos a entornos que pueden ser peligrosos si no tomamos medidas de precaución. Al usar internet y cada vez más tecnología, los distintos riesgos a los que nos exponemos aumentan diariamente, por esto es imprescindible conocer y entender cuáles son los peligros actuales y saber qué podemos hacer para evitarlos.

Peligros en internet

Internet, como cualquier ámbito público, puede ser peligroso en tanto no tengamos conciencia de los riesgos que corremos y tomemos recaudos. Una buena forma de interpretarlo es imaginarlo como si fuera un espacio físico. En un ámbito real desarrollamos actividades, como relacionarnos con otras personas, ir de un lugar a otro, tomarnos fotos, grabarnos, escribir, dar opiniones, cuidarnos de posibles robos y muchas cosas más.

Si asumimos internet como una analogía del mundo físico, la comprensión se simplifica, ya que también en el mundo online hablamos, vamos a lugares (virtuales), compartimos fotos, nos protegemos, etcétera. En este sentido, una medida de cuidado general podría ser comportarnos en internet con la misma prudencia con que lo hacemos fuera de ella.

Como vemos, el hecho de estar expuestos a determinado entorno hace que tengamos que comprenderlo. Cuando somos niños, nuestros padres nos explican cómo hay que comportarse fuera de casa, cruzar una calle, manejarnos con personas desconocidas, tomar un medio de transporte público y otras cosas que son fundamentales para que aprendamos a interactuar en ese ámbito de manera segura. Si bien internet es una parte importante del contexto en que nos desenvolvemos, se trata de un entorno virtual donde nuestra información está representada en formato digital, con sus ventajas y desventajas. Un espacio en el que, como ocurre cuando somos niños, debemos aprender a manejarnos para evitar los problemas típicos del ámbito y no ser víctimas de las amenazas que están presentes en internet.

Los peligros son muchos y variados, y conocerlos para poder prevenir es algo cada vez más importante en nuestras vidas debido

a que –como mencionamos anteriormente– dependemos cada vez más de la tecnología y del uso de la red.

La identidad virtual

En el contexto de internet se habla de la existencia de una identidad virtual distinta de la física (o real). Esta nueva faceta de la identidad fue muy bien aceptada por personas que se llevaban bien con la tecnología y sentían comodidad detrás de las pantallas, aunque muchos siguen considerándola una parte ajena a sí mismos. Lo cierto es que cuanto más conectados estamos, más nos adentramos en el mundo digital y el uso de la tecnología, por lo que más importancia toma nuestra identidad virtual.

Podemos decir que nuestra identidad virtual está conformada por todos los servicios que utilizamos en internet y en las aplicaciones de nuestros dispositivos móviles. Así, tanto los perfiles de redes sociales como nuestro e-mail, cuenta de Facebook, Instagram, WhatsApp y otros, constituyen una parte de nuestra vida que no pasa por lo físico, sino que se desarrolla en el mundo digital. De hecho, aunque creyéramos que podemos evitar nuestra identidad virtual prescindiendo de perfiles online, alguien lograría –si quisiera– crear perfiles nuestros falsos; o bien podría existir en internet información sobre nosotros sin que lo sepamos, sea esta verdadera o no.

Puede existir, entonces, información personal en internet sin que lo hayamos autorizado, lo que podría darse por diversas razones, como aparecer en bases de datos ilegales, o padrones consultables en sitios web, o porque alguien escribe o comparte datos nuestros sin autorización. Por todo esto, y especialmente cuando encontramos en internet información personal que atenta contra nuestra privacidad, es importante saber «qué es lo que internet sabe». Al respecto, puede verificarse de forma muy simple si buscamos nuestro nombre y apellido en un motor de búsqueda

(como Google o Bing). Esto arrojará resultados según lo que exista en internet sobre nosotros, por lo que esta sencilla práctica puede darnos un punto de partida en la averiguación de nuestros propios antecedentes digitales.

Si nos encontramos en los resultados de los buscadores, debemos averiguar si se trata de referencias a nuestra persona, o alguien que se llame de la misma manera, y en qué condiciones es que aparecemos.

Google facilita –y sugiere– esta práctica de «googlearnos a nosotros mismos» mediante el uso de una función llamada Google Alertas, que puede configurarse para recibir un aviso por correo electrónico cada vez que aparece en internet un nuevo contenido en donde se menciona nuestro nombre y apellido.

Google Alertas también puede utilizarse para cualquier otra palabra que refleje nuestros intereses, gustos o preferencias. Esto es importante dado que, hoy en día, buena parte de las decisiones sobre las personas (especialmente las laborales) se toman basadas en su identidad virtual y en sus perfiles en redes sociales.

Es posible afirmar que estar en internet y tener identidad virtual es equivalente a pertenecer al mundo moderno, pero debemos balancear la necesidad de estar online y usar los distintos servicios de internet con el cuidado de la privacidad y la seguridad.

Para quienes aún estén en duda sobre la conveniencia de crear o no un perfil virtual, entendemos que suele ser mejor tener perfiles registrados, aunque sea para reservar nuestro nombre o usuario, y así evitar el robo de identidad, una práctica que desarrollaremos más adelante.

Nuestra información en internet

Aunque pueda sorprendernos, no importa si usamos o no internet, siempre hay información nuestra disponible en la red. Por ejemplo, es posible encontrar información impositiva y financiera que proveen organismos del gobierno, información relacionada con los servicios que suministran empresas que comúnmente contratamos y utilizamos, como las compañías de electricidad, telefonía fija y celular, medicina prepaga, seguros de vida y automotor, televisión por cable, internet, bancos, etcétera. Además, existe información nuestra que provee gente que nos conoce, como sucede cuando alguien pone en Facebook una foto con nuestro nombre completo más algún otro dato.

Debido a la digitalización de la información, el incremento en el uso y la dependencia tecnológica, hay demasiada información nuestra en diferentes sistemas, ya sean del gobierno o de empresas, y gran parte de ella está accesible desde internet de manera directa o indirecta. Con solo conocer el número de documento de identidad de alguien, es posible obtener información en internet, por ejemplo, buscando tales números de identificación de la persona y ver todo lo que aparece. Por más que esto pueda ser útil en determinados aspectos, igualmente crea riesgos, ya que esa información también puede ser utilizada por hackers o personas maliciosas con motivos dañinos.

Lamentablemente, no hay mucho que podamos hacer para limitar la divulgación de este tipo de datos personales disponibles en la red. Lo que sí podemos hacer es ser conscientes de esto y prevenir problemas si estamos atentos a las distintas amenazas.

Anonimato y privacidad

Como ya analizamos, la privacidad se refiere a la esfera en la que manejamos nuestra propia información personal. En ecosistemas como internet esto es algo muy difícil de mantener.

En esta línea de pensamiento, uno de los aspectos más valorados en la seguridad es el anonimato, que implica no poder ser reconocidos individualmente como una persona determinada al realizar cualquier acción. Es decir, que todo registro que se genere sobre nuestros comportamientos sea solo para fines estadísticos y no de espionaje o análisis específico de lo que cada usuario hace.

Pero podemos llevar el tema más allá si pensamos, por ejemplo, un caso en el que una empresa obtenga datos sobre nuestro comportamiento como consumidores para ofrecernos mejores productos y servicios orientados especialmente, situación que no tendría por qué ser considerada como algo negativo en sí misma. Este concepto, llamado comúnmente perfilación (*profiling*) –porque busca crear perfiles de consumo o comportamiento–, es un territorio muy estudiado en el ámbito de los negocios, el marketing y la publicidad. De hecho, muchos de los servicios de internet gratuitos que empleamos utilizan nuestros datos para tales motivos.

Cuando nos conectamos a internet, el proveedor de acceso nos asigna una dirección de internet, llamada dirección IP (Internet Protocol Address). Se compone de cuatro números decimales separados por puntos, en su versión más antigua, o de ocho números hexadecimales separados por dos puntos, en su versión más nueva, y es usada por el funcionamiento más básico de internet, quedando registrada en todos los lugares que visitamos. Por lo tanto, puede ser aprovechada para monitorearnos, seguirnos y conocer nuestra actividad en internet.

Todos los movimientos que desplegamos en internet quedan registrados, ya sea en nuestro proveedor de acceso a internet –que nos brinda el servicio de conexión– como en los sitios que visitamos.

La mayoría de los sitios de internet usa sistemas de estadísticas, seguimiento y de publicidad que ponen marcas –llamadas cookies– en nuestro navegador y a partir de las cuales pueden saber qué tipo de sitio visitamos y en qué momento lo hicimos.

Seguramente nos ha sucedido alguna vez que, habiendo visto un electrodoméstico en una página de comercio electrónico –por ejemplo, un televisor–, luego, al usar Instagram, vemos que coincidentemente se nos presentan publicidades de televisores. Esto se debe a que el sitio de comercio electrónico que visitamos, utilizando sistemas de seguimiento y publicidad, puso marcas (cookies) en nuestro navegador y guardó tanto la información sobre qué cosas estuvimos viendo en el sitio como nuestra dirección de IP. Luego Instagram, utilizando los mismos sistemas, obtiene de nuestro navegador aquellas marcas y la información de qué estuvimos mirando, y es por eso que nos muestra publicidad de televisores.

En situaciones como la descrita, la información es recolectada para exponernos ofertas de productos específicos sobre los que demostramos cierto interés; pero esto no necesariamente es algo malo si consideramos que ello nos ayuda a comprar un producto que buscábamos. Por otro lado, esto mismo puede ser considerado como una invasión de la privacidad, ya que «alguien» sabe qué sitios visitamos y qué cosas vemos. De modo que todo lo que hagamos en internet quedará registrado en algún lugar y eso puede ser usado a favor o en contra nuestro.

¿Hasta qué punto podemos, entonces, mantener cierto anonimato en internet? La respuesta no es simple, pero es claro que cuantos más conocimientos tengamos, más medidas de protección

y anonimato podremos tomar para permanecer lo más ocultos posible de aquellas organizaciones y sistemas que se dedican a recopilar datos.

Para aquellos que son usuarios sin muchos conocimientos, es bueno tener en cuenta las características de privacidad de los propios navegadores, que pueden impedir –ante ciertos escenarios– que nuestra información sea recolectada y reducir así el seguimiento de aquellas actividades que desarrollamos. También hay bloqueadores de publicidad y de seguimiento (tracking) que anulan estos sistemas, brindándonos mayor privacidad y, a su vez, mayor velocidad de navegación, ya que la carga de publicidades hace que generalmente se navegue más lento.

Un bloqueador bueno y conocido es Ghostery, es gratuito y cualquiera lo puede instalar en su navegador de internet. Utilizando bloqueadores de este tipo evitamos, en gran medida, el seguimiento y que nuestra información de navegación sea recolectada por los sitios que visitamos.

Para evitar que nuestro proveedor de acceso a internet sepa sobre nuestra actividad tenemos que tomar medidas diferentes a las ya mencionadas. Esto requiere un poco más de conocimiento, pero es bueno mencionarlo para aquellos usuarios que quieran tener más privacidad. En este caso, se necesita utilizar una red privada virtual (Virtual Private Network, VPN) que protegerá nuestra conexión; por lo tanto, el servicio que nos provee internet no podrá ver la actividad que realizamos, detectando solamente nuestra conexión a dicha red.

Hay distintos softwares gratuitos y pagos para utilizar una red privada virtual; uno es SurfEasy VPN, que ofrece un servicio gratuito hasta determinada cantidad de datos por mes y luego pasa a ser pago en caso de que necesitemos mayor capacidad de datos. Pero es importante tener en cuenta que esto no nos protegerá de los

sistemas de seguimiento y publicidad mencionados anteriormente, por lo que ambas protecciones –bloqueador de publicidad y seguimiento y la VPN– deberían ser usadas para mayor privacidad.

Si bien una VPN nos protege de que nuestro proveedor de acceso a internet sepa qué actividades realizamos en este espacio, el sistema de red privada virtual conocerá nuestras actividades, pero la mayoría de estos sistemas garantizan que no guardan los datos, en tanto buscan proveer un servicio de privacidad confiable.

Si se desea que una actividad de navegación no sea guardada en el dispositivo que se está utilizando, debe activarse la navegación en modo privado o incógnito; de esta manera no se guarda localmente información de los sitios visitados. Esto es útil cuando se comparte el uso del dispositivo con alguien más y no queremos que sepa qué estuvimos viendo en internet. Vale aclarar que la configuración en modo privado o incógnito solo evita el guardado en forma local de la información de los lugares por los que se navegó, pero no impide que los sitios visitados registren la actividad realizada, así como tampoco que el proveedor de internet sepa qué hacemos.

Finalmente, en caso de querer tener una privacidad absoluta, existe la red Tor, que puede ser utilizada instalando el software disponible en www.torproject.org, el cual también trae un navegador especial llamado Tor Browser, que utiliza la red Tor para brindarnos una navegación anónima.

La red Tor encripta todas las comunicaciones y esconde la dirección IP; de esta forma, nadie puede saber qué hacemos en internet. Debido a la tecnología que utiliza este sistema, nos brinda el mayor anonimato en el uso de internet al impedir que nuestra actividad sea monitoreada. Hay que tener cuidado con realizar otras acciones en internet que no sean a través de Tor Browser y la red Tor, porque estas sí podrán ser vistas por terceros. Por lo tanto, se

debe tener bien configuradas todas las aplicaciones que acceden a internet para que lo hagan siempre a través de la red Tor. Para acceder a internet y navegar de forma anónima, lo mejor es limitarse a utilizar solamente Tor Browser, o bien recurrir a la VPN con aquellas aplicaciones que no sean para navegar.

Almacenamiento en la nube

Actualmente hablamos de «la nube», una idea fácil de entender si consideramos que se refiere, de forma sencilla, a todo lo que está fuera del dispositivo que utilizamos (computadora, teléfono, tablet, etcétera). Es decir, aquello que está en internet –o sea, online– en forma de distintos servicios. Así aparecen las ideas de computación en la nube (*cloud computing*) como paradigma en el que la información es procesada y almacenada online en internet, mientras que la recibimos a través de nuestros dispositivos desde cualquier parte del mundo en que nos encontremos ubicados. La idea se aplica desde hace muchos años, pero el término se popularizó cuando empresas como Google, Amazon o Microsoft comenzaron a vender servicios desde su propia infraestructura en internet, a gran escala.

La nube da a los usuarios la ventaja de no necesitar capacidades locales de almacenamiento y procesamiento más allá del dispositivo desde el cual se conectan, pero tiene la desventaja de que los vuelve totalmente dependientes de la conexión a internet y de que los recursos e infraestructura son propiedad de la empresa que presta los servicios (sean gratuitos o pagos), por lo tanto, están fuera de nuestro control.

Uno de los usos más aprovechados de la nube son sus servicios de almacenamiento de archivos en línea (*cloud storage*), que permiten tener nuestros datos siempre disponibles desde cualquier ubicación geográfica y dispositivo. Algunos de los más conocidos son Dropbox, Google Drive, iCloud de Apple y OneDrive de Microsoft, todos con sus versiones gratuitas y pagas. En general, se integran con herramientas de ofimática (Microsoft Office,

OpenOffice, Google Apps, etcétera) para visualización y edición de documentos.

Con respecto a la funcionalidad y la disponibilidad (aspecto esencial de la seguridad), los servicios de almacenamiento en la nube son ideales para tener sincronizados nuestros archivos, de modo que podamos acceder a la versión más reciente desde cualquier dispositivo; además, funciona como si en cada ubicación sincronizada existiera una copia de respaldo (*backup*), de modo que podamos acceder a la información por varias vías, aun habiéndose extraviado o roto alguno de nuestros dispositivos.

Otra ventaja importante es que la nube permite a varias personas editar un mismo documento en forma sincronizada, lo que facilita el trabajo en equipo.

Más allá de las grandes ventajas mencionadas, una consideración elemental a tener en cuenta desde el punto de vista del riesgo es que, al utilizar servicios en la nube, estamos dejando toda nuestra información en manos de un tercero. En sí mismo esto no es algo malo, pero se debe tener en cuenta si lo almacenado es contenido confidencial o íntimo. Por lo tanto, no se recomienda el almacenamiento de información sensible en la nube, excepto que esta tenga aplicadas otras medidas de seguridad como el cifrado, o sea que la información esté encriptada.[2]

Una de las mayores ventajas de la nube –tener todo disponible y fácilmente accesible en un solo lugar– puede ser, a su vez, un factor de riesgo; en tanto, si un hacker malicioso logra acceder a nuestra cuenta en la nube tendrá paso también a toda nuestra información, la cual podría ser robada y/o borrada definitivamente si este así lo quisiera. Además, debemos recordar que, si tenemos en la nube información personal que apreciamos mucho, como fotos o videos, no deberíamos utilizar la plataforma en cuestión como único medio de almacenamiento, sino que esta actúe como copia de seguridad.

Tales contenidos tendrían que estar siempre sincronizados con otro dispositivo o almacenados aparte.

En caso de sincronización, debe tenerse también en cuenta que, si se eliminan o modifican archivos de una ubicación, esto se reflejará en las demás ubicaciones al conectarse a internet, por lo que debe tomarse especial precaución con el borrado y la sobreescritura de archivos.

Cuando eliminamos algo por error, podemos recuperarlo al mantener cualquiera de los otros dispositivos sin conexión, hasta recuperar los archivos buscando la versión que allí se encuentra. No obstante, la mayoría de los servicios de almacenamiento en la nube cuentan con papelera de reciclaje desde donde se pueden recuperar archivos borrados.

Muchos servicios, al ser gratuitos, tampoco garantizan la disponibilidad del servicio, y al haber algún problema podemos llegar a perder nuestra información. Por lo tanto, mientras más valioso sea para nosotros el contenido, más aún deberíamos optar por servicios pagos que garanticen que esté debidamente resguardado y no se pierda por problemas en el servicio.

Finalmente, no está de más mencionar los últimos dos temas relacionados con la seguridad del almacenamiento en la nube: las contraseñas de acceso y la legalidad de los contenidos.

Más adelante, abordaremos en detalle la cuestión de las contraseñas, por lo que aquí solo diremos que estos servicios a los que aludimos emplean usuario y contraseña para acceder; esta última debe ser robusta para que no pueda ser descubierta fácilmente por hackers maliciosos que intentarán robar y/o borrar nuestra información.

Para terminar, no debemos tener en nuestros almacenamientos en la nube copias de archivos con derechos de autor (películas, música o libros de origen ilícito) ya que podrían ser detectados por

el proveedor del servicio, y que este mismo nos bloquee la cuenta, con la consiguiente pérdida de la información almacenada que teníamos. Al ser un servicio gratuito, no hay muchos reclamos que se puedan hacer cuando, por cualquier razón, perdemos acceso a nuestra cuenta. Esto es muy importante tenerlo en consideración, en tanto la mayoría de los servicios de internet que utilizamos son gratuitos.

Redes sociales

Antes de entrar en el aspecto online de las redes sociales, es conveniente comprender su concepto previo. Las redes sociales son, por definición, estructuras sociales formadas por individuos que se interrelacionan de distintas maneras. Internet, junto con los avances tecnológicos en general, han conformado versiones virtuales, sumándose a las relaciones sociales ya conocidas. Así surge la posibilidad de conectar con amigos y conocidos, en base a la idea de que todos podemos estar potencialmente conectados con todo el mundo a través de los contactos de nuestros contactos, según lo afirma la famosa teoría de los seis grados, la cual sostiene que estamos separados de cualquier persona en el mundo por un máximo de otras seis conocidas entre sí.

Esta nueva forma de relacionarse en internet dio origen a un modo distinto de comunicarse, que debió ser en los comienzos necesariamente por escrito, hasta que aparecieron las capacidades multimedia, las cuales permitieron interactuar por medio de imágenes, voz y video.

Además de Facebook, existen otras para compartir contenidos en forma de fotos y material gráfico, como lo son Instagram, TikTok, Pinterest, de videos como YouTube (aunque no sea considerada estrictamente una red social) o también de contenidos cortos como X (antes Twitter). Incluso hay algunas redes de uso más bien profesional y de negocios, como LinkedIn.

Pero no todo ha sido ventajoso, ya que la tecnología trae aparejados riesgos a veces poco visibles. En este caso, las propias capacidades de las redes sociales han permitido que gente malintencionada pueda abusar de sus características. Un ejemplo es la cantidad de perfiles en redes sociales que difunden noticias

falsas, publicidad engañosa, aplicaciones maliciosas y que buscan realizar estafas y robar datos. Todo esto no es fácil de controlar ni siquiera por la propia red y da lugar a que sea, desde el principio, un canal de distribución de contenidos inapropiados y aplicaciones maliciosas.

En general hay que tener mucho cuidado al instalar aplicaciones recomendadas en redes sociales (ya sean para el teléfono móvil, tablet o computadora) que prometen funcionalidades novedosas o extraordinarias, como verificar quién vio tu perfil, quién dejó de seguirte, quién leyó tu mensaje, aunque tenga bloqueada esa funcionalidad, etc. Por lo general estas aplicaciones son falsas, y si las instalamos podrían terminar robando nuestros datos, cuenta de la red social e, incluso, infectar con programas maliciosos las computadoras o dispositivos móviles.

Actualmente es muy común que varios servicios en internet, ya sean aplicaciones web, móviles, entre otras, permitan registrarnos e ingresar utilizando nuestra cuenta de una red social u otro servicio (por ejemplo, una cuenta de Google), de manera tal que no tengamos que ingresar usuario y contraseña, así como tampoco proveer datos personales ya que estos últimos son obtenidos de nuestro perfil de la red social. Cuando utilizamos esta funcionalidad, los servicios necesitan que les demos permisos específicos sobre las acciones que pueden realizar con nuestra red social, con lo que hay que estar muy atentos y examinar detenidamente qué aprobaciones solicitan y si realmente es necesario otorgárselas (a veces se puede elegir qué permisos autorizar).

La mejor opción es siempre otorgar la menor cantidad de permisos posible. De este modo, si un servicio es hackeado, su impacto en nuestra red social será limitado. Algunas autorizaciones permiten incluso agregar contenido, lo que podría ser aprovechado por un atacante para publicar libremente en nuestra cuenta.

Otro de los temas a tener en cuenta en las redes sociales es el de los contactos, ya que la mayoría de la gente acepta agregar en su red social a gente que no conoce personalmente o a cualquier persona que se lo solicita. Esto probablemente se deba a la falsa sensación de confianza que brinda el hecho de estar conectado a través de la tecnología, que es una relación virtual y no se está físicamente en un lugar compartiendo algo con esas personas.

Lógicamente, no se recomienda tener como contactos en las redes a personas que no conocemos, a menos que por contactos en común puedan resultarnos confiables, condición que debería ser validada por alguno de dichos contactos. Las personas desconocidas pueden ser de cualquier parte del mundo y tener distintas intenciones que pueden no ser buenas. En el caso de los niños y jóvenes que utilizan permanentemente las redes sociales, es importante que conozcan los riesgos de agregar contactos que no pertenecen a su círculo de confianza.

Antes de añadir un contacto deberíamos tomarnos un tiempo para analizar si es alguien a quien realmente conocemos y no un perfil falso. No se pierde nada con preguntarle a la persona quién es y de dónde nos conoce. Una buena regla es desconfiar siempre. Hay que tener en cuenta que al aceptar a alguien que no conocemos –o con una identidad falsa– en nuestra red social, quien esté detrás de ese perfil podrá tener acceso a gran parte de nuestra información, dependiendo de cómo tengamos configurada las opciones de privacidad de la red social. Una buena estrategia es optar por restringirlas en la mayor medida posible para evitar compartir información.

Continuando con los riesgos de las redes sociales, es muy común que llenemos los perfiles de información personal, fotos u opiniones, lo cual no tiene nada de malo. El tema a analizar aquí es si realmente queremos que se vea reflejado tanto de nosotros en

internet ya que, si bien solo queda visible para nuestros contactos directos, cualquiera de ellos podría copiarlo y llevarlo a otro entorno donde no cuenten las reglas de privacidad de nuestra red social en cuestión.

Para estar siempre precavidos y tener mayor seguridad en el uso de las redes sociales, es bueno pensar que cualquier cosa que compartamos con alguien puede llegar a muchas más personas, ya que una vez compartido no tenemos más control sobre eso, en tanto la persona que lo recibió lo puede compartir fácilmente con cualquiera. Por ejemplo, si comparto una foto del cumpleaños de mi hijo solo con unos pocos amigos a través de Facebook, cualquiera de ellos puede compartir luego esa imagen, por más que inicialmente yo haya querido limitar el acceso. O sea, compartimos algo con unas pocas personas, pero después no podemos controlar qué es lo que ellas hacen.

Una buena regla general a adoptar para minimizar los riesgos es preguntarnos si la información que pensamos subir a una red social se la comentaríamos a un extraño o si eso podría ser usado en contra nuestra al caer en manos de desconocidos. En base a la respuesta que nos demos podremos decidir mejor lo que exponemos en forma más consciente y teniendo en cuenta las posibles consecuencias.

Una cuestión que no escapa a ningún servicio online es el de las contraseñas; debemos cuidar que no sean fácilmente deducibles, así como tampoco utilizar las mismas que aplicamos en otros servicios. Una configuración muy útil que presentan varios servicios es la posibilidad de agregar un segundo factor de autenticación, que usualmente es un código numérico. Esa clave es requerida además de la contraseña y enviada al usuario vía mensaje de texto (SMS) o correo electrónico para confirmar que sea quien dice ser. De esta forma, si alguien obtiene nuestra password, no podrá ingresar si no

cuenta también con el código. Al ser dependiente de cada red social, es necesario configurar esta característica en cada plataforma.

Mensajería instantánea

Una de las formas de conexión más relevantes desde la masificación de internet fueron los sistemas de mensajería instantánea –también llamada IM, por Instant Messaging.– Son sistemas de charla virtual o chat en tiempo real entre personas que interactúan mediante texto, voz, imagen y video. Esto requiere que un usuario utilice un software que se conecta a un servicio de internet donde también se suman otras personas, permitiendo la interacción entre todos. La conexión se realiza de forma transparente para el usuario, por lo que solo debe instalar el software correspondiente, obtener una cuenta válida y acceder.

Algunos de los servicios de mensajería instantánea más populares han sido ICQ, Yahoo!, Messenger, AOL Instant Messenger, Windows Live Messenger y Google Talk, entre otros; muchos de ellos ya no existen o están en desuso. Hoy los sistemas de mensajería instantánea son dominados por aquellos que permiten el uso directo desde el teléfono celular o tablet, aunque tengan sus versiones para computadora o, incluso, versión web online. Ejemplos de estos son WhatsApp, Telegram, Signal, Messenger.

Actualmente también las redes sociales permiten intercambio de mensajes directos entre usuarios con casi la misma funcionalidad que los sistemas de mensajería instantánea.

En los sistemas de mensajería instantánea, además de chat e intercambio de mensajes, se permite también –por lo general– el envío de ciertos tipos de archivos, conversaciones de voz y video, entre otras funcionalidades. Así, la posibilidad de generar conversaciones con amigos, familiares y conocidos, sumado a la facilidad de tener todo disponible desde un dispositivo móvil, hace

que la mensajería instantánea sea el medio de comunicación preferido por las nuevas generaciones, incluso por sobre el correo electrónico.

Los riesgos asociados a la mensajería instantánea no son muy diferentes a los existentes en las redes sociales. Dado que muchos están asociados a nuestro celular y a nuestro número de teléfono, debemos configurar los programas para que no queden visibles nuestros datos y foto de perfil antes de aceptar comunicarnos con alguna persona, o bien hasta no haberla agregado a nuestra agenda de contactos.

Es importante, además, no confiar solamente en la foto de perfil para creer que se trata de la persona en cuestión, ya que cualquiera podría ponerse el retrato de otra persona para así generar confianza y ser agregada a la lista de contactos.

En el caso de los menores, adicionalmente, es importante que solo agreguen a sus contactos a personas conocidas. En este mismo sentido, si detectamos un comportamiento extraño de parte de alguien, si pide determinada información o cosas similares, debemos asegurarnos de que esa persona es quien dice ser, ya que quizás su teléfono ha sido robado o su cuenta hackeada.

Otro riesgo que debemos considerar a la hora de utilizar sistemas de mensajería instantánea es el de los mensajes fraudulentos o engañosos (scam), los cuales son enviados de forma directa entre usuarios o masivamente (spam) que aseguran que hemos ganado un premio, que el sistema se hará pago y que para mantenerlo gratuito se debe donar un dólar o reenviar el mensaje a una determinada cantidad de contactos, similar a lo mencionado luego en «el cuento del tío» y otros engaños, o visitar cierto sito web.

En la misma línea descrita anteriormente, debemos tener especial cuidado con los enlaces hacia sitios web que abrimos

desde los programas de mensajería, ya que se podría acceder a contenidos maliciosos o descargar algún tipo de programa dañino.

Finalmente, hay que recordar que no se debe confiar en las aplicaciones ni software de cualquier tipo que prometa funcionalidades especiales para los sistemas de mensajería instantánea. Por ejemplo, que permita saber quién abrió la foto de perfil, si un usuario está conectado o a qué hora lo hizo por última vez, aunque tenga desactivada la función, detectar quién nos tiene bloqueados y cualquier otro tipo de promesa similar, ya que, como se ha mencionado, son falsas.

Como último consejo, es importante saber que, aunque muchos sistemas de mensajería ofrecen comunicación segura de extremo a extremo por medio de canales encriptados, no se recomienda el envío de información confidencial o sensible (audios, fotos y videos comprometedores) a través de estos sistemas. Si bien algunas aplicaciones borran inmediatamente los mensajes, nunca podemos estar seguros de que el mensaje no caiga en manos equivocadas, ya sea por descuidos, robos o hacking.

Juegos online y de consola

Suele creerse erróneamente que los juegos de computadora, consolas y teléfonos móviles son solo cosa de niños, pero nada más lejos de la realidad. Muchos adultos son usuarios de juegos y, aunque no corren los mismos riesgos, deben tener en cuenta algunos puntos para permanecer más seguros. Por ejemplo, las consolas de videojuegos como Microsoft Xbox, Nintendo Wii y Sony PlayStation ofrecen una plataforma especialmente diseñada para jugar, tanto individualmente como en grupo. Estos dispositivos no deberían incluir riesgos en particular, salvo que el fabricante sea víctima de un ataque que permita que se conozca la información de las tarjetas de crédito de sus clientes, como ocurrió con la PlayStation Network de Sony en el año 2011. En estos casos no es posible tomar medidas de prevención, ya que dicho problema no depende del usuario final sino del proveedor del servicio.

En el caso de los juegos de PC o dispositivos móviles, por lo general, es necesario disponer de una cuenta de acceso al igual que con otros servicios, ya que debemos proveer un usuario y contraseña, datos personales, en algunos casos de tarjeta de crédito y demás. Muchos malintencionados buscan apropiarse de cuentas de usuarios para obtener acceso a información personal. Para ello utilizan cuentas de correo electrónico falsas, envío de mensajes por SMS o mensajería instantánea a fin de contactarse para solicitar un cambio de contraseña utilizando mensajes engañosos que nos lleven a tener que acceder a un sitio falso en el que, de ingresar nuestro usuario y contraseña, serán capturados por el criminal. Ante la duda, podemos contactar al servicio de atención al cliente del juego por otra vía para determinar si el mensaje es auténtico; asimismo, podemos verificar si el sitio web que nos pide

nuestro usuario y contraseña es realmente un sitio válido del servicio que utilizamos.

En la actualidad, muchos juegos disponen de algún tipo de moneda virtual, que es usada para comprar objetos y servicios adicionales dentro del propio juego o para acelerar niveles y características. En estos casos, debemos evitar realizar compras de bienes para el juego fuera de la plataforma. También hay quienes se ofrecen a jugar por nosotros para avanzar niveles o realizar trucos, lo que también debemos evitar ya que, para hacerlo, deberíamos proporcionarle datos de acceso personales a la plataforma, en la que se encuentran nuestros datos e ítems virtuales (monedas, bienes, etcétera).

Como en todo software, algunos usuarios utilizan programas llamados cracks que permiten su uso sin pagar las licencias correspondientes, lo que es ilegal. Hay quienes recurren a juegos comerciales sin pagar, mediante la aplicación de estos cracks, en donde es común que los ciberdelincuentes puedan incluir software malicioso que termine infectando la computadora del usuario para luego realizar acciones malintencionadas hacia el propio sistema como el robo de contraseñas, secuestro de archivos y demás. Para evitar este problema, debemos asegurarnos de obtenerlos a través de proveedores autorizados o vías oficiales del fabricante, evitando así actividades ilegales.

Respecto a los menores, es importante que eviten el contacto con jugadores desconocidos por medio del sistema de mensajería interna (chat) de la plataforma, ya que esto podría derivar en un caso de acoso, extorsión, etcétera. Es común que lo niños jueguen, confíen y hablen con cualquiera que los contacte dentro de los juegos, lo cual puede ser peligroso ya que pueden relacionarse con un desconocido desde cualquier parte del mundo que no tenga buenas intenciones.

Con relación a la problemática que apuntamos aquí, puedo referir una situación vivida con mi hijo de ocho años, quien me comenta que alguien desde el chat de un juego de internet lo había insultado. Por supuesto, no me pareció bien que esté usando estos sistemas de mensajería para hablar con desconocidos. Si bien ya le había recomendado que no utilice estos chats, de hacerlo, que no hable con cualquier persona, pero él seguía haciéndolo ya que también se comunicaba con sus amigos.

Mi hijo, entonces, me mostró el chat –que es abierto para quien quiera acceder– y observé, incluso, que muchos de sus compañeros exponían su nombre y hasta nombraban la escuela. Le expliqué, nuevamente, sobre los peligros de hablar con desconocidos con un ejemplo, quizás extremo: un delincuente que se haga pasar por un amigo suyo para sacarle información personal y localizarlo para hacerle daño a él o a la familia. Tal suposición llamó su atención y lo asustó, pero le señalé sobre la importancia de que los niños sepan que esos peligros existen y deben ser evitados. Claro que sigue usando el chat, pero ahora con mayor precaución. Por eso, es fundamental alertarlos y explicarles hasta que comprendan los riesgos que se corren usando estos chats.

Descarga segura de contenidos

Cuando queremos bajar contenidos desde internet existen varias opciones. Las más comunes son las directas y las redes P2P (*peer to peer*). Estas últimas permiten que un contenido pueda ser descargado y compartido por muchos usuarios a la vez sin que haya necesidad de un sitio central que lo almacene, sino que todos los usuarios actúan como potenciales distribuidores. De tal manera, cuando uno quiere obtener un archivo, la operación se realiza desde las computadoras de los usuarios que lo comparten y están conectados en ese momento. En contrapartida, un sitio de descarga directa ofrece enlaces al mismo sitio u otros que alojan los archivos, por lo que el archivo se recibe directamente desde un lugar especial.

Los programas para realizar descargas por redes P2P (eMule, BitTorrent, etcétera) nos permiten configurar qué carpetas de nuestro sistema deseamos compartir con el resto de los usuarios de la red, por lo que debemos prestar mucha atención y asegurarnos de que solo compartimos la que corresponde (en general es la misma en la que se descargan los archivos) y ninguna otra, sin cometer el error de poner archivos privados a disposición de cualquiera, algo que suele suceder, en tanto los usuarios terminan compartiendo información con todo el mundo sin darse cuenta.

Es importante mencionar que los archivos se bajan de a fragmentos, de forma que, al terminar de descargarse, este se pone a disposición del resto de los usuarios de la red pese a no haber completado aún la descarga total. El problema de esto es que podríamos estar bajando contenidos ilegales sin saberlo y funcionando como canal de redistribución de tales contenidos, pues los fragmentos se comparten todo el tiempo y no sabemos si el material descargado es el esperado hasta tanto no finalice la

operación en cuestión. Al momento de la verificación, cuando está en nuestro disco rígido, ya habremos compartido el material ilegal en toda la red. Para evitarlo es necesario revisar los comentarios de los demás usuarios antes de actuar, analizar las puntuaciones que se le dio a la descarga y ver la cantidad de personas que lo comparten, lo cual es falible, pero mejora las posibilidades de estar obteniendo lo que efectivamente deseábamos.

Luego de finalizada la descarga, siempre es importante constatar que se trate del contenido esperado, revisándolo detenidamente, ya que muchas veces bajamos cosas que quedan almacenadas y corremos el riesgo de estar compartiendo material ilegal sin siquiera saberlo. Al compartir material fraudulento, podemos tener serias consecuencias, como problemas judiciales, en caso de ser detectados.

El material ilegal más común puede ser música, películas, software, entre otros; pero también podría ser material muy sensible –como imágenes y videos inapropiados– que pueda causarnos graves problemas al distribuirlo sin darnos cuenta.

Otro riesgo típico de las descargas de internet, en general, es que los archivos contengan algún tipo de software malicioso (malware). Esto es especialmente peligroso cuando son archivos ejecutables, como aplicaciones o programas de computadora. Para que esto no suceda se recomienda tener siempre un programa antivirus funcionando y actualizado, así como también evitar descargar programas de sitios dudosos o que no sean los sitios oficiales del fabricante del software que queremos obtener.

Siguiendo con los riesgos y considerando que algunos sitios de descarga directa ganan dinero principalmente por medio de las publicidades en sus páginas web, es importante saber que muchas veces estos carteles de anuncios se presentan simulando ser un

botón o enlace para bajar el archivo, para así llevarnos a sitios que puedan infectar nuestra computadora con programas maliciosos.

Es fundamental también evitar cualquier tipo de acción que solicite el sitio de descarga como paso intermedio para acceder al contenido, por ejemplo, instalar una aplicación, modificar la configuración del navegador, enviar mensajes de texto, proveer el número de teléfono celular, etcétera. Si realizamos esas acciones podríamos terminar con nuestra computadora infectada con software malicioso o subscriptos a algún servicio pago de telefonía celular. De igual manera, si algún cartel o mensaje de un sitio nos indica que nuestro equipo está infectado, no debemos prestarle atención y solo hacerlo cuando nuestro propio software antivirus nos alerte de una posible amenaza.

Es un engaño común que un sitio web malicioso nos diga que nuestro equipo está infectado y que debemos descargar e instalar el programa que nos recomienda para poder limpiarlo. A lo que, de hacerle caso, seguro terminaremos infectándolo verdaderamente con ese mismo programa que nos está sugiriendo, ya que se trata de un programa malicioso y no de un antivirus real.

Finalmente, existen muchos sitios web que, al querer bajar de allí un archivo, nos piden introducir nuestro número de teléfono celular bajo cualquier excusa, como la verificación de edad o identidad para el envío de un enlace a lo que se busca descargar por SMS o pretextos similares. Se trata de procedimientos que no debemos accionar dado que, en ese caso, es muy posible que terminemos suscritos a algún tipo de servicio de tarifa especial (SMS Premium) que nos generaría costos y cargos adicionales a nuestro servicio de telefonía móvil, o que luego nos envíen mensajes para engañarnos.

En general, se debe evitar introducir cualquier información personal que nos soliciten los sitios desconocidos al momento de querer realizar una descarga.

Cómo evitar los virus y otras amenazas

Los virus son un tipo de software malicioso a los que, de manera general, se denomina malware (de *malicious software*). En la actualidad, técnicamente es incorrecto hablar siempre de virus ya que las infecciones se dan por distintos tipos de malware, pero dado que es un concepto que prácticamente cualquier persona conoce o tiene referencia, se lo utiliza a menudo para describir a este tipo de amenazas que infectan nuestro sistema.

El malware llega a nuestros sistemas por distintas vías:

- Correo electrónico: los mensajes de e-mail pueden contener archivos adjuntos maliciosos o bien enlaces a sitios maliciosos que buscarán infectarnos al hacer clic. Los mensajes pueden, incluso, provenir de personas conocidas, ya que es posible que sus equipos hayan sido infectados o que el mensaje recibido tenga el remitente falsificado.
- Medios de almacenamiento externos: los pendrives, discos USB, discos externos, tarjetas de memoria y cualquier tipo de dispositivo que se conecte al equipo puede contener software malicioso, el cual se transmite a nuestra computadora al abrir archivos infectados, aunque a veces con solo conectar el dispositivo el equipo también podría quedar afectado. Por lo tanto, se debe evitar conectar cualquier dispositivo desconocido a nuestro equipo, como así también abrir un archivo sin tener el antivirus actualizado y activado.
- Descarga de archivos de internet: siempre que bajamos programas de internet tenemos que analizar si no contiene

algún tipo de malware, especialmente si no lo hacemos desde un canal oficial o conocido.

- Sitios web maliciosos: existen muchos sitios especialmente diseñados por los ciberdelincuentes para infectar a los usuarios que los visitan mediante el aprovechamiento de alguna vulnerabilidad en sus sistemas. También podría haber sitios web reales que han sido alterados por un agresor para atacar, aprovechándose de la confianza de los usuarios.
- Redes sociales: los ciberdelincuentes buscan víctimas en aquellos ámbitos donde hay mayor cantidad de personas, por lo que las redes sociales son terreno fértil. Por esto es que debemos tener cuidado de evitar acceder por curiosidad a enlaces o publicaciones que anuncien alguna noticia muy novedosa o llamativa (muerte de algún famoso, catástrofes, eventos internacionales, etcétera), ya que podríamos terminar en un sitio web malicioso, como indicábamos anteriormente. De aparecer alguna aplicación que nos pida autorización innecesaria para acceder a nuestra información personal, debemos cancelar y bloquearla.
- Vulnerabilidades: en caso de que cualquier programa de nuestro equipo (el sistema operativo o alguna aplicación) no esté totalmente actualizado, correremos el riesgo de que esto pueda ser aprovechado por atacantes y ser infectados por malware –por lo general– sin que el usuario siquiera haya ejecutado algo, pues solo basta con visitar un sitio web o abrir algún archivo.

El malware puede acarrear distintas consecuencias, pero sus principales acciones maliciosas suelen ser las siguientes:

- Cifrado (encriptación) de nuestros archivos: existe un tipo llamado ransomware que bloquea el acceso a nuestros propios archivos mediante su cifrado, evitando así que podamos acceder a la información a menos que realicemos un pago a través de internet por el monto que indique el atacante –a modo de secuestro extorsivo virtual. Una vez realizado el pago, los delincuentes suelen proveer un mecanismo para que recuperemos los datos, pero al tratarse de delincuentes nada garantiza que después de abonar podamos recuperar nuestra información.
- Robo de datos: nuestra información personal y archivos son un blanco típico para los atacantes, ya que luego son vendidos en bases de datos o utilizados para otros malos fines. Más allá de la pérdida de la privacidad, esto también puede derivar en el robo de identidad (virtual o físico) y la pérdida de acceso a nuestros servicios.
- Pérdidas económicas: si un virus puede acceder a nuestros datos –de tarjetas de crédito o débito, nombres de usuario y contraseñas, etcétera– podrá enviar al atacante dicha información para que luego él mismo se conecte, por ejemplo, a nuestro sistema bancario y nos robe el dinero de las cuentas, o bien realice operaciones con nuestras tarjetas de crédito o débito.

Para evitar este tipo de problemas, existen varias medidas que deben ser tomadas en simultáneo:

- Utilizar un software antivirus: es fundamental usar algún programa antivirus en nuestros sistemas y mantenerlo siempre actualizado. Esto aplica no solo para sistemas Windows sino también para sistemas Mac OS o Linux, pese a que las

amenazas para estos últimos son menores en cantidad al ser menos populares en comparación con Windows. El software antivirus incluye, además, funciones como la verificación de sitios web y la protección del correo electrónico, entre otras.

- En cuanto a la descarga de antivirus piratas, debe ser evitada, ya que, de estar «crackeados» (es decir, modificados ilegalmente), pueden ser el canal principal para que nos infectemos, que es justamente aquello que queremos evitar. En caso de que no queramos o no estemos en condiciones de pagar por un producto antivirus, podemos utilizar productos gratuitos que funcionan muy bien y son igualmente efectivos la enorme mayoría de las veces. En cualquier caso, el software debe descargarse del sitio oficial del fabricante. Otra cuestión a tener en cuenta es que no debe instalarse más de un antivirus en un mismo sistema, ya que sus funcionamientos podrían ser inestables al convivir en tal equipo.
- Mantener la totalidad del software actualizado: las actualizaciones de seguridad de todo programa (sistema operativo, navegadores, aplicaciones y demás software del sistema) deben ser siempre instaladas apenas estén disponibles. Esto evita que las vulnerabilidades que las actualizaciones reparan sean aprovechadas por malware y otros programas para infectar nuestros equipos. La forma más sencilla de evitar olvidarnos de esto es configurar los programas para que descarguen e instalen las actualizaciones automáticamente, algo que estos pueden ejecutar casi siempre.
- Realizar copias de seguridad: ante el riesgo de perder archivos por infecciones de malware, es conveniente tener copias de respaldo realizadas con cierta frecuencia (según su uso) en

una ubicación diferente a la del equipo que contiene los archivos originales. Otra alternativa es tenerlos sincronizados con un servicio de almacenamiento en la nube u otro almacenamiento externo.

- Pero hay que tener cuidado cuando la sincronización con almacenamiento externo se hace de forma automática, ya que, si los archivos están infectados o cifrados por malware, al realizarse se pueden sobrescribir las copias que teníamos que no estaban infectadas y, de esta forma, se contagiarían.
- Evitar usuarios administradores: los usuarios administradores del sistema operativo (Windows, Linux, etcétera) tienen control total sobre el sistema, por lo que cualquier acción que un software malicioso realice utilizando un usuario administrador podría tener consecuencias graves. Para evitar esto pueden utilizarse usuarios comunes en el uso cotidiano del sistema, puesto que cuentan con menores privilegios y permisos, y no pueden ejecutar ciertos programas o accionar sobre el sistema de la misma forma que el administrador. De esta manera, se puede minimizar el impacto de un software malicioso, ya que así se limitan las acciones que puede realizar en nuestro sistema.
- Utilizar un firewall personal: este software puede evitar las conexiones indeseadas desde y hacia nuestro sistema, además de mejorar la detección de comportamientos maliciosos en el equipo. En general, el propio sistema operativo cuenta con un firewall personal que se recomienda mantener activado siempre.
- Aplicar el sentido común: el uso mismo de internet y la tecnología hace que vayamos detectando las cosas normales y las diferenciemos de las anómalas. La actitud de precaución

y buenas prácticas de uso cotidiano pueden evitar –en gran medida– que nuestros equipos resulten infectados. Por ejemplo, abstenerse de ejecutar programas de origen desconocido o de acceder a enlaces y sitios web sospechosos, así como también de abrir archivos adjuntos dudosos en correos electrónicos.

Cuentos del tío y otros engaños

Una de las técnicas más comunes que emplean los hackers maliciosos para realizar ataques es el engaño a través de distintos métodos.

Así como en la vida real la gente dedicada al fraude trata de engañar a las víctimas a través de elaboradas técnicas, como por ejemplo los «cuentos del tío», en la vida online hay estafas similares que explotan la confianza, la urgencia, los descuidos y la ambición de las personas para obtener información o lograr que estas realicen determinada acción.

Estos ataques, en los cuales se busca engañar a la víctima para que provea sus datos y robárselos, se los llama phishing, que es una deformación de *fishing*, cuyo significado es «pescar», ya que se utiliza una «carnada» (engaño) para obtener lo buscado y se «pesca» a la víctima.

El medio más común para realizar estos ataques es el correo electrónico, pero también se utilizan mensajes de texto (SMS), de WhatsApp y de Facebook, entre otros. La trampa consiste en hacerle creer a la víctima que tiene que realizar determinada acción que puede ser abrir un archivo, hacer clic en un enlace, ingresar su usuario y contraseña o proveer otros datos, etcétera. Para esto se utilizan distintos tipos de mensajes que dicen provenir de una fuente confiable para la víctima, como su banco, Facebook, su empresa de tarjeta de crédito, su proveedor de telefonía móvil, etcétera.

Los mensajes utilizados para este tipo de estafas suelen apelar a la urgencia para que la víctima tome acción inmediata sin pensar mucho. Por ejemplo, una persona puede recibir un e-mail que parece provenir de su banco diciendo que necesita actualizar su nombre de usuario y contraseña haciendo clic en un enlace, o

puede parecer un e-mail desde Facebook diciendo que alguien ha querido ingresar a su cuenta y que necesita confirmar su usuario y contraseña para ver que esté todo bien. Una vez que la víctima ingresa los datos solicitados, estos quedan en posesión de los atacantes.

Otros mensajes explotan la ambición de la víctima para que esta realice lo que se le pide; estos pueden aludir a que la víctima se ha ganado un premio o dinero y que necesita proveer sus datos personales de forma urgente para poder cobrarlo. También, los mensajes pueden traer archivos adjuntos y tratar de engañar a la víctima para que los abra, en tanto, generalmente, contienen malware y, una vez abiertos, infectan la computadora para luego robar datos.

En general, estas artimañas pueden ser bastante convincentes, ya que utilizan los mismos diseños gráficos (imágenes, textos, estética, etcétera) de las empresas verdaderas de las cuales simulan provenir. Incluso, las direcciones web de los sitios falsos donde se pide a las víctimas ingresar sus datos son similares a la de los verdaderos. Por ejemplo, la dirección web del engaño puede ser www.faceb00k.com; en vez de dos letras «o» son dos ceros («0»), pero, a simple vista, parece que fuera la dirección verdadera www.facebook.com, al ser los ceros parecidos a la letra «o».

Otro recurso utilizado por los atacantes para engañar es ocultar las direcciones de los sitios web falsos utilizando direcciones web acortadas; estas se obtienen mediante servicios de direcciones web que hacen que una dirección web determinada pueda ser representada en forma más corta y distinta. Por ejemplo, Google tiene un servicio goo.gl en el cual podemos ingresar cualquier dirección web y permite crear una nueva dirección acortada y distinta como goo.gl/Ub1XC1. Entonces, una víctima puede recibir un enlace con una dirección web acortada que, al cliquear sobre

ella, el navegador web es redirigido automáticamente hacia la dirección web final del sitio falso, que es distinta a la que decía el enlace donde se hizo clic.

Debido a esto, siempre se debe prestar atención a qué direcciones contienen los enlaces en los mensajes que nos llegan y luego, si hacemos clic, ver qué dirección termina mostrando nuestro navegador, ya que la que tiene el enlace sobre el que cliqueamos puede ser muy distinta a la que se nos muestra.

Para no ser víctima de estos engaños, en primera instancia hay que evitar hacer clic ya sea sobre enlaces o sobre archivos que recibamos a través de un mensaje (e-mail, SMS, WhatsApp, Facebook, etcétera) si este proviene de alguien que no conocemos; lo ideal sería ignorarlos.

En caso de que el mensaje provenga de una fuente confiable (o lo pareciera), nunca debemos proveer nuestros datos ya que, por lo general, los servicios que utilizamos no los requieren de esta forma; por eso, ante la duda, se puede llamar por teléfono a la empresa para confirmar la veracidad del mensaje. Si el mensaje parece real y muy convincente, el último recurso que queda para evitar engaños es inspeccionar detalladamente que el sitio web donde se nos pide ingresar información personal sea ciertamente el sitio verdadero de nuestro servicio. Para esto debemos ver que la dirección del sitio web corresponda exactamente con la dirección real; o sea, si se trata de Instagram, que la dirección sea www.instagram.com y no otra; si es de «nuestro banco», que la dirección sea www.NuestroBanco.com. Si usamos con regularidad el servicio, seguramente conocemos cuál es la dirección auténtica, y, si no la sabemos, es bueno averiguarla para evitar estos engaños.

Se debe desconfiar siempre de cualquier tipo de mensaje que se recibe y pensar dos veces antes de hacer clic; de no sospechar,

probablemente se termine siendo víctima de estas estafas virtuales. Nunca descuidarse, estar siempre atentos.

La mayoría protegemos fuertemente nuestros hogares. En la parte externa, usualmente ponemos rejas en las ventanas, en el frente, paredes altas con alambres de púas o elementos cortantes. Iluminamos bien la entrada y también colocamos cerraduras con llave o candados en puertas y portones de entrada. En algunos casos, incluso, hay cámaras de vigilancia y hasta contratamos servicios de alarmas para detectar posibles intrusos. Estas son protecciones comunes en nuestros hogares; sin embargo, los delincuentes siempre encuentran formas de sobrepasarlas.

Podemos decir, entonces, que no debemos confiar solamente en las protecciones; no importa con cuántas contemos, tenemos que ser precavidos y estar atentos a todo. Lo mismo sucede en el mundo virtual: podemos tener muchas protecciones, pero nunca hay que descuidarse; siempre tenemos que estar alerta y sospechar cuando vemos algo extraño al utilizar cualquier tecnología e internet de la misma forma que lo hacemos en nuestra vida cotidiana. Es bueno estar informado y actualizado constantemente sobre las amenazas y peligros relacionados con el uso de la tecnología.

Importante recordar

- En internet estamos expuestos a muchos riesgos, debemos conocer y entender cuáles son los peligros actuales y saber qué podemos hacer para evitarlos.
- Debemos proteger nuestros datos. No importa si usamos o no internet, nuestra información puede encontrarse de manera accesible igualmente.
- Todo lo que hacemos en internet queda registrado. Si queremos ser anónimos y tener privacidad tenemos que tomar medidas usando herramientas específicas.
- Si hay información muy importante para nosotros, siempre debemos tenerla guardada en más de un lugar, sin importar que esté o no en la nube; de esta manera, si por cualquier causa esa información deja de estar disponible en la nube, siempre la tendremos a salvo en otro lugar.
- Debemos tener cuidado y verificar a quiénes agregamos como contactos a nuestras redes sociales. Lo que allí publicamos puede ser visto por cualquiera, por más que inicialmente lo compartamos solo con unas pocas personas. Hay que limitar al máximo los permisos que otorgamos a los servicios a los que ingresamos con nuestra cuenta de red social. Pensar antes de publicar si aquello que compartiremos se lo diríamos a un extraño o si podría ser utilizado en nuestra contra de alguna manera.
- No enviar información confidencial o comprometedora a través de mensajería instantánea; nunca se sabe en manos de quién puede caer. No aceptar comunicaciones de desconocidos.

- Evitar utilizar programas para sobrepasar protecciones de juegos y no pagar, ya que esto –además de ser ilegal– puede terminar infectando nuestro sistema con software malicioso. Recomendar a los menores que no se comuniquen con extraños, que no utilicen sus nombres reales ni provean información en los chats de los juegos.
- Prestar atención al contenido que se descarga, que no sea ilegal.
- Siempre recurrir a contenidos de fuentes seguras y no de sitios extraños.
- Evitar introducir cualquier información para realizar una descarga.
- Evitar los virus y otras amenazas.
- Estar alerta a los posibles engaños, desconfiar siempre y verificar la veracidad de lo que recibimos. Nunca descuidarse.

---

2 Método de codificar datos para que no puedan ser leídos por nadie excepto por las partes autorizadas.

Capítulo 3

Contraseñas de acceso

En pocas palabras, podemos decir que una contraseña es la barrera principal de protección de nuestra privacidad contra personas malintencionadas.

Las contraseñas son parte de nuestra vida moderna debido al uso constante de la tecnología. Como usuarios estamos obligados a utilizarlas todo el tiempo para asegurar el acceso a un determinado sistema, servicio o autorizar alguna acción.

Las contraseñas, también llamadas claves o passwords, constituyen una de las medidas de seguridad más usadas e importantes a tener en cuenta tanto en el ámbito personal como profesional. Desde el punto de vista del acceso a un sistema o servicio, constituyen lo que se denomina un factor de autenticación, es decir, permiten que un sistema o servicio o plataforma verifique que el usuario es quien dice ser y, si es exitosa, aprueba el acceso posibilitando utilizarlo.

En un principio, hace muchos años, la verificación de las personas autorizadas se realizaba cuando estas ingresaban solamente el nombre de usuario, ya que se consideraba que no era

necesario comprobar que tal usuario era quien decía ser. Esto se debía probablemente a la poca gente que utilizaba los sistemas, que estos no estaban interconectados y que requerían generalmente acceso físico.

Con el tiempo los sistemas comenzaron a estar cada vez más interconectados y a existir personas malintencionadas, por lo que apareció la necesidad de verificar identidades que llevó a la aparición de las contraseñas aplicadas a sistemas.

Las claves se consideran un elemento delicado dentro del entorno de la seguridad de la información ya que, si una persona tiene el usuario y password de otra y lo utiliza, para un sistema será como si se tratara del usuario correcto, no pudiendo, en principio, distinguirla de un potencial atacante o usuario malintencionado. Por este motivo es que las contraseñas deben ser cuidadas y protegidas apropiadamente, ya que su pérdida o el conocimiento de estas por parte de otra persona podrían suponer que perdamos el acceso a sistemas y servicios de forma definitiva, como así también a nuestra información.

A medida que fue avanzando la tecnología, se fueron agregando dispositivos electrónicos, software y todo tipo de sistemas que requirieron una contraseña de acceso. Por su efectividad, su uso se hizo tan masivo que una persona que sea usuaria de tecnología y servicios debe manejar una cantidad de contraseñas que, en muchos casos, es difícil de recordar y gestionar.

El uso es tan cotidiano que generalmente no las tratamos como si fueran un elemento tan importante, y es por eso que es muy habitual escuchar casos de claves olvidadas, servicios a los que se ha perdido el acceso, entre otros problemas que complican a todos los usuarios.

Medidas de protección

Muchos acuden a medidas elementales para evitar el olvido de las claves: anotarlas en un papel, en un archivo de su computadora o dispositivo móvil. Esta medida se considera insegura, dado que viola el principio de confidencialidad que supone la existencia de un elemento que solo la persona debe conocer.

Cualquier otra persona que vea nuestra contraseña anotada conocerá y podrá utilizarla para ingresar al servicio correspondiente haciéndose pasar por nosotros. Con esto es lógico pensar que las contraseñas no deben ser anotadas, pero tampoco compartidas para que otro pueda recordarlas en nuestro lugar o para permitir el acceso a algún sistema en nuestra ausencia. Esto debe tenerse en cuenta muy especialmente para evitar riesgos innecesarios entre menores de edad, quienes suelen compartir sus contraseñas con amigos.

En caso de anotarlas en un papel, este tendría que ser guardado y cuidado como lo hacemos con aquellas cosas muy valiosas como dinero, joyas, etcétera. Es decir, guardar las contraseñas en una caja fuerte o de seguridad para que, en caso de que olvidemos alguna de ellas, podamos recuperar el acceso al servicio consultando el papel donde las anotamos.

Con relación a la dificultad para recordar las contraseñas cuando son varias, otra técnica empleada por los usuarios es repetirlas entre distintos servicios y sistemas, es decir, utilizar la misma para todo. Si bien esto puede ser muy práctico y funcional, es muy peligroso debido a que si una es comprometida –sea hackeada o conocida por alguien malintencionado– la persona que lo hizo podría acceder no solo a uno sino a todos los sistemas o servicios en los que utilizamos la misma contraseña. Esto es muy grave y podría

significar el robo y pérdida de toda nuestra información almacenada en los distintos sistemas y servicios que utilizamos.

En general se considera que cuanto más se utiliza una contraseña, más probable es que pueda ser adivinada y haya sido comprometida a medida que pasa el tiempo. El peor caso de todos sería si la contraseña estuviera en poder de un usuario malicioso, por lo que esta persona podría estar ingresando a nuestros sistemas con la contraseña en cuestión sin que nosotros estemos enterados de ello. Por tal motivo es que los sistemas obligan a cambiar la contraseña luego de un determinado período de tiempo, que puede ir desde algunas semanas hasta varios meses. Pero también depende del tipo de sistema del que se trate, incluso algunos nunca solicitan el cambio, por ejemplo, los servicios de correo electrónico.

En caso de que el sistema no solicite un cambio obligado de contraseña, es importante que el usuario igualmente lo realice cada tanto –cada dos, cuatro o seis meses– si quiere incrementar su seguridad, lo que elimina toda posibilidad de acceso por parte de una persona maliciosa que tuviera la contraseña anterior.

Para revertir el olvido de una contraseña, una de las medidas de seguridad provistas por distintos servicios es el de realizarnos una o más preguntas, cuya respuesta deberíamos conocer solo nosotros (llamadas normalmente «preguntas secretas»). Por ejemplo, interrogaciones típicas se refieren al nombre de la primera mascota, el apellido de soltera de la madre, el nombre de alguna abuela, el restaurante favorito y cosas por el estilo. Este mecanismo de recuperación permite que, si olvidamos la clave, podamos generar una nueva luego de responder la o las preguntas en cuestión (a veces también se solicitan algunos datos personales y otros elementos que permitan verificar fielmente al usuario). Lo importante del uso de este sistema es que podamos seleccionar cuidadosamente las preguntas que deberemos responder en caso

de olvido de clave, ya que podría ocurrir que los datos solicitados y las respuestas a dichas preguntas sean conocidos por otra persona y pueda así suplantar nuestra identidad digital para acceder, de esta manera, al sistema en nuestro lugar. En efecto, un truco que utilizan muchos es el de responder con datos falsos para evitar cualquier posible intento de adivinar la clave por parte de personas que puedan conocernos; el único detalle a tener en cuenta en estos casos es que deberíamos recordar el dato en cuestión.

Otra opción cada vez más común y útil para recuperar nuestra clave es establecer un número de teléfono celular; así, cuando la queramos rescatar, se nos enviará un mensaje de texto (SMS) con un código o instrucciones que nos permitan utilizarlos para restablecer una clave.

Algo importante con lo que también debemos tener cuidado es el uso que les damos a las funciones de «recordar contraseña» con las que cuentan todos los navegadores de internet, ya que –pese a que son realmente muy útiles– pueden tornarse riesgosas en caso de que el dispositivo sea compartido con otras personas o bien se trate de un equipo de uso público. Si nuestras claves quedan guardadas en el navegador y luego otra persona utiliza la misma computadora o dispositivo (celular, tablet, etcétera), ella podrá ingresar a nuestros servicios sin necesidad de conocer la clave. Afortunadamente, en sistemas modernos y dependiendo de la configuración, se pide otra clave o verificación biométrica para acceder.

Elección de contraseñas seguras

Ya comprendiendo la importancia de las contraseñas y sus medidas básicas de protección, es necesario conocer cómo se confecciona una contraseña para que sea considerada segura. Muchos sistemas no dejan que los usuarios elijan claves débiles y los obligan a superar un determinado nivel de complejidad para ser aceptada, lo cual, pese a su incomodidad, es una buena medida.

De nuestra parte, sea que el sistema nos fuerce o no, debemos garantizar ciertas características para una clave: que tenga una longitud mínima de ocho caracteres y que combine letras en mayúscula y minúscula, números y símbolos (caracteres especiales y signos de puntuación).

En contrapartida, podemos hablar de las claves que nunca debemos elegir, como aquellas que contengan palabras comunes de diccionario en el propio idioma, nombres de personas o lugares, el nombre mismo del usuario (o parte), fechas de nacimiento, números de teléfono (o fragmentos), números de documento (o fragmentos), números consecutivos, repetición de tres o más caracteres seguidos, combinaciones básicas (por ejemplo, nombre y año de nacimiento), o letras consecutivas del teclado.

También existen algunas técnicas utilizadas para mejorar la complejidad de las claves, como las siguientes:

Tomar una frase, quitar los espacios y cambiar las vocales por números con algún criterio determinado, como podría ser: a = 1, e = 2, i = 3, o = 4, u = 5. Por ejemplo: «Mi casa es pequeña» = M3c1s12s p2q52ñ1.

1. Utilizar alguna regla mnemotécnica, como tomar la primera letra de cada palabra de una frase que sea fácil de recordar para nosotros. Por ejemplo: «El sábado juego al fútbol 5 con mis amigos»

formaría la contraseña Esjaf5cma. De igual manera, se puede realizar con una frase de una canción que nos guste, tomando la primera letra de cada palabra para formar nuestra contraseña.

2. Basarse en un patrón determinado incorporando variantes sencillas según el sitio o servicio que se trate. Por ejemplo: tomando como base la clave «axa45mA!» podríamos utilizar en Facebook «axa45mA!FB», en Twitter «axa45mA!TW», en Gmail «axa45mA!GM», y así con cualquiera, considerando dos o tres letras que representen al servicio en cuestión. El único problema de este método es que, si un atacante descubre una de ellas, es posible que pueda deducir alguna otra si nota el patrón.

3. Las técnicas descriptas anteriormente también se pueden combinar para aumentar la seguridad, por ejemplo, la primera, o la segunda, con la tercera.

Algunas personas utilizan distintos niveles de complejidad dependiendo del servicio y de su importancia. Por ejemplo, si se trata de sitios en los que manejamos información privada o financiera, podemos utilizar contraseñas más complejas de lo normal; en aquellos que tienen poca importancia, pueden emplearse contraseñas más simples para facilitar su memorización.

Finalmente, siempre es posible utilizar algún software de generación de contraseñas, los cuales producen combinaciones de caracteres muy complejas, prácticamente imposibles de memorizar, pero que pueden ser manipuladas por gestores de contraseñas, como explicaremos a continuación.

Uso de gestores de contraseñas

Los gestores de contraseñas (*password managers*) son programas que corren en los diferentes sistemas operativos y tipos de plataforma (PC, tablets y celulares), y permiten almacenar, de forma segura, las claves de acceso a cada uno de los sistemas y servicios que se utilizan. Esto se realiza por medio de diversas técnicas y aplicación de algoritmos criptográficos que posibilitan que la información se guarde en un archivo cifrado, protegido de todo tipo de ataques externos.

En caso de utilizar un gestor, la única password que debemos recordar es la del gestor mismo, que nos permite acceder al resto de las contraseñas almacenadas. Esto implica que esa clave principal debe ser muy segura ya que, de lo contrario, quien la pueda adivinar o averiguar por algún medio podría tener acceso a toda la información de nuestras cuentas y claves guardadas. La buena noticia es que debemos recordar una sola, llamada contraseña maestra o *master password*, pero por ningún motivo debemos olvidarla ya que perderíamos el acceso al resto de las claves.

Existen gestores pagos y gratuitos. Las opciones gratuitas son muy confiables y de calidad, por lo que son altamente recomendables. Algunas opciones típicas son LastPass, RoboForm, 1Password y Dashlane.

Los programas de gestión de contraseñas permiten una serie de opciones interesantes, además de un simple almacenamiento seguro, como organizar por categorías los servicios donde se utilizan, lo que podría facilitar la gestión al tener separadas las claves de redes sociales, las de *homebanking* y tarjetas de crédito, las de servicios generales y demás.

Otra funcionalidad interesante, que no todos los gestores poseen, es la de poder sincronizarse entre distintos dispositivos para reflejar los agregados o cambios que se hagan desde cualquiera de nuestros equipos (computadora, teléfono, tablet, etcétera). Esto solo suele estar disponible en las versiones pagas de los programas. Además, no solamente puede almacenarse allí la contraseña junto al nombre de usuario y la dirección del sitio web a la que corresponde, sino también otros datos relacionados como las fechas del último cambio de clave y de acceso, el tiempo de expiración dado por el servicio en cuestión, notas adicionales y hasta archivos adjuntos.

Una característica muy interesante es la función que permite copiar la contraseña en el portapapeles del sistema operativo sin la necesidad de que se visualice en pantalla (para evitar que alguien pueda estar mirando) y que, además, el portapapeles se limpie automáticamente al cabo de una cantidad de tiempo determinada. Estos mecanismos de seguridad son muy útiles, incluso en entornos donde la confidencialidad de la información manejada sea alta y los requisitos de protección estrictos.

Los gestores también permiten manejar distintas bases de datos de contraseñas, cada una accesible con su propia clave maestra configurada individualmente, separada de las demás. Es importante hacer copias de seguridad de cada base de datos en caso de un eventual incidente con el sistema, algo que –en general– puede hacerse desde el mismo programa.

Al ser gratuitos, los servicios no se responsabilizan si perdemos nuestras contraseñas o nos hackean, por lo que –la mayoría de las veces– no puede hacerse nada al respecto.

Constantemente me contactan desconocidos por redes sociales o distintos medios para que los ayude a «hackear algo». Muchas veces es para hacer algo ilegal, para lo cual ni respondo o me limito a explicarles que lo que solicitan es ilegal y que no hago ese tipo de

cosas. Muchas consultas están relacionadas a la obtención de acceso a su propia cuenta de correo electrónico, Instagram, etcétera, porque se han olvidado la contraseña o alguien les hackeó la cuenta luego de robarle la clave. Es muy importante proteger las contraseñas, porque si la perdemos no podremos recuperarla y perderemos la cuenta para siempre junto con la información que tengamos en ese servicio.

Doble autenticación

Dado que las contraseñas constituyen el factor de autenticación más difundido, en caso de que se quiera realizar una acción de verificación más segura es necesario agregar otra forma para que el sistema nos reconozca como usuarios válidos. Esto se realiza por medio de un nuevo factor de autenticación que, en el caso de ser el segundo, implica lo que se llama «doble autenticación», «autentificación de dos factores» o «autenticación o verificación de dos pasos».

Para realizar esta acción, es necesario proveerle al sistema un elemento que le permita constatar que uno es quien dice ser. Para esto existen distintos elementos que se dividen en tres categorías: algo que uno sabe, algo que uno tiene y algo que uno es. El primero es el caso de las claves o contraseñas y todo tipo de pin o código de autenticación. El segundo se refiere a los elementos físicos que sirven para validarse frente a un sistema, por ejemplo, las tarjetas de coordenadas que proveen los bancos para utilizar en los sistemas de *homebanking* o las tarjetas de proximidad utilizadas para ingresar a oficinas, al igual que las tarjetas de banda magnética como las de crédito, entre otros tipos de elementos físicos. El último caso se refiere a los sistemas biométricos, que implican que se debe presentar ante un dispositivo una parte del cuerpo, puede ser la huella digital, la palma de la mano o nuestro rostro, para que se decida sobre el acceso.

En el mundo de la tecnología, lo que se utiliza normalmente es un factor adicional que está compuesto por un valor generalmente numérico (código) que el sistema nos provee por un medio alternativo, como el teléfono celular o el correo electrónico. Al ingresar este código en el sistema, se interpreta que solo una

persona podría haber sido la que lo reciba (en su e-mail o teléfono vía SMS), validando así que esa persona, además de ser quien dice ser en función de que la contraseña ingresada es correcta, también lo es en función de que el código recibido es el indicado.

Utilizar este procedimiento de autenticación de doble verificación cada vez que ingresamos a un sistema sería poco práctico y bastante incómodo, por lo que se emplea principalmente para verificar la identidad en situaciones especiales, como puede suceder cuando el servicio (Facebook, Gmail, X o cualquiera que ofrezca esta característica) sospecha que la persona que está intentando ingresar no es el usuario real. Esto podría identificarlo a través de varios métodos:

- Si se detecta que la conexión desde la que se realiza el acceso no es la habitual del usuario.
- Si se detecta que el navegador desde el que se realiza el acceso no es el normal del usuario.
- Si se detecta que el equipo (notebook, computadora, tablet o teléfono) desde el que se realiza el acceso no es el normal del usuario.

Esto es técnicamente posible porque tales servicios almacenan mucha información cada vez que accedemos a ellos y, por lo tanto, pueden sacar conclusiones al correlacionar datos de todas las veces anteriores que accedimos.

Es decir, si lo pensamos paso a paso, sería de la siguiente forma:

El sistema detecta un intento de acceso o acceso dudoso (lo que podría tratarse de un posible atacante que ingresó o quiere ingresar a nuestro servicio).

1. El sistema nos envía un código de verificación a nuestro correo electrónico o teléfono celular a través de SMS.

2.Si quien desea acceder es otro y no nosotros, nunca recibirá el código que fue enviado, a menos que haya también accedido previamente a nuestra cuenta de correo o tenga en su poder nuestro teléfono celular, según sea el caso.

3. Esta situación de verificación forzada de parte del sistema puede ocurrir cuando instalamos un equipo nuevo, cuando cambiamos de navegador o de dispositivo móvil, o bien cuando estamos de viaje y nos conectamos desde una ubicación muy distinta a la habitual. Por lo tanto, es posible que el sistema nos esté alertando de una acción sospechosa que en realidad no es tal, y solo deberemos verificar que se trata de nosotros mismos intentando realizar el acceso.

Este tipo de sistema de doble autenticación debe existir en el servicio en cuestión, y como no viene habilitado por defecto, debemos activarlo explícitamente si queremos contar con esta protección adicional. Para lograrlo, nos pedirá una dirección de e-mail adicional o un número de teléfono celular para el envío de mensajes de texto (también existe la opción de que se realice automáticamente una llamada que nos dicte el código), y luego validará esta información para asegurarse que sea correcta, ya que, si cometemos un error, podemos perder el acceso a la cuenta que intentamos proteger.

Algunos servicios, como Google, Facebook y Outlook, proveen una aplicación para dispositivos móviles (o una función dentro de la propia aplicación) que genera códigos de autenticación cuando son solicitados, lo que facilita el procedimiento. Al existir la posibilidad de que, en algún momento, el usuario no cuente con una conexión a internet ni esté conectado a una red de telefonía celular, también es posible generar una lista de códigos de verificación que pueden ser impresos y guardados en un lugar seguro para el caso en que sea necesario, como durante un viaje.

Otro caso típico es, como ya mencionamos, el de los bancos. Estos, por cuestiones de seguridad, facilitan una tarjeta de coordenadas que permite validar determinadas transacciones del usuario para evitar que las realice alguien que haya robado su contraseña de acceso. Si bien no es obligatoria en muchos casos, es recomendable habilitar esta funcionalidad.

Otra forma de validación de los bancos es proveer a los clientes lo que se denomina un «token criptográfico». Se trata de un dispositivo electrónico que, por medio de un visor digital, al presionar un botón muestra números que conforman el código de verificación mencionado anteriormente.

En líneas generales, el uso de un segundo factor de autenticación es muy recomendable, especialmente en servicios en los que se maneja información confidencial, como aquellos que incluyen operaciones monetarias o datos personales sensibles. Si bien no todos los servicios ofrecen la posibilidad de tener este tipo de acceso, es probable que en un futuro sea cada vez más común encontrarlos, dada su gran utilidad en la prevención del fraude, el robo de cuentas y de identidad digital.

Importante recordar

- No es recomendable compartir las contraseñas con otras personas. En caso de necesitar brindarla de manera urgente por necesidad, debe ser modificada luego para evitar problemas futuros.
- Debemos tener certeza de que las contraseñas que utilizamos sean seguras. Esto significa que deben ser complejas y no estar formadas por datos personales directos. De ser posible, hay que incluir letras mayúsculas, minúsculas, números y caracteres especiales.
- Tienen que ser difíciles de adivinar.
- Es bueno tener un método propio de elección de contraseñas, sabiendo qué números o letras evitar (por asociación directa con uno mismo) y qué caracteres incluir para aumentar su complejidad.
- Utilizar alguna regla mnemotécnica para recordar las contraseñas, como las primeras letras de una frase, o bien tener algún criterio de elección que permita tener claves complejas de fácil memorización.
- Evitar utilizar la misma contraseña en sistemas o servicios distintos, ya que si una de ellas es comprometida podría ser utilizada para acceder a todos los sistemas en los que utilizamos la misma contraseña.
- Seleccionar con cuidado las preguntas de seguridad y sus respuestas debido a que –si son fáciles de responder– alguien

con esa información podría contestarlas y conseguir acceso a nuestras cuentas.

- Es una buena idea utilizar un gestor de contraseñas en caso de que se deba manejar una cantidad considerable de servicios distintos o si resulta difícil memorizarlas.
- No debe anotarse las contraseñas en papeles, libretas o anotadores y tampoco en archivos de la computadora o el celular. Si bien esto puede resultar cómodo, también introduce riesgos innecesarios. En caso de anotarlas, se debe guardar el papel en un lugar muy seguro.
- Cuidar que nadie esté observándonos al momento de escribir las contraseñas en el teclado. Si en alguna ocasión estamos rodeados constantemente de gente, debemos tener cuidado de no resultar demasiado obvios al ingresarla.
- Recordar que es útil cambiar las contraseñas de tanto en tanto, según el uso que se le dé al servicio y el tipo del que se trate. Es bueno hacerlo incluso sin esperar que el sistema nos obligue.
- En caso de que detectemos actividades extrañas en nuestras cuentas de cualquier tipo de servicio, la contraseña debe cambiarse de forma urgente para evitar que siga siendo utilizada por otra persona.
- Habilitar el sistema de segundo factor de autenticación siempre que sea posible para reducir el riesgo de robo de cuentas y el fraude bancario.
- No enviar jamás una contraseña por correo electrónico ni mensaje de texto (SMS), sea cual fuere el motivo por el cual se la solicita.

- Siempre cambiar las contraseñas que vienen por defecto en los dispositivos de red (routers inalámbricos, switches y demás), dispositivos electrónicos en general, software y servicios online, ya que estos serían conocidos por un potencial atacante.

Capítulo 4

Protegiendo teléfonos celulares y otros dispositivos móviles

Los teléfonos móviles modernos cuentan con una gran cantidad de avanzadas funcionalidades que exceden nuestras necesidades de comunicación tradicional, y se han transformado en un centro neurálgico de interconexión con el mundo, especialmente a través de las redes de datos que permiten conectarse a internet. Esto trae consigo nuevos riesgos a considerar en cuanto a nuestra privacidad y seguridad.

Características y usos posibles

Los teléfonos celulares modernos cuentan con capacidades que hace tan solo unos años hubieran sido inimaginables. Si bien los usos básicos (telefonía y mensajes de texto) se mantienen –aunque cada vez se utilizan menos–, se han sumado muchas funciones. Esto fue promovido principalmente por los avances tecnológicos de la última década, entre los cuales se encuentran el aumento de la velocidad de las redes de telecomunicaciones y la miniaturización de los componentes electrónicos, que llevaron a las altas velocidades de procesamiento y transmisión de datos.

Un teléfono inteligente (o smartphone) puede típicamente ser controlado tocando la pantalla (o *touch screen*) y accediendo al sistema de forma táctil. Esto facilita el uso y hace que sea más intuitivo, especialmente para los niños, quienes tienden a esperar que los dispositivos tengan alguna clase de interacción directa. Si bien algunas personas siguen prefiriendo el uso de botones y pequeños teclados físicos, la tendencia hacia lo táctil va en aumento y ya casi no son comunes los teléfonos con teclado.

Desde un smartphone es posible escuchar música, reproducir películas, ver y sacar fotos en alta resolución, grabar videos o conectarse a internet, como si se tratara de una computadora de escritorio, para utilizar las redes sociales, como Facebook, X u otras, y los servicios o sistemas de mensajería instantánea, como WhatsApp, Telegram o Snapchat. También se pueden utilizar todos los servicios de correo electrónico conocidos, tales como Outlook, Gmail o Yahoo. Un dispositivo móvil moderno, además, permite visualizar todo tipo de archivos, que pueden ser almacenados en el dispositivo o en la nube, y, como si fuera poco, existen videojuegos exclusivos con características y efectos visuales extraordinarios.

Todo esto sin contar los innumerables programas que existen para descargar e instalar –muchos de ellos, de forma gratuita– que permiten realizar multiplicidad de tareas relacionadas con la productividad, la educación, el ocio y el entretenimiento.

Vale destacar también la posibilidad que tienen los dispositivos modernos de conectarse a redes y otros aparatos en forma inalámbrica (wifi, bluetooth, etcétera), además de las redes de datos del proveedor de servicios de telefonía y la función de GPS, que permite conocer la ubicación geográfica del dispositivo en cualquier parte del mundo para ser visualizada luego en un mapa con enorme nivel de detalles.

Finalmente, es importante mencionar que todas estas características modernas nos hacen muy dependientes de nuestros dispositivos y eso se refleja en la imposibilidad de estar alejados por mucho tiempo del teléfono móvil, en la necesidad de prestar atención todo el tiempo a las cosas que ocurren cuando recibimos una notificación y, por supuesto, la sensación de desamparo que sufrimos cuando tenemos un problema con el aparato por mal funcionamiento, robo, pérdida o falta de batería.

Cuando perdemos acceso a nuestro teléfono móvil por cualquier motivo, como los anteriormente mencionados, caemos en la cuenta de lo dependiente que somos de su uso por todos los problemas que nos ocasiona. Justamente por esto es muy importante aprender a protegerlos de manera apropiada y usarlos de forma segura para no sufrir las consecuencias.

Importancia de la protección

La responsabilidad que delegamos en nuestros teléfonos u otros dispositivos móviles es enorme, y muchas veces el cuidado que le damos no está a la altura de esa responsabilidad, lo cual deberíamos tomar en consideración para reducir los riesgos de su uso natural.

Es importante proteger apropiadamente cualquier dispositivo que contenga nuestra información; por ello, mucho de lo tratado aquí aplica tanto a teléfonos como a dispositivos móviles en general (tablets, relojes inteligentes, etcétera).

Imaginemos por un momento que una persona malintencionada toma control de nuestro dispositivo móvil (por hackeo, robo, hurto, pérdida o lo que sea). Esta persona podría acceder a todas nuestras redes sociales, cuentas de correo electrónico, *homebanking*, sitios de compras y otras aplicaciones con información sensible, y comenzar a utilizarlas como si fuera nosotros mismos. Tal situación podría no ser detectada en un primer momento por nuestros contactos, quienes leerían todo como si se tratara de nosotros, y pudiendo, a su vez, ser víctimas del mismo atacante. Esta terrible situación nos ubicaría en una posición de absoluta impotencia, además del trabajo que nos costaría avisarles a todos los contactos que no somos nosotros los que estamos operando desde las cuentas. En muchas ocasiones esto no tiene vuelta atrás, por lo que deberíamos sacar nuevas cuentas para continuar utilizando los servicios en cuestión.

En este mismo sentido, es fundamental cuidar el material multimedia (fotos, audios y videos) que producimos con el dispositivo y que allí se almacena, ya que en muchos casos puede tratarse de contenidos de carácter privado o sensible (ceremonias

religiosas, grabaciones íntimas, situaciones confidenciales, y más). Lo recomendable para estas situaciones es pasar los contenidos privados o sensibles (o simplemente aquello que no queremos que se conozca) a un equipo más seguro, como una computadora de escritorio o almacenamiento externo, de modo que, de perder el dispositivo móvil y que nos roben los archivos, no existan contenidos privados entre los almacenados en el dispositivo.

También es una buena práctica revisar de vez en cuando los archivos antiguos, ya que muchas veces generamos material que no recordamos dada la facilidad de hacerlo con los modernos dispositivos. Por seguridad –y también para ahorrar espacio de almacenamiento– es recomendable borrar todos los contenidos que no utilizamos, los antiguos, como mensajes de texto, imágenes, audios, videos, e-mails y archivos en general. Las aplicaciones que utilizamos en el celular guardan muchos datos que no son necesarios y pueden ser borrados regularmente.

Cuidados físicos de los aparatos

El cuidado físico de los dispositivos móviles es uno de los temas más relevantes a la hora de proteger nuestros datos, ya que un potencial robo o daño del equipo podría hacer que perdamos el acceso a todo su contenido. Para evitar esto debemos tomar una serie de medidas de protección y cuidado, comenzando por el aspecto más obvio: evitar roturas.

Cada día es más común escuchar que a alguien se le rompió la pantalla del teléfono móvil o tablet, o que se le cayó y al golpearse no volvió a encender. Esto responde al poco cuidado que solemos tener para con lo que se convierte en algo de uso cotidiano, tanto que en ocasiones lo naturalizamos como si fuera parte de nuestro cuerpo.

Para proteger el dispositivo es conveniente contar con dos elementos: el protector para la pantalla y la funda o protector de carcasa. El primero permite que no se produzcan rayones y evita –hasta cierto punto– que el cristal se astille por un golpe y provoque el efecto de rotura ramificada típico de los vidrios que se agrietan.

Existen protectores de distintas calidades y tipos, que van desde el resguardo contra raspaduras hasta materiales especiales que pueden absorber un golpe y evitar el impacto sobre el cristal. Por otro lado, tenemos las fundas o protecciones de carcasa que, así como limitan la suciedad, también contribuyen a evitar que los golpes dañen el aparato, además de mantenerlos a salvo del desgaste normal que sufren los equipos por el propio uso. Si bien ambos entran en la categoría de accesorios para celulares, conviene contar con ambas medidas de protección.

Otra precaución que debe tenerse en cuenta es el hecho de que el dispositivo no se moje, ya que eso puede dañar los circuitos

electrónicos. Peor podría ser si en lugar de agua es algún otro tipo de líquido con propiedades abrasivas, como lo son las bebidas gaseosas de cola o el café. Si bien las fundas pueden ayudar a mitigar este inconveniente, no suele ser suficiente. Algunos equipos, de hecho, son resistentes al agua, es decir, pueden ser mojados, pero no sumergidos (como en una pileta), ya que no soportan la presión que ejerce el líquido bajo la superficie, aunque existen otros que sí lo hacen.

Cuidado de la privacidad en el uso

Al utilizar los dispositivos móviles con un sinfín de aplicaciones y en distintos lugares, como el trabajo, el subte o el colectivo, esperando en el médico, en una reunión social, etcétera, nos vemos expuestos a que personas que se encuentren cerca nuestro puedan ver lo que estamos haciendo con nuestro dispositivo, que puede ser desde ver un video privado hasta leer o escribir un correo electrónico o mensaje confidencial.

Es importante proteger nuestra privacidad y evitar las miradas indiscretas; para ello existen unos filtros de privacidad especiales para las pantallas de los dispositivos móviles que, además de protegerlas contra ralladuras y golpes, impiden que el contenido que muestran sea visible desde los costados; es decir, solo la persona que está usando el dispositivo y lo tiene enfrente puede ver el contenido reproducido por la pantalla y no quienes estén alrededor.

Otro aspecto de la privacidad en el uso de dispositivos móviles son las notificaciones. Estas son mensajes que se muestran en la pantalla del dispositivo ante determinados eventos, desde un simple mensaje de texto, de WhatsApp o correo electrónico, hasta algo que un contacto comparta en Facebook o una solicitud de amistad, etcétera. Todo ello nos llega en forma de notificación cuando no estamos utilizando dicha aplicación.

Las notificaciones son un mecanismo útil; el problema es que a veces muestran demasiada información cuando no estamos usando el dispositivo, haciendo que la pantalla se encienda y las muestre, incluso cuando el dispositivo está protegido/bloqueado. El riesgo con las notificaciones es que pueden contener información sensible o confidencial y ser vistas por cualquier persona que se encuentre cerca del aparato. Tal es el caso si dejamos nuestro dispositivo

móvil sobre una mesa y, al alejarnos, nos llega una notificación; la pantalla, entonces, se encenderá y reflejará su contenido, que puede ser leído por alguien que esté cerca.

El riesgo es mayor cuando recibimos un mensaje confidencial; por ejemplo, para recuperar una contraseña que nos olvidamos es común que algunos sitios nos envíen un mensaje de texto o e-mail con un código que deberemos ingresar para poder acceder sin la contraseña.

Un hacker malintencionado que quisiera acceder a alguna de nuestras cuentas (correo, Facebook, Instagram, etcétera) podría hacerse pasar por nosotros y pedir recuperar una contraseña en el momento que tiene a la vista nuestro teléfono móvil. De esta forma, cuando llegue la notificación del mensaje de texto o e-mail, podrá ver el código en la pantalla del teléfono y luego utilizarlo para acceder a nuestra cuenta.

Para prevenir estos tipos de ataques podemos –además de usar un filtro de privacidad– configurar el dispositivo para que no muestre demasiada información en las notificaciones cuando el teléfono no está desbloqueado, o sea, que sea necesario introducir código, contraseña y demás para poder ver el detalle de la notificación. Esto debe establecerse en cada aplicación o a nivel general en la sección de configuración de las notificaciones del dispositivo.

Carga segura del dispositivo

La mayoría de los dispositivos móviles se cargan mediante un cable por conexión USB, lo que permite al mismo tiempo sincronizarse o copiar información desde y hacia una computadora. Si bien esto es muy útil, presenta un riesgo importante cuando lo hacemos en alguna terminal de carga, ya sea un aeropuerto, terminal de ómnibus, evento, etcétera. El riesgo se debe a que la terminal puede haber sido manipulada en forma maliciosa y, aprovechando la funcionalidad de copia de datos, cuando conectemos nuestro dispositivo se nos robe la información que este contiene o nos instale algún malware. Para protegerse contra esto, es importante no conectar nuestro dispositivo por USB en lugares poco confiables o, de hacerlo, utilizar un adaptador especial, conocido como condón USB, que no permita la copia de datos. Otra opción práctica y más segura es recurrir a baterías portátiles para cargar nuestros dispositivos, lo que evitará conectarlos en cualquier lado.

Algunos dispositivos poseen la opción de conectarse en modo «solo carga» para evitar la copia/sincronización de datos; es necesario utilizar tal opción para prevenir el robo de datos al conectar el dispositivo en lugares desconocidos. Hay que tener la misma precaución al vincularlo a computadoras de terceros.

Protecciones ante robo o pérdida

El robo o hurto del dispositivo móvil es un problema que afecta con frecuencia a los usuarios, y es por eso que –más allá de tomar las medidas adecuadas para que eso no nos suceda– debemos también considerar qué haríamos en caso de que indefectiblemente dicha situación ocurra. También podría acontecer la pérdida del aparato, lo cual no es menos peligroso ya que, en definitiva, perderíamos el acceso a nuestra información y al dispositivo físico.

En los casos mencionados existen dos cuestiones a considerar; la primera es que otra persona tenga acceso a nuestra información, lo que podríamos evitar activando el bloqueo del dispositivo, permitiendo que solo pueda ser utilizado si se lo desbloqueara por medio de un pin numérico, código, contraseña, patrón (dibujo de líneas en la pantalla), nuestra huella digital o fisonomía (disponible en los dispositivos más modernos). Esto evita que nadie –que no seamos nosotros– pueda acceder a las aplicaciones y archivos que se encuentran en el dispositivo, a excepción de todo aquello (archivos de distintos tipos) que esté almacenado en tarjetas de memoria externas, que pueden ser removidas y colocadas en un lector para su acceso fuera del aparato. Ante estas recomendaciones, lo conveniente es el cifrado de datos en caso de que estos sean confidenciales; para ello se debe activar la encriptación de la memoria externa desde las opciones de seguridad del dispositivo.

En los dispositivos más modernos, una vez que se activa la funcionalidad de bloqueo, también se acciona automáticamente la encriptación de toda la información, lo que aumenta considerablemente la seguridad de nuestros datos. De no activarse

automáticamente la encriptación, se deberá hacerlo a través de la configuración de seguridad del dispositivo.

En cualquier dispositivo móvil es importante activar el autobloqueo; esta funcionalidad permite que, si dejamos de utilizar el aparato por un tiempo determinado, se bloqueará automáticamente, por lo que luego será necesario desbloquearlo con el código, contraseña y demás. El autobloqueo puede configurarse, por ejemplo, de tal modo que, si pasan diez segundos sin que el dispositivo se utilice, se bloquee, protegiéndose así el acceso de terceros en caso de habernos descuidado.

Además de proteger el ingreso al dispositivo móvil con un código/pin de acceso o contraseña, en los dispositivos de telefonía celular (teléfonos y algunas tablets también) es sumamente importante, además, proteger la tarjeta SIM con un código/pin de acceso. Esta es un chip inteligente que nos da el proveedor de telefonía celular y que permite el uso de la línea telefónica, ya sea para voz, SMS o datos.

¿Por qué es importante, entonces, proteger la tarjeta SIM? Porque puede ser extraída de un dispositivo móvil y colocada en otro para poder utilizar los servicios de telefonía celular, así como también acceder a los datos que contenga la tarjeta, como información de contactos y de nuestro servicio de telefonía móvil. También permite el uso de algunas aplicaciones, como WhatsApp, que utilizan nuestro número telefónico como autenticación; esto quiere decir que si nos roban el teléfono pueden ingresar a nuestra cuenta de WhatsApp sin problemas si la tarjeta SIM no está protegida. Por otra parte, que alguien tenga acceso a nuestro servicio telefónico le permitirá recibir mensajes de SMS enviados a nuestro número con códigos para recuperar contraseñas y obtener así la posibilidad de ingresar a las cuentas de los distintos servicios de internet que utilizamos. Afortunadamente, algunos nuevos

teléfonos ya vienen con eSIM (*embedded SIM*), que es una tarjeta SIM que ya viene integrada con el dispositivo y no se puede extraer; de esta forma estamos más protegidos sin necesidad de configurarle un código/pin de acceso.

En caso de robo y extravío, la funcionalidad de GPS del dispositivo móvil es muy útil, ya que es posible detectar su posición geográfica con mayor o menor precisión, según sea el caso, si previamente instalamos un software de rastreo (de no venir ya instalado en el dispositivo). Este tipo de aplicaciones nos permite visualizar en un mapa la posición aproximada del equipo desde un sitio web al que accederemos con nuestra cuenta. En efecto, no es necesario que el móvil se extravíe o nos lo roben para comprobarlo; de hecho, es conveniente hacer la prueba para saber cómo se utiliza la función.

Si nuestro teléfono tiene habilitado la geolocalización, la precisión de la ubicación será buena, en tanto, si no lo está, intentará ser ubicado por algún otro medio, como la estimación de la zona por red wifi o bluetooth (incluso es técnicamente posible hacerlo por las propias antenas de la empresa de telefonía). Vale mencionar que puede realizarse la activación remota del GPS dependiendo de la funcionalidad del software de rastreo. Para poder hacerlo correctamente, el dispositivo deberá estar conectado a internet. Por lo general, tales aparatos ya traen aplicaciones con funcionalidad de rastreo que tienen nombres como «Encontrar mi dispositivo» o «Encontrar mi móvil», y en las que pueden configurarse distintas opciones de rastreo ante un eventual robo o pérdida.

Frente una emergencia también es posible –mediante el mismo software de rastreo– realizar un borrado completo del dispositivo en forma remota, o bien bloquearlo de manera especial para que nunca pueda ser utilizado, por más que el dispositivo sea borrado hasta que este bloqueo sea desactivado. Un ejemplo de esto sería

accionar el modo «perdido», que solo muestra nuestra información de contacto por si alguien lo encuentra. Esto logrará, al menos, que nuestros datos no queden accesibles para cualquier persona y que el dispositivo no pueda ser utilizado.

De todas maneras, debemos tener en cuenta que, en caso de tratarse de robos comunes, los delincuentes suelen apagar el teléfono inmediatamente para evitar cualquier tipo de acción que procure recuperarlo; aunque a veces suelen encenderlo nuevamente y conectarlo a internet para intentar desbloquearlo.

Por último, es útil tener anotado el número de serie del dispositivo de manera que, de realizar una denuncia policial por robo o extravío, podamos brindar esta información para identificarlo fácilmente y recuperarlo.

A veces las personas que roban o encuentran los dispositivos cometen errores que hacen que podamos recuperarlos más fácilmente. Este fue el caso de lo ocurrido a un amigo que perdió su teléfono móvil y no sabía dónde estaba. Preguntó en aquellos ámbitos donde había estado recientemente y nadie lo había encontrado, lo cual le pareció muy raro, ya que había frecuentado solo un par de lugares.

Por suerte tenía configurado su teléfono para que guardara automáticamente las fotos y videos en la nube en su cuenta de Google Drive. A los pocos días de haberlo perdido, accedió a su cuenta de Google Drive y, para su sorpresa, vio que había fotos nuevas, en las que se evidenciaba que habían sido tomadas por un conocido suyo: un empleado de un comercio donde había estado el día en que perdió el teléfono. Mi amigo, entonces, se dirigió al comercio, habló con el dueño y le mostró lo sucedido. Por supuesto, pudo recuperar lo suyo.

***

No todas las historias tienen final feliz. A un familiar mío, llamémosle José, mientras estaba de viaje, le robaron su teléfono celular. Era un iPhone, por lo que le significó una pérdida económica importante.

Por lo general, la pérdida de un dispositivo electrónico –un teléfono celular en este caso– no es lo más importante, sino los datos que allí almacenamos, pudiendo tratarse de información confidencial y privada. Por suerte, el teléfono tenía configurado un código de bloqueo que, si no se ingresa, es imposible usarlo. Por otra parte, José procedió a reportarlo como perdido inmediatamente, utilizando la funcionalidad brindada por Apple (fabricante del dispositivo), lo cual hace que quien haya obtenido el teléfono, para utilizarlo, necesite indefectiblemente especificar el usuario y contraseña de iCloud (servicio de Apple) de José, en este caso. Si bien con estas medidas parecía que los datos y privacidad de José estaban protegidos, no resultó suficiente.

Al comunicarse con otro amigo y contarle lo ocurrido con su celular, este le dijo que le había parecido extraño que no le contestara unos mensajes de WhatsApp y que estos le figuraban como recibidos y leídos. Esto le generó muchas dudas a José, ya que era raro que eso sucediera estando bloqueado el teléfono. Luego de investigar un poco, se dio cuenta de que quienes habían robado el teléfono habían puesto la tarjeta SIM en otro dispositivo y le estaban viendo los mensajes de WhatsApp que le llegaban, y también podrían contestar y enviar mensajes si así lo quisieran. Esto puso muy nervioso a José, y se dio cuenta de que le había faltado avisarle a su compañía de telefonía celular que bloqueara el uso de su tarjeta SIM –o sea, su línea telefónica– hasta que pudiera obtener otra y un teléfono nuevo. Pero aun luego de realizar ese trámite ¡detectó que continuaban usando su WhatsApp! Esto se debió a que, antes de gestionar el bloqueo de la línea, los delincuentes habían activado esa aplicación de mensajería desde otro equipo, que también funciona por conexión wifi sin necesidad de que la línea telefónica se encuentre habilitada. Tras una serie de averiguaciones, descubrió que, para evitar que le siguieran utilizando su WhatsApp, debía enviar un correo electrónico a una dirección de este servicio de mensajería, especificando su número de teléfono y solicitando que bloquearan el acceso. Por supuesto, para que su pedido fuera procesado debió esperar varios días; luego de su viaje solicitó una nueva tarjeta SIM, restauró su línea telefónica en otro equipo y volvió a tomar el control de su WhatsApp.

Después de tantos problemas y trámites, lamentablemente la pesadilla no terminó allí. A los pocos días, mi amigo recibió un mensaje de texto (SMS) que decía: «Tu iPhone ha sido encontrado a las 3:19 AM. Ver localización enlace movil-gps-sys.com/?x=apZr2 Soporte Apple». Tal mensaje le pareció raro, ya que, cuando reportó como perdido su equipo, le habían dicho que podía recibir una notificación por e-mail si el teléfono era encendido y utilizado, pero no un mensaje de texto.

Al hacer clic en el enlace, se accedía a un sitio que parecía de Apple y desde el cual se le solicitaba ingresar su usuario y contraseña para poder obtener la información. Por suerte, José siempre ha escuchado mis consejos y se dio cuenta de que podía ser un engaño. En efecto, los delincuentes –al no poder utilizar el teléfono por estar bloqueado– habían recurrido a esta artimaña por mensaje de texto para obtener su usuario y contraseña.

Instalación segura de aplicaciones

La cantidad de aplicaciones para teléfonos móviles crece a diario de forma muy rápida, a un ritmo que hace que sea difícil para las tiendas oficiales de descarga determinar si todo el nuevo software está libre de virus y programas maliciosos, o si se trata de alguna clase de engaño para el usuario. Esto hace que las personas malintencionadas aprovechen para intentar subir apps propias con la intención de que sean descargadas por los usuarios.

Si bien las tiendas App Store (dispositivos iOS) y Google Play Store (dispositivos Android) cuentan con diferentes características de seguridad y formas de validar las aplicaciones para evitar que las maliciosas puedan ser distribuidas, a veces fallan en detectarlas. De todas maneras, las tiendas oficiales son las más confiables para instalarlas y no debemos confiar en otras fuentes, ya que, al descargar software de otros sitios, aumentamos el riesgo de terminar descargando software perjudicial sin saberlo.

Las aplicaciones pueden ser maliciosas en sí mismas o bien tener alguna clase de efecto secundario maligno que no se note de manera directa al ser utilizada. Para causar un efecto dañino, usualmente estas apps solicitan una gran cantidad de permisos innecesarios en el sistema, lo cual es un indicador de su potencial peligro. Esto no es fácil de determinar, pero sí podemos emplear el sentido común. Por ejemplo, difícilmente una aplicación para editar fotos tendría necesidad de acceder a la funcionalidad de realizar llamadas o enviar mensajes; o una aplicación para ver archivos de texto no requerir acceso a la cámara de fotos.

La reputación de las aplicaciones es un indicador importante de su confiabilidad, ya que la valoración que dan los usuarios supone que la han probado y utilizado, por lo tanto, sus comentarios podrían

evitarnos muchos problemas. Si una app se comporta de manera sospechosa, los usuarios más experimentados pueden notarlo y colaborar así con el resto de la comunidad reportándolo a través de sus comentarios.

En general, debemos evitar instalar cualquier aplicación desconocida o que no esté disponible en las tiendas oficiales, impidiendo de esta forma posibles problemas. Las de mala calidad también pueden causar problemas en nuestros dispositivos, haciendo que funcione con mayor lentitud, que consuma más datos, que pierda información, etcétera. Las aplicaciones conocidas y confiables son más estables y de mejor calidad, ya que tienen un proceso de desarrollo profesional y son probadas exhaustivamente alcanzando un mejor funcionamiento en general.

Actualización de aplicaciones y sistema operativo

Como todo software, el sistema operativo y las aplicaciones de los dispositivos móviles también pueden ser actualizados.

Las actualizaciones permiten que se corrijan problemas de seguridad en el software y mejoren sus funcionalidades en todo sentido. Si bien ambos aspectos son importantes, el que mayormente puede afectarnos es el relacionado a cuestiones de seguridad.

Actualmente, dada la cantidad de aplicaciones que tenemos en los teléfonos, es posible que periódicamente (a veces incluso en cuestión de días) recibamos alertas de actualizaciones disponibles y, aunque esto puede resultar incómodo, es recomendable que siempre se realice ni bien se pueda. Lo aconsejable en estos casos es utilizar una conexión wifi para evitar que las descargas consuman datos móviles.

Las actualizaciones de seguridad evitan que un potencial atacante pueda aprovecharse de las fallas de seguridad que se hayan encontrado en aquellas versiones de las aplicaciones que se reemplazarán o corregirán en la correspondiente actualización. Al tener el software renovado, estamos reduciendo el riesgo de ser atacados por hackers maliciosos o afectados por malware y otros programas dañinos.

En cuanto a los sistemas operativos, el fabricante del dispositivo, por lo general, mantiene la gestión de actualizaciones y las pone a disposición de los usuarios cuando lo considera apropiado. Apple controla el hardware y software de sus dispositivos, a diferencia de otros fabricantes que utilizan sistemas Android, el cual es desarrollado mayormente por Google. En estos casos, los usuarios

deciden si incorporan o no las nuevas versiones de software que van apareciendo en la distribución oficial de Android de Google.

La actualización del sistema operativo es, por lejos, la que más puede afectar el uso y la compatibilidad del resto de las aplicaciones, pero también suele ser aquella que los dispositivos móviles realizan de forma más controlada y segura. Por su parte, las aplicaciones comunes se instalan, actualizan y desinstalan por voluntad del usuario, por lo que a veces son esas elecciones las que ponen en riesgo al sistema.

En cualquier caso, tener versiones más actualizadas de los productos es una de las grandes ventajas que nos da el software, y desaprovecharlas por falta de conocimiento o negligencia puede implicar someter a riesgos innecesarios a nuestros dispositivos e información. En resumen, siempre debemos actualizar el software, aunque resulte molesto.

Desprotección del dispositivo

Una de las cosas que los usuarios más experimentados y con conocimientos técnicos hacen con su dispositivo es la desprotección, que se denomina comúnmente *rooting* (en sistemas Android) o *jailbreaking* (en sistemas de Apple), términos que refieren al proceso que permite eliminar las limitaciones que el fabricante incluye en los equipos. Esto se realiza con el objeto de conseguir acceso total e irrestricto al sistema operativo y a sus funcionalidades. Cabe aclarar que también, en muchos casos, es posible restablecer el dispositivo a su estado original, aunque no siempre es así.

La desprotección permite, entre otras ventajas, mejorar el rendimiento, quitar software del operador de telefonía celular o del fabricante, cambiar la versión del sistema operativo, instalar aplicaciones especiales que requieren privilegios superiores al usuario común, instalar ciertas aplicaciones pagas de forma gratuita, reemplazar aplicaciones del sistema, cambiar configuraciones, o alterar carpetas y archivos protegidos. No obstante, es necesario considerar que dichas modificaciones suelen invalidar la garantía que da el fabricante, por lo que –en caso de que posteriormente tengamos un problema con el equipo– es posible que tal garantía pierda validez al llevarlo a reparar de ser necesario. También puede que el sistema se torne inestable luego del proceso de desprotección. Adicionalmente, si el procedimiento no se realiza de manera precisa y correcta es probable que el equipo quede inservible y su reparación sea muy difícil.

Finalmente, es necesario aclarar que estas limitaciones al sistema realizadas por el fabricante ayudan a que sea posible

controlar más al software malicioso y evitar que puedan ocurrir problemas complejos en el dispositivo por un mal uso.

Como conclusión sugerimos evitar ser tentados por las ventajas de la desprotección, ya que la enorme mayoría de los usuarios no se beneficiará prácticamente en nada por esta medida, al tiempo que aumentará mucho el riesgo al que están expuestos, poniendo en peligro sus sistemas, sus dispositivos y, por lo tanto, la información.

Cuidados en las conexiones

Es importante destacar que la conexión de datos de nuestro proveedor de servicios de telefonía móvil es más segura que las conexiones wifi abiertas que puedan encontrarse en lugares públicos como cafeterías, centros comerciales, parques y plazas. Ya que la conexión de datos del proveedor de telefonía es encriptada (cifrada) –es decir, protegida– y la conexión wifi pública se comparte con todos los que se conectan, un usuario malicioso, entonces, puede interceptar nuestra información. Por este motivo, si usamos redes inalámbricas públicas debemos tratar de protegernos utilizando una VPN, como se ha mencionado anteriormente respecto a la navegación en forma segura; de esta manera, nuestra información no podrá ser interceptada ya que se encontrará protegida por encriptación.

En el caso de la conectividad con bluetooth, se recomienda mantenerla apagada si no se está utilizando para realizar una llamada con manos libres o escuchando música con auriculares inalámbricos. Esto, además de consumir más batería, podría funcionar como canal de acceso al dispositivo para un potencial atacante que quiera aprovecharse de algún problema de seguridad. Adicionalmente, como mencionamos, debemos cambiar cualquier contraseña provista por el fabricante por defecto. De manera similar, debemos evitar tener activada cualquier tipo de funcionalidad de conexión si no está siendo empleada, y cambiar también sus contraseñas predeterminadas.

Estafas por mensajes de texto

Por más que nos hayamos desacostumbrado, los teléfonos modernos siguen cumpliendo sus funciones principales, que son básicamente hablar por teléfono y enviar mensajes de texto. Estos servicios no han tenido avances tecnológicos significativos en los últimos años y están cada vez más en desuso, dado que hoy todo se orienta hacia las comunicaciones digitales por internet, tanto para servicios de voz como de mensajería instantánea. De todas formas, algunas estafas siguen aprovechando las características de la telefonía celular tradicional.

Un ejemplo de estos fraudes es cuando se recibe un SMS desde un número desconocido que dice, por ejemplo, que es un amigo o conocido con nuevo número, o que le está escribiendo por otro medio y no logra contactarse, por lo que incita al usuario a responder el mensaje. Al hacerlo, el usuario termina por darse de alta automáticamente en un servicio de suscripción a SMS Premium, que le cobrará una suma de dinero por ese envío y, tal vez luego, una suma mensual sumada al costo regular del plan de telefonía con que cuenta.

La forma de evitar este tipo de estafas es estar atentos ante cualquier mensaje sospechoso y no responder nunca por SMS a un número desconocido. Ante la duda conviene contactar por otro medio a la supuesta persona que nos escribió y corroborar con ella la veracidad de los mensajes recibidos.

También, como vimos en el relato del teléfono robado, es posible recibir enlaces a sitios web por medio de mensajes de texto con engaños para obtener nuestra información como contraseñas, tarjetas de crédito, cuentas bancarias, etcétera. Al recibir un enlace a un sitio web, lo mejor es evitar hacer clic, excepto que estemos

sumamente seguros de que lo haya enviado una fuente confiable. A veces solo cliqueando podemos comprometer la seguridad de nuestro dispositivo móvil si es que este no tiene las últimas actualizaciones de seguridad.

Copias de seguridad

La mayoría de los dispositivos móviles permiten ser conectados a una computadora para sincronizar datos y realizar copias de resguardo o seguridad (*backups*).

Es importante sincronizar y hacer copias de seguridad de nuestro dispositivo móvil regularmente para que, en caso de hackeo, robo, pérdida o rotura, nuestros datos estén a salvo y puedan ser recuperados con facilidad. Otra opción es sincronizarlo con la nube, es decir, que nuestros datos estén guardados en internet, ya sea en servicios de Google, Apple u otro proveedor, pudiendo ser recuperados fácilmente cuando sea necesario.

En caso de contar con copia de seguridad, cuando no tenemos más acceso a nuestro dispositivo por cualquier motivo, luego, al usar un nuevo dispositivo similar, podemos recuperar rápidamente todos nuestros datos e incluso la misma configuración que teníamos en el dispositivo anterior, con todas las aplicaciones y servicios.

> Un día mi teléfono iPhone se estaba quedando sin baterías, así que lo conecté para cargarlo. Luego de un tiempo, cuando quise usarlo, el teléfono no encendía, no funcionaba nada. Me pareció muy extraño que dejara de funcionar sin que nada le haya pasado, por lo que busqué respuestas y soluciones en internet.
>
> Probé decenas de posibles soluciones sin éxito y lo único factible era hacerlo revisar por un especialista. Mientras tanto, yo estaba sin celular, lo cual implica posibles problemas dependiendo del uso que uno le dé, ya que estar incomunicado puede afectar nuestra vida laboral o familiar. Por suerte pude conseguir otro iPhone similar y, al tener copia de seguridad, rápidamente recuperé todos los datos e incluso las aplicaciones y configuraciones que tenía en el teléfono.
>
> Cualquier dispositivo, independientemente de su modelo y marca, puede dejar de funcionar de un momento a otro, y si no tenemos copia de seguridad, perderemos todos

los datos que tengamos ahí guardados.

Importante recordar

- Evitar que quede almacenado de forma permanente en el teléfono cualquier tipo de imagen o video que pueda ser de contenido sensible o confidencial. Es recomendable pasar los archivos a una computadora y eliminarlos del aparato para evitar riesgos.
- Utilizar un filtro de privacidad en la pantalla del dispositivo para evitar miradas indiscretas. Configurarlo para que no muestre demasiada información en las notificaciones cuando el aparato se encuentra bloqueado o no está en uso.
- No cargar los dispositivos en cualquier lugar; de hacerlo, utilizar protección y configurarlos en modo solo carga sin que sincronice datos.
- Configurar el dispositivo para que solo pueda ser utilizando luego de introducir nuestro código, contraseña, etcétera. Configurar para autobloqueo. Habilitar la encriptación de los datos, tanto internos como los almacenados en memorias externas. Establecer código/pin en tarjeta SIM.
- Asegurarse de tener instalado en el dispositivo algún tipo de software que permita la determinación de la ubicación en caso de pérdida o robo; es decir, que pueda ser rastreado y habilite la realización de acciones, como el borrado de datos y el bloqueo del equipo en caso de ser necesario.
- Descargar aplicaciones solo desde las tiendas oficiales para tener una mayor certeza de que han atravesado un proceso de verificación de la empresa y de la comunidad de usuarios.

- Prestar atención a las opiniones y revisiones de otros usuarios antes de bajar una aplicación, ya que, en caso de tratarse de una aplicación maliciosa, probablemente se haya comentado con anterioridad. También la cantidad de descargas que tiene la aplicación puede ayudar a determinar si estamos ante un producto genuino, ya que el hecho de que una mayor cantidad de personas la hayan descargado supone un poco más de confianza.
- Observar los permisos que solicitan las aplicaciones al ser instaladas, y si consideramos que son excesivos, realizar más comprobaciones sobre su procedencia y fiabilidad. Ante la duda es mejor no proseguir y consultar con alguien que conozca o tenga más experiencia en el tema.
- Mantener las aplicaciones y el sistema operativo de los dispositivos siempre actualizados.
- Evitar realizar el *rooting* o *jailbreaking* (desprotección) del dispositivo, salvo que se trate de un usuario avanzado y lo realice con mucho cuidado considerando los riesgos.
- Desactivar wifi, bluetooth y todos los tipos de conexiones en general mientras no se estén utilizando. Esto, además de reducir el consumo de batería, limita el riesgo ante posibles canales de ataque.
- No responder SMS de números desconocidos ni llamar, así como tampoco acceder a enlaces web enviados desde orígenes desconocidos y no solicitados.
- Asimismo, no debemos confiar en promociones o avisos que comuniquen que hemos sido beneficiados con premios o regalos.

- Sincronizar el dispositivo con la computadora o la nube y realizar copias de seguridad regularmente.

Capítulo 5

Criptomonedas y blockchain

En los últimos años ha venido creciendo el uso de criptomonedas (*cryptocurrencies*) y las tecnologías relacionadas como cadena de bloques (blockchain), NFT (tokens no fungibles), contratos inteligentes (*smart contracts*), etc. Si bien todavía su uso no ha sido adoptado masivamente, cada vez se realizan más transacciones con fines de inversión, juegos, pagos, intercambio, etc.

Recientemente ha comenzado a crecer cada vez la adopción y aceptación de las criptomonedas, por lo tanto, pronto pasarán a ser de uso común; así como hoy usamos dólares o pesos, utilizaremos criptomonedas diariamente. Debido a esto es importante conocer los aspectos básicos sobre qué son, cómo se usan y principalmente saber cómo hacer un uso seguro para evitar ser víctimas de fraudes, estafas o robos.

Criptomonedas, contratos inteligentes, NFT, RWA…

Las criptomonedas son activos digitales de intercambio que utilizan encriptación para asegurar las transacciones, para controlar la creación de nuevas unidades de esa criptomoneda y para verificar las transferencias de activos. Todo esto se realiza de manera descentralizada a través de tecnología blockchain. Las más populares actualmente son bitcoin y ethereum, pero hay decenas de tecnologías y cientos de distintas criptomonedas.

El avance de esta tecnología ha permitido el desarrollo e implementación de contratos inteligentes, que, básicamente, es código de software que se ejecuta sobre un blockchain. Los contratos inteligentes consisten en reglas para realizar distintas acciones sin intermediación de un tercero, de forma segura y automática. Estas nuevas tecnologías se refieren a sistemas online descentralizados basados en tecnología blockchain y componen lo que se llama Web3.

Los NFT son criptoactivos que tienen la característica de representar activos únicos. Pueden ser cualquier cosa: música, una obra de arte, contenido digital (imágenes o texto), etc. De esta manera, un NFT puede representar digitalmente una obra de arte famosa y, por lo tanto, el poseedor de ese NFT tendrá ciertos derechos sobre la obra. Básicamente, un NFT representa un activo que puede ser físico o digital, y el poseedor de un NFT tiene derechos sobre el activo que este representa.

La representación de un activo físico o tradicional a través de tecnología cripto se llama «tokenizar», ya que se representa a través de un token digital en un blockchain. Existen también los llamados activos del mundo real, RWA (Real World Assets), que pueden incluir acciones de empresas, bonos, materias primas,

bienes raíces, etc., y que al ser tokenizados se pueden transaccionar en forma más fácil, rápida y eficiente. Al igual que los NFT, el poseedor de RWA tiene los derechos de los activos que estos representan.

Las distintas criptomonedas y otros criptoactivos, como los NFT y RWA, poseen valor que puede ser mucho, poco o nada, dependiendo del tipo de criptomoneda y el activo que representen. Por ejemplo: tanto las criptomonedas como los NFT y RWA pueden ser comprados y vendidos con dinero o con otras criptomonedas, llegando algunos a ser muy valiosos. Debido al valor que poseen, es necesario saber protegerlos debidamente para evitar su pérdida, ya sea por accidente, robo o por un hackeo.

Lamentablemente, para hacer un uso seguro de los criptoactivos se necesita conocimientos específicos sobre el tema, ya que su práctica todavía es algo compleja para un usuario regular de tecnología. Por lo tanto, aquí lo describimos de forma simple y práctica, para hacerlo de la forma más segura.

Claves privadas y criptowallets

Los criptoactivos digitales se protegen con una clave privada, que se usa para poder realizar transacciones en el blockchain y asegurarse de que solo quien la posee puede transaccionar con ellos. Es decir, si la perdemos o nos hackean, ponemos en riesgo los criptoactivos digitales y difícilmente los recuperemos.

Los criptoactivos permiten que nosotros mismos los manejemos a través de criptowallets (billeteras). Estas wallets no guardan realmente los criptoactivos digitales, sino que contienen las claves privadas que se utilizan para realizar las transacciones. Esas contraseñas son números largos, imposibles de adivinar, y, por lo tanto, no son fáciles de memorizar. Para acceder a nuestra wallet se usa una contraseña o pin elegido por nosotros mismos, que protege la wallet. Cada vez que queremos realizar una operación con un criptoactivo solo necesitaremos acceder a nuestra wallet con la contraseña o pin.

Hay dos tipos de wallets: las *hot wallets*, que son las que se guardan en un dispositivo conectado o que se conectan comúnmente a internet, y las *cold wallets*, que se guardan en un medio que nunca se conecta a internet, es decir, un medio offline. Las hot wallets son un software que se puede instalar en una computadora, teléfono celular, tablet, etc., o usar desde algún servicio en la nube. Por otro lado, las cold wallets son, generalmente, pequeños dispositivos de hardware específico que tienen un diseño muy seguro y muy difícil de hackear. Al no estar conectadas a internet, y como las claves privadas que guardan nunca salen del dispositivo, son consideradas la opción más segura para almacenarlas.

El uso de criptowallets acarrea riesgos que debemos conocer y tomar medidas para minimizarlos. El principal peligro es si perdemos el acceso por cualquier motivo. Esto puede pasar, por ejemplo, si se rompe o nos roban nuestra computadora o teléfono celular, si nos olvidamos la contraseña, se rompe o roban el dispositivo de la cold wallet, perdemos acceso al servicio en la nube, etc. Para evitar perder nuestros criptoactivos, lo que debemos hacer al momento de empezar a utilizar las wallets es crear la llamada frase de recuperación o frase semilla (*recovery phrase*, *seed phrase*), que consiste en un rango de entre 12 y 20 palabras generadas automáticamente de forma aleatoria. Entonces, con la frase de recuperación, podremos recobrar las claves privadas que teníamos. Es importante anotar esta frase y guardarla en un lugar muy seguro, como puede ser una caja de seguridad. No es recomendable guardarla en ningún dispositivo que se conecte a internet, ya que quien tenga acceso a esa frase podrá acceder a todas las claves privadas y robarnos nuestras criptomonedas, NFT, etc.

Riesgos con servicios y empresas cripto

Si operamos con algún servicio centralizado para la compraventa o custodia de criptoactivos, ese servicio manejará las claves privadas y nosotros solamente tendremos un usuario y contraseña para acceder al servicio, pero no a las wallets. Esto quiere decir que el servicio tiene control total de nuestros criptoactivos ya que son ellos quienes manejan las wallets. Podríamos compararlo con el sistema online de un banco, donde, a través del sistema, podemos realizar transacciones, pero el banco sigue teniendo guardado nuestro dinero físico y tiene el control total sobre él. El problema es que, a diferencia de los bancos, la mayoría de los servicios cripto no tiene ningún tipo de seguro contra la pérdida de los criptoactivos. Esto significa que si el servicio es hackeado o tiene algún problema y desaparecen nuestras criptomonedas, nadie se haría responsable. Es importante tenerlo presente al usar cualquiera de estos servicios, ya que podemos perder todo de un momento a otro sin tener posibilidad de reclamar nada.

Todo esto se debe a que, al ser una nueva tecnología y un nuevo negocio, hay distintas regulaciones (e incluso falta de ellas) en los países donde están basados los servicios. Esto crea vacíos legales y áreas grises en la materia. Teniendo en cuenta que muchas empresas y servicios cripto ponen en riesgo los activos de los usuarios por no tener buena seguridad o por hacer inversiones arriesgadas, incluso a veces sin decirles a los usuarios, siempre es bueno revisar los términos y condiciones del servicio para saber las responsabilidades, si tienen seguros, posibles riesgos, y cualquier información relevante para esto.

Lamentablemente, todos los años hay hackeos y pérdidas por miles de millones de dólares en criptoactivos. Cada vez existe más

dinero en este formato y los hackers maliciosos aprovechan para robar a empresas y servicios cripto y también a usuarios directamente. Siempre debemos tener esto presente y desconfiar de los servicios que utilicemos, ya que, por lo general, no van a responsabilizarse ante ningún problema. Queda en el usuario la responsabilidad de cuidar sus criptoactivos teniendo extremo cuidado con los servicios que utiliza, evitando dejar sus activos en los servicios más del tiempo necesario.

Problemas con los contratos inteligentes

Los servicios Web3 están potenciados por contratos inteligentes. Por lo general, interactuamos con ellos cuando usamos servicios Web3, donde conectamos nuestra wallet para realizar transacciones de distinto tipo como comprar o vender criptomonedas o NFT, cambiar o prestar nuestras criptomonedas a cambio del pago de un interés.

Los contratos inteligentes, al igual que cualquier software, pueden tener problemas de seguridad que sean aprovechados por hackers maliciosos para sobrepasar protecciones o robar información. Una diferencia importante con otros tipos de software es que manejan criptoactivos de mucho valor, entonces si son hackeados, se puede obtener de manera fraudulenta una gran cantidad de dinero. Ha habido muchos incidentes en que servicios Web3 han sido hackeados, y algunos o todos los criptoactivos, robados. Esto siempre termina perjudicando a los usuarios que confían en estos servicios ciegamente, sin tener en cuenta que rara vez se hacen responsables. Al igual que con los servicios y empresas cripto, hay que tener mucho cuidado, ya que si son hackeados y perdemos nuestros criptoactivos, es, por lo general, para siempre.

Importante recordar

- La manera más segura de manejar criptoactivos es guardando las claves privadas en una cold wallet y proteger la frase de recuperación guardándola en un lugar seguro.
- Utilizar cualquier servicio cripto es riesgoso ya que ante cualquier incidente podemos perder nuestros criptoactivos. Es muy importante revisar los términos y condiciones del servicio para saber qué problemas podríamos llegar a tener ante determinadas situaciones.
- Los contratos inteligentes pueden ser hackeados y los criptoactivos, robados; por eso, hay que tener cuidado con los servicios Web3 ya que podríamos perder para siempre nuestros criptoactivos.

Capítulo 6

Consejos prácticos para el día a día

El entorno más privado que tenemos es el hogar. El lugar donde uno debería sentirse más seguro y cómodo, lejos de los riesgos que pueden representar los peligros que hay puertas afuera. Sin embargo, en la actualidad, las amenazas también pueden llegar de forma remota vía internet o redes inalámbricas, por lo que debemos incluir algunas protecciones en el entorno de la casa para resguardar a nuestra familia. También es necesario saber los riesgos que enfrentamos y cómo prevenirnos cuando salimos de casa, ya sea en nuestro trabajo, al hacer compras o al irnos de viaje.

Evitar el robo de identidad

Uno de los delitos de mayor crecimiento en el mundo es el robo de identidad (también referido como usurpación de identidad) y se relaciona con la sustracción de datos personales con el fin de ser utilizados para cometer delitos, por lo general para realizar fraudes.

Algunos de los elementos a los que apunta el robo de identidad son: el documento de identidad, las tarjetas de crédito o débito, recibos de sueldo y boletas de servicios, entre otros. Esto se complementa con el robo de datos digitales y con la averiguación de información de la documentación sin tenerlos en formato físico. Por ejemplo, los datos de la tarjeta de crédito o débito sin tener el plástico, o los datos de la cédula de identidad y el pasaporte sin poseer el documento físico. Las redes sociales ayudan mucho a los delincuentes a obtener estos y otros datos en base a las preferencias, información que el usuario comparte y demás.

Un delincuente que usurpa identidad busca principalmente realizar actividades –normalmente financieras– en nombre de otra persona, tanto de forma física como virtual. En pos de esto, buscará realizar gastos con tarjetas de crédito o débito robadas (en negocios virtuales o físicos), abrir cuentas bancarias que le permitan la emisión de cheques, obtener préstamos personales, líneas de telefonía celular, etcétera. En caso de que se hayan robado tarjetas de débito, el delincuente podría extraer dinero por medio de un cajero automático o realizar compras.

Otras estafas incluyen la generación de documentos falsos a nombre de la víctima, pero con la fotografía del delincuente, a fin de conseguir un empleo o realizar ilícitos utilizando la identidad falsa, lo que provocaría problemas legales a la persona real. Por lo general, un individuo no toma conocimiento de que se ha utilizado su nombre

y sus datos hasta que aparece algún impedimento para realizar una operación financiera, como la denegación de un crédito o la contratación de un servicio. La víctima también puede darse cuenta cuando es contactada e intimada para que pague deudas que nunca contrajo, sino que han sido contraídas por el que usurpó su identidad. Algunos también se enteran cuando notan que falta dinero de sus cuentas o aparecen cargos desconocidos en sus tarjetas de crédito de compras que no realizaron.

Para la prevención de estos riesgos es fundamental entender que todas las acciones cotidianas que realizamos dejan huellas (algunas físicas y otras digitales), y es por esto que, de no tener en cuenta alguna forma de cuidarnos, podemos estar expuestos incluso sin hacer nada particularmente riesgoso. Esto va desde el acceso a cuentas de correo electrónico y servicios de internet, hasta el acceso físico a oficinas y edificios, el paso por sistemas de pago electrónico en medios de transporte público, etcétera. Todo ello genera muchos datos sobre nuestras actividades que se diseminan en distintos sistemas públicos y privados; luego, quien tenga acceso a tales datos obtendrá mucha información sobre nosotros.

También debe tenerse en cuenta a los niños, ya que ellos pueden conocer mucha información personal de sus padres. Por eso, debemos instruirlos para que no proporcionen a nadie ningún dato nuestro ni de ellos. Utilizar a los menores como canal hace que el problema se transforme no solo en un tema de los adultos sino de la familia en su conjunto.

Existen algunos comportamientos que permiten minimizar las posibilidades:

- Evitar completar encuestas y formularios en la vía pública y tener precaución cuando se nos solicita firmar petitorios aduciendo causas nobles, ya que todo esto es utilizado para recabar datos de las personas.

- En cajeros automáticos, verificar que no existan los llamados «pescadores», que son elementos que retienen el dinero que sale de la máquina, y constatar que no haya ningún elemento externo sobre el lector de la tarjeta y teclado del cajero.
- Minimizar los documentos y papeles que cargamos a diario, llevar encima solo lo indispensable, como las tarjetas y documentos que necesitemos en cada situación en particular. Las partidas de nacimiento, certificados y pasaportes no suelen ser necesarios en lo cotidiano.
- Conservar los recibos y registros de todas las transacciones electrónicas realizadas, verificar los tickets y facturas de gastos contra los resúmenes mensuales de las tarjetas de crédito para garantizar que no se han realizado operaciones desconocidas ni fraudes.
- Recortar los plásticos de las tarjetas de crédito, débito y otras luego de su vencimiento y cerrar las cuentas bancarias que han quedado inactivas o se han dejado de utilizar (como cuentas sueldo y demás), sin importar que nos digan que se cerrarán automáticamente luego de un tiempo.
- Evitar el uso de datos numéricos personales (teléfono, documento de identidad, fecha de nacimiento, etcétera) en los códigos y pins de tarjetas y claves telefónicas. Una técnica muy utilizada en los teclados numéricos es el uso de contraseñas visuales que no se recuerdan por sus dígitos sino por la ubicación en el teclado. Además, nunca escribir el pin de la tarjeta en la tarjeta misma.
- Mantener la información y la documentación personal en un lugar seguro de la casa en caso de que haya personas ajenas a la familia trabajando en ella.

- Averiguar la política de privacidad de las entidades financieras y bancos antes de darse de alta como clientes para saber cómo podría utilizarse nuestra información personal en un futuro. Además, es una buena práctica pedir un informe crediticio de uno mismo al menos una vez por año para verificar que no aparezcan actividades desconocidas o información sospechosa.
- Destruir todos los documentos antes de desecharlos, de forma que queden ilegibles. Hay gran cantidad de documentación, como resumen de cuentas bancarias y tarjetas de crédito, boletas de servicios e impuestos, etcétera, que contiene mucha información sobre nosotros y, al tirarla, cualquiera puede revisar nuestra basura y obtener esa información.
- No proporcionar demasiada información personal en los servicios de internet que utilizamos; proporcionar información falsa si no es un servicio importante.

En caso de detectar que hemos sido víctimas de robo de identidad, se debe tomar medidas de forma urgente y es importante mantener registro de todas las llamadas que se realicen y correos electrónicos, tanto enviados como recibidos, con empresas de servicios con relación al caso. En cuanto a las acciones, debemos comenzar por las denuncias a la policía y avisos a las empresas de las que somos clientes, así como también los bancos con los que operamos. Luego de la denuncia policial, no debemos olvidarnos de conservar la constancia para demostrar inocencia si llegaran a aparecer operaciones a nuestro nombre realizadas con posterioridad a la denuncia. Finalmente, en el mundo virtual, algunas redes sociales y servicios online proveen un canal para realizar denuncias por usurpación de identidad.

Proteger nuestro dinero: cuentas bancarias, tarjetas de crédito y débito

Cada vez es más común acceder a nuestras cuentas bancarias por medio de sistemas de *homebanking*, es decir, a través de internet con nuestra computadora, tablet o teléfono. Esto hace que podamos desde consultar fácilmente nuestros saldos hasta pagar servicios y hacer transferencias a otras cuentas bancarias. También es muy habitual realizar compras y pagos por internet con nuestras tarjetas de crédito y débito, además de usarlas comúnmente en comercios físicos (como supermercados y estaciones de servicio). Pero todas estas facilidades vienen acompañadas de muchos riesgos, ya que un hacker malicioso podría acceder a nuestra cuenta bancaria u obtener los datos de nuestras tarjetas para luego robarnos dinero o hacer compras y pagos sin nuestra autorización.

En internet, para realizar compras o pagos, no es necesario tener las tarjetas físicas; basta con tener el número de tarjeta, fecha de vencimiento, código de seguridad, etcétera. Esto hace que los hackers maliciosos realicen todo tipo de fraudes con tarjetas en internet.

Además de proteger nuestros datos y contraseñas –como se ha explicado anteriormente– también debemos monitorear el uso de nuestras cuentas bancarias y tarjetas en caso de que alguien quiera robarnos dinero o hacer compras y pagos no autorizados. Una manera sencilla es configurando alertas en el sistema de *homebanking* ante ciertas acciones, como débitos, pagos, transferencias, etcétera. Los sistemas modernos nos permiten realizar esto fácilmente y nos alertarán –mediante notificaciones al teléfono– a través de canales, como los mensajes de texto o e-

mails, lo cual nos permitirá identificar rápidamente si alguien está haciendo uso indebido de nuestras cuentas bancarias y tarjetas. Luego, ante cualquier operación sospechosa que se detecte, se deberá contactar rápidamente al banco o la empresa de la tarjeta de crédito para denunciar el uso no autorizado y evitar perder dinero. Algunos sistemas de *homebanking* también permiten desactivar/activar las tarjetas de manera tal que, si no utilizamos regularmente una tarjeta, podemos desactivarla fácilmente y luego activarla cuando la necesitemos; de esta forma podremos evitar su uso indebido.

Una vez, un amigo, siguiendo mis consejos, había activado alertas en todas sus tarjetas de crédito, incluyendo las extensiones, es decir, tarjetas a nombre de otra persona, pero dentro de la misma cuenta bancaria. Una tarde empezó a recibir varias notificaciones de compras en comercios por una de las tarjetas, ante lo que no se alertó ya que sabía que su pareja había salido de compras. Los mensajes continuaban apareciendo, entonces contacta a su pareja para decirle, amablemente, que si no le parecía que estaba gastando demasiado; pero ella le respondió que aún no había comprado nada. Inmediatamente mi amigo cayó en la cuenta de que, evidentemente, otra persona estaba utilizando esa tarjeta, por lo que denunció lo sucedido al banco para su desactivación inmediata.

Las alertas le permitieron a mi amigo reaccionar rápidamente, minimizar los problemas y así no perder dinero, si bien luego tuvo que realizar algunos trámites para que no le cobraran las compras no autorizadas.

Asegurar conexiones wifi

Las conexiones inalámbricas nos han dado la posibilidad de tener completa movilidad mientras permanecemos conectados a internet sin necesidad de cables, con todos los beneficios que esto implica. De hecho, con un solo dispositivo comercial estándar (router o *access point*) es posible cubrir una superficie bastante amplia, incluso a través de distintas habitaciones.

Las ventajas del wifi son muchas, pero, como todo en la tecnología, puede implicar ciertos riesgos que no debemos dejar de tener en cuenta para tener protegido el ámbito hogareño o del trabajo.

El principal riesgo de seguridad relacionado con las conexiones inalámbricas es que alguien ajeno al hogar u oficina la pueda utilizar sin permiso. El uso de nuestra red wifi por parte de terceros implica, por lo general, que nuestra conexión a internet también está siendo compartida, y esto, que *a priori* podría parecer hasta solidario, puede en verdad derivar en graves consecuencias que detallaremos a continuación:

- Posibilidad de acceso a nuestros dispositivos de red y recursos compartidos. Esto implica desde las notebooks y tablets hasta celulares y equipos de escritorio, pero también los nuevos dispositivos conectables a internet (TV, cámaras, etc.). En el peor de los casos, podría derivar en el acceso a nuestros datos y el control de nuestros dispositivos y sistemas.
- Uso del ancho de banda, con la consecuente reducción del ancho de banda disponible y disminución de la velocidad del acceso a internet. Si hay muchos equipos ajenos conectados

podríamos hasta tener problemas para vincular nuestros propios dispositivos.

- Intercepción de la información que se transmite, con la probabilidad de robo. Si bien el hecho de utilizar el mismo medio de transmisión (en este caso, el aire) hace propenso el acceso a los datos que viajan por él, la posibilidad de ser espiados dependerá de la seguridad en la transmisión de datos y la configuración de seguridad de la red.
- Uso de la conexión para acciones ilícitas, lo que implica que la responsabilidad respecto al hecho será del dueño de la conexión, o sea nosotros, ya que el proveedor de servicios de conexión a internet asocia el lugar físico de nuestra casa u oficina con la dirección de internet (llamada IP) que nos ha provisto, pudiendo así identificarnos. O sea, que alguien podría hackear sistemas desde nuestra red wifi y nosotros resultaríamos incriminados, lo que podría generarnos graves consecuencias.

Por todo esto, es recomendable cuidar nuestra conexión configurando correctamente la red inalámbrica. Nuestra red podrá ser utilizada sin autorización en caso de que alguien realice correctamente la conexión, situación que podría presentarse en los siguientes casos:

- Que la red se encuentre abierta sin ningún tipo de configuración de seguridad.
- Que el nivel de seguridad configurado sea bajo, lo que implica el uso de protocolos obsoletos que podrían ser hackeados utilizando diferentes técnicas.

- Que la contraseña de acceso sea débil o se trate de la contraseña por defecto de la red (predefinida en el dispositivo de red), lo que haría que un tercero pueda adivinarla incluso si se está utilizando un sistema de conexión seguro. Es común que los dispositivos suministrados por las empresas que nos dan acceso a internet tengan una contraseña por defecto fácil de adivinar.

Para protegernos de los riesgos derivados de las conexiones inalámbricas debemos tener en cuenta diversas medidas de seguridad que podrán ser seleccionadas desde el dispositivo de red (router iwfi o *access point*). Si no tenemos suficiente conocimiento para configurar el dispositivo, debemos llamar a un técnico que se encargue de hacerlo. Las opciones que debe tenerse en cuenta son las siguientes:

- Configurar el protocolo WPA-2 con el algoritmo de cifrado llamado AES y asignarle una contraseña difícil de adivinar. Evitar cualquier otro protocolo (WPA o WEP, básicamente).
- No dejar la contraseña por defecto que define el fabricante del router o nuestro proveedor de servicio de internet, ya que son las que primero probará un potencial atacante.
- Cambiar el nombre de la red wifi (llamado SSID). En general, tal definición viene predefinida y suele estar relacionada al nombre del fabricante del equipo o del proveedor de internet, lo que podría dar información importante a un atacante para averiguar contraseñas por defecto o problemas de seguridad conocidos.
- No dejar encendido el dispositivo en caso de que nos vayamos de vacaciones o estemos ausentes por varios días, para evitar

cualquier posible intento de ataque sin que nos demos cuenta mientras no estamos.

- Los usuarios más avanzados pueden activar el filtrado por MAC (dirección física de red) ya que, si bien es una medida adicional y puede ser salteada por atacantes con suficiente conocimiento, reduce las posibilidades de abusos eventuales.

Estas medidas nos permitirán disfrutar de todos los beneficios de las conexiones wifi, contando a la vez con la mejor garantía posible de que nuestros datos permanecerán seguros.

Cuidado con internet de las cosas

El concepto de «internet de las cosas», o IoT, por su sigla en inglés Internet of Things, refiere a la capacidad de los dispositivos de uso cotidiano de conectarse a internet, ya sea una heladera, un equipo de aire acondicionado, una cafetera, un televisor o casi cualquier dispositivo al que se pueda acceder y ser controlado de forma remota a través de internet, normalmente mediante el uso de una aplicación para teléfono celular que admita su manejo.

Cada vez son más los dispositivos que ofrecen esta funcionalidad. Como ejemplo de uso cotidiano podríamos mencionar un usuario que desea que su casa esté a una determinada temperatura cuando él llegue, pero no sabe a qué hora será eso. Para lograrlo, se conecta con su acondicionador de aire o calefactor mediante el teléfono celular antes de salir de la oficina y le indica que se encienda y permanezca a cierta temperatura.

Esta nueva tendencia a conectar todo a internet para que se pueda acceder remotamente incluye un riesgo y es el hecho de que, para ser accesibles desde el exterior, los dispositivos deben estar «visibles» en internet. Esto implica que, si están accesibles para el dueño, también lo pueden estar para un potencial hacker malicioso. No obstante, que se encuentren a la vista no significa que de forma directa puedan ser controlados por cualquiera, ya que, por lo general, los fabricantes incorporan alguna medida de protección básica, como la conexión por medio de un canal seguro y el uso de contraseñas, aunque esto suele ser insuficiente.

Las estadísticas realizadas por importantes empresas de seguridad sobre los dispositivos IoT indican que más del 80 % posee problemas de seguridad que pueden ser aprovechados remotamente. Aunque la solución podría ser la aplicación de alguna

actualización o parche de seguridad por parte del fabricante, estos dispositivos electrónicos generalmente no están preparados para recibir actualizaciones de su software en forma sencilla, limitando así la posibilidad de que su seguridad sea mejorada. Esto deja a los usuarios desprotegidos y sin la opción de tomar otro camino que no sea la aceptación del riesgo si quieren disfrutar de los beneficios.

En caso de que un dispositivo tenga un problema de seguridad que pueda ser aprovechado por un ciberdelincuente, él podría explotarla y tomar control del equipo manejándolo remotamente. Pero esto no termina aquí, ya que el aparato está emparentado a internet por medio de la conexión que tenemos en el hogar, la que interconecta a todos nuestros dispositivos (notebooks, tablets, PC, teléfonos celulares, impresoras y demás). Eso podría significar que, atacando un dispositivo IoT, el hacker pueda llegar a acceder a la red de nuestra casa u oficina, por lo tanto, a nuestra información y privacidad. Las principales formas de protegernos contra estos problemas son las siguientes:

- Antes de comprar un dispositivo IoT, ver si cuenta con problemas de seguridad conocidos o si tiene la posibilidad de recibir actualizaciones del fabricante en caso de que surjan problemas en el futuro.
- Habilitar todas las configuraciones que permitan aumentar el nivel de seguridad, ya sea mediante el uso de contraseñas, de encriptación o cualquier otra medida que el fabricante provea en la funcionalidad del dispositivo.

Proteger nuestras computadoras

Tiempo atrás, la computadora de escritorio era el único dispositivo que nos permitía acceder a internet, seguido por las notebooks, que pronto dominaron el mundo de la movilidad. En los hogares y pequeñas oficinas era normal tener una sola PC en alguna habitación, hasta que la reducción de costos y la popularización de las redes hicieron que comenzaran a sumarse más PC y otros equipos como notebooks, netbooks, etcétera. Luego vinieron las tablets, con funcionalidades similares, pero de gran movilidad, incluso superando a las portátiles, y finalmente aparecieron los teléfonos inteligentes, que prácticamente tienen todas las funcionalidades de un equipo de escritorio en un tamaño reducido.

Actualmente, tanto en el hogar como en oficinas, existen varias computadoras interconectadas que tienen acceso a nuestra información. Al igual que lo hablado hasta aquí, siempre es importante analizar que todo puede incorporar nuevos riesgos, y nuestras computadoras no escapan a esto. En este caso, si bien aplican muchos de los mismos consejos que hemos visto, analizaremos algunos más específicos.

Uno de los más importantes es que debemos realizar copias de seguridad (*backups*) de nuestros archivos importantes con frecuencia (dada por el ritmo al que creamos y modificamos nuestros datos). Esta práctica tan simple les ahorraría muchos dolores de cabeza a las personas cuando, por algún accidente o ataque de un hacker malicioso o software dañino (malware), pierden sus datos y no pueden recuperarlos.

Para hacer copias de seguridad o respaldo se puede conseguir un disco rígido externo o pendrives USB de alta capacidad de almacenamiento para grabar en ellos lo que consideramos más

importante entre nuestros archivos. Si bien en un caso ideal podríamos hacer copia de todo, suelen dejarse fuera de estas los archivos multimedia –como videos o música– que podrían conseguirse nuevamente, ya que ocupan gran cantidad de espacio. Claro que esta decisión es de cada persona, y tanto la cantidad de archivos como la ubicación y la frecuencia con la que se realizará el *backup* deben ser analizadas a fin de aplicar la medida con efectividad. Por ejemplo, realizar una copia de seguridad una vez por año (supongamos que se hace en cada inicio de enero) implicaría que si ocurre un problema un día lejano a ese momento (por ejemplo, que se rompa el disco rígido en octubre), habríamos perdido casi diez meses de archivos generados. Tampoco tiene sentido realizar el *backup* una vez por semana si no se hacen demasiadas modificaciones o no se crean archivos nuevos, aunque podría haber casos en los que sí es conveniente.

Si generamos archivos nuevos regularmente –ya sea del trabajo o relacionados con nuestros estudios– debemos considerar hacer *backups* diarios o cada pocos días, ya que, ante un problema, podríamos perder datos valiosos e importantes, lo que nos generaría numerosos inconvenientes. Como vemos, depende del uso que se le dé a la computadora y la importancia de los datos que se manejen con ella.

Por otro lado, tenemos la posibilidad de hacer copia de seguridad de archivos en la nube, donde, más allá de los riesgos considerados, podemos mantener una copia sincronizada constantemente, normalmente de almacenamiento bastante limitado con relación a la cantidad de archivos que se suele tener en las computadoras.

Otra buena práctica es mantener nuestras computadoras siempre con el software actualizado, tanto el sistema operativo como las aplicaciones, así como hemos dicho para el caso de

celulares y tablets. Dicho hábito reducirá la posibilidad de que sean afectados por problemas de seguridad que ya han sido arreglados en las actualizaciones.

Debemos tener en cuenta que una computadora de escritorio, al no ser móvil, tiene menos riesgo de ser afectada por factores externos, como ocurre con los celulares, tablets y notebooks, que, dependiendo de a dónde se los lleve, pueden conectarse a redes inseguras, por ejemplo. A su vez, al contrario que los dispositivos móviles, son más difíciles de ser robadas o extraviadas. Esto es una ventaja ya que, si la mantenemos cuidada, se transforma en un equipo más confiable desde el cual se pueden realizar con menos riesgos transacciones por *homebanking*, compras online y otras operaciones financieras.

Asimismo, debemos tener cuidado cuando colocamos en la computadora una unidad de almacenamiento externo (disco, memoria, pendrive) desconocida o que haya sido conectada anteriormente en un equipo que no es nuestro, ya que corremos el riesgo de infectarla con malware que se encuentre oculto en la unidad de almacenamiento externo. Para evitar esto, siempre debemos tener un antivirus instalado y actualizado.

Ante el mal funcionamiento habitual del software de nuestra computadora, suele ser recomendable reinstalar el sistema operativo, algo a lo que muchos usuarios se rehúsan porque debe realizarlo un técnico o persona idónea, corriendo así el riesgo de perder programas instalados o archivos que quedaron en ubicaciones no consideradas.

Reinstalar el sistema es especialmente útil cuando se trata de equipos con Windows, ya que el uso diario, sumado a la instalación y desinstalación constante de aplicaciones, hacen que, con el tiempo, el equipo pueda volverse menos eficiente, más lento, etcétera. En caso de no realizar una reinstalación completa, es

importante asegurarse de que al equipo se le efectúe un correcto mantenimiento preventivo.

Cuidado con conexiones fuera del hogar y la oficina

Cuando nos encontramos fuera de nuestros lugares habituales de conexión a internet, pero necesitamos estar online, es común buscar alguna cafetería o conexión pública que nos permita el acceso. Esto, desde el punto de vista de la seguridad, como vimos, es considerado un comportamiento riesgoso, ya que, en principio, desconocemos sus medidas de protección ante ataques.

Algunas de las medidas más importantes que podemos tomar para reducir el riesgo que se corre al conectarse desde un acceso que no sea el de uso cotidiano y confiable son las siguientes:

- No confiar en cualquier red wifi abierta y sin contraseña, ya que hay hackers maliciosos que colocan puntos de acceso a internet que ellos mismos controlan. Lo que hacen es crear redes wifi abiertas que cualquiera pueda utilizar para que las comunicaciones de todo usuario que se conecte puedan ser espiadas y la información que circule, capturada. También les permite realizar ciertos tipos de ataques a nuestros dispositivos y hackearlos en forma remota. Por eso, no debemos dejarnos tentar por conexiones abiertas que proveen acceso a internet, aunque lo necesitemos (los hackers maliciosos aprovechan esto). Ante una urgencia es provechoso emplear la función de compartir internet del teléfono celular (la mayoría cuenta con esta característica), que, si bien utilizará la red de datos de telefonía celular, no sería un inconveniente si se tratara de un caso especial.
- No utilizar conexiones wifi públicas para acceder a servicios sensibles como *homebanking* y sitios donde se maneja

información financiera, aunque estemos utilizando nuestro propio dispositivo para conectarnos.

- No recurrir a computadoras de uso público para acceder a cualquier servicio online, desde redes sociales hasta correo electrónico, en tanto desconocemos el mantenimiento que reciben, por lo que aumenta –en gran medida– el riesgo que se corre. Tales computadoras podrían tener programas espías que capturen nuestras contraseñas y demás datos.
- Tener cuidado con las sincronizaciones automáticas, puesto que se activan en cuanto encuentran conectividad disponible. Conviene que algunos programas no se inicien –o al menos no se conecten– de manera automática, especialmente cuando se está utilizando una red pública.
- Utilizar software de protección adicional al antivirus básico, es decir, un firewall local. De hecho, los sistemas operativos (tanto las plataformas Windows más nuevas como Linux) cuentan con un sistema de protección generalmente activado o que debemos encender para mejorar nuestra seguridad. También muchos productos antivirus disponen de protecciones adicionales contra amenazas de red. Estas protecciones complementarias evitan que se realicen conexiones entrantes a nuestros sistemas por parte de otros usuarios de la red. Los sistemas Windows, por ejemplo, incluyen el «centro de redes y recursos compartidos», donde se puede asignar un nivel de confianza a la red a la que nos conectamos. Las opciones disponibles son «Pública» y «Privada», esta última para seleccionar solo cuando confiamos en el entorno; por ende, al conectarnos a redes desconocidas siempre debemos elegir la opción «Pública».

- Seleccionar prudentemente las redes wifi a las que los dispositivos se conectarán de forma automática, ya que un hacker malicioso podría forzar el nombre de una red para que un equipo se conecte. Además, debemos eliminar cada tanto las redes de uso no frecuente de la lista de puntos de acceso memorizados por el sistema.
- Mantener siempre los equipos y dispositivos actualizados, tanto a nivel de sistema operativo como de aplicaciones.
- Utilizar software de VPN para que todos los datos que «viajen» desde nuestro dispositivo hacia el sitio de destino lo hagan a través de un canal protegido por cifrado (encriptado); así, nuestros datos no podrán ser capturados o interceptados.

En general, decimos que no es posible eliminar completamente los riesgos que presenta el uso de redes desconocidas, pero, tomando las medidas mencionadas, sí podemos hacer una enorme reducción de los peligros. A esto debe sumarse la prudencia en el uso general de los dispositivos y la aplicación del sentido común.

Proteger dispositivos al viajar

Una situación particular sobre la necesidad de conexión se da cuando estamos de viaje. Si bien deberíamos en principio seguir las mismas pautas que mencionamos anteriormente, eso no alcanza para reducir los riesgos, ya que también necesitamos tomar medidas de protección adicionales sobre nuestros dispositivos (al menos del teléfono celular, tablet y/o computadora portátil).

En el caso del teléfono celular, suponiendo que hemos realizado un viaje al exterior del país, a veces no contamos con la posibilidad de utilizar nuestro servicio de telefonía móvil por no poder conectarlo a la red local. Esto nos obliga a recurrir a una conexión wifi para emplear las distintas funciones de nuestro dispositivo móvil, debiendo tomar las precauciones a las que referimos anteriormente.

Es recomendable tener instalado un software de localización del equipo y activar el GPS durante el viaje para que, en caso de que lo perdamos o nos lo roben, tengamos alguna posibilidad de recuperarlo. Para mayor información sobre la seguridad en dispositivos móviles, consultar nuevamente el capítulo donde se trató el tema de forma exclusiva.

Respecto a las tablets, aplican prácticamente las mismas medidas que para los teléfonos celulares, ya que se pueden utilizar contraseñas de acceso, geolocalización (localización por coordenadas GPS), protección física, etcétera.

Si nos referimos a las notebooks, la situación es un poco más compleja, ya que debemos considerar medidas adicionales:

- Utilizar protección por contraseña de acceso al equipo (se solicita apenas se enciende el equipo) como barrera adicional de seguridad ante accesos no autorizados al sistema. Para

esto deberemos ingresar a las opciones de configuración de la computadora (depende de cada modelo) y programarlo para que solicite la contraseña ante cada reinicio.

- Emplear contraseña para el inicio de sesión del sistema operativo y no permitir que lo realice de forma automática. Esto es fundamental para evitar que cualquier persona tenga acceso a nuestros datos. También es útil configurar el sistema para que se autobloquee luego de un tiempo de inactividad, que puede ser al transcurrir unos segundos o unos pocos minutos; de esta forma, si nos alejamos del equipo este se bloqueará al poco tiempo y requerirá contraseña para desbloquearse, evitando así que alguien pueda acceder.
- Habilitar el uso del cifrado de disco rígido, que es una medida que ofrecen los sistemas operativos modernos para que los datos se almacenen protegidos en forma encriptada, todo de forma transparente para el usuario. De esta manera, si alguien quisiera aplicar ataques más avanzados –como iniciar el equipo desde un pendrive o extraer físicamente el disco rígido para sacar la información– se encontraría con que los datos no pueden ser leídos por estar encriptados.
- Contar con un cable de seguridad que permita que el equipo pueda ser sujetado a un punto fijo (o de difícil movilidad), como una mesa, para evitar que pueda ser llevado fácilmente del lugar. Aunque este cable podría ser cortado con alguna herramienta, ofrece protección contra descuidos eventuales o intentos casuales de robo por distracción.
- Tomar todas las medidas viables para garantizar la seguridad en las conexiones inalámbricas y, de ser posible, utilizar conexiones a través de una VPN. Los equipos deben ser

configurados para conectarse de forma segura cuando se encuentran fuera de una ubicación confiable.

Al viajar es importante tener cuidado con el uso del doble factor de autenticación para los servicios de internet que utilizamos con frecuencia, ya que al estar de viaje puede que alguno de ellos nos impida ingresar al detectar que nos estamos conectando desde una ubicación diferente a la habitual y nos mande un código por mensaje de texto para verificar nuestra identidad. Por este motivo, es fundamental tener en cuenta que es posible que no estemos en condiciones de recibir SMS con los códigos para validar nuestra identidad debido a limitaciones en el servicio. Para evitar este problema se puede configurar que los códigos nos sean enviados por e-mail en vez de mensaje de texto.

Si viajamos a países que puedan ser conflictivos o inestables por no ser democráticos, estar en guerra o tener leyes muy estrictas, hay que tomar precauciones extras, en caso de que nuestros dispositivos puedan ser registrados, confiscados, interceptados, etcétera. Al viajar a este tipo de destinos, lo mejor es llevar dispositivos (teléfonos, computadoras, tablets) que estemos dispuestos a perder si es que nos los confiscan o roban. Tienen que tener la menor cantidad de información posible (datos y aplicaciones) y no contener información que nos pueda incriminar porque violemos sus leyes. Por ejemplo, en algunos países están prohibidas las imágenes y los videos con desnudos, así como el uso de algunos tipos de aplicaciones.

Respecto al uso de e-mail, lo mejor es crear una nueva cuenta de correo (en cualquier servicio gratis al que se pueda acceder en el país que visitaremos), específica para el viaje, y utilizar solo esa cuenta y ninguna otra, quitando todas las demás cuentas de e-mail de los dispositivos que llevemos. De esta forma, si alguien obtiene acceso a nuestros dispositivos solo podrá ingresar a esa cuenta

nueva, que no es importante y no tendrá demasiada información. En caso de necesitar seguir recibiendo e-mails de nuestras cuentas habituales durante el viaje, se puede redirigir los correos hacia la cuenta que creemos eventualmente. Esto último se puede hacer cambiando la configuración de cada cuenta para el reenvío de e-mails, y establecer la dirección nueva a donde serán redirigidos.

Siempre antes de viajar a países que no conozcamos debemos investigar si suele haber problemas con el uso de la tecnología, para evitar cualquier posible inconveniente.

Ayudar a los adultos mayores con la tecnología

Si los niños requieren una atención especial con relación al uso de las nuevas tecnologías, los adultos mayores también se encuentran en este grupo. En su caso, no será por las mismas cuestiones, pero sí por acompañarlos en el proceso de adaptación. Muchos de nuestros padres y abuelos argumentan tener cierta aversión a la tecnología, pero la realidad muestra que cuando realmente se disponen a intentarlo pueden aprender en no mucho tiempo y aprovechar todos sus recursos y beneficios.

Algunas de las problemáticas y temas que deben abordarse respecto a los adultos mayores son las siguientes:

- Explicarles los conceptos y la jerga: la tecnología y la cultura moderna han producido expresiones, palabras y conceptos nuevos que no resultan familiares para quienes no estén en el tema, por lo que es muy importante enseñarles lo que significan términos como chat, virus, malware, backup, spam, phishing, y muchos más.
- Advertirles de los cuidados que se deben atender respecto al robo de identidad, teniendo en cuenta las acciones que los delincuentes realizan mediante el uso de la tecnología.
- Instruirlos sobre el manejo prudente de las contraseñas, así como también las reglas para crearlas fuertemente y métodos para poder recordarlas.
- Mantener actualizados los sistemas que los adultos mayores utilizan para evitar problemas derivados de la falta de actualizaciones de seguridad. Para esto, puede configurarse el software de manera tal que se actualice de forma automática.

- Explicarles el funcionamiento de los ataques de phishing, haciendo hincapié en que no deben hacer clic en ningún vínculo que llegue de desconocidos por correo electrónico o mensaje de otro tipo. También indicarles que no deben ingresar datos personales en cualquier sitio de internet, y que ante cualquier duda nos consulten.
- Referirles sobre el uso prudencial de los teléfonos celulares, tal como se ha explicado aquí anteriormente. Esto incluye el hecho de que puedan aprender a utilizar teléfonos inteligentes modernos y aprovechar sus capacidades, en lugar de estar resignados a utilizar teléfonos básicos.
- Alertarlos de los mensajes de correo electrónico, mensajería instantánea y llamadas telefónicas de personas desconocidas o cuya identidad no pueda verificarse. Nunca responder a los pedidos que pudieran surgir de estos contactos dudosos.
- Informarles sobre las distintas formas de engaño que los delincuentes desarrollan, como las llamadas telefónicas, en las que se hacen pasar por una empresa de servicios, la policía o algún miembro de la familia, con el fin de que provean información, envíen dinero o realicen alguna otra acción determinada.

Las experiencias con adultos mayores indican que el uso de la tecnología no tiene por qué ser una barrera infranqueable, sino que, por el contrario, muchas veces aparecen motivaciones para querer utilizarla, como poder hacer videollamadas con los nietos o contactarse con viejos amigos por redes sociales. En cualquier caso, es importante encontrar los incentivos que podrían tener los mayores y fomentarlos para que no queden excluidos ante los avances de la tecnología.

Importante recordar

- Tomar medidas de precaución para evitar el robo de identidad, ya que es muy complicado recuperarse de un problema de esta magnitud. Para esto, es recomendable manejarse cautelosamente con la información privada, y evitar que nuestros datos y documentación personal caigan en manos de terceros de forma no autorizada.
- En caso de descubrir que se es víctima de un robo de identidad, se recomienda consultar urgentemente a un especialista y tomar medidas con rapidez a fin de evitar que el problema crezca.
- Asegurarse de que la conexión wifi hogareña se encuentre protegida, ya que, de lo contrario, un hacker malintencionado podría acceder a nuestra red y, por ende, a nuestros dispositivos y datos.
- Configurar nuestro router wifi de forma segura, seleccionando las opciones convenientes. De no contar con el conocimiento para hacerlo, consultar con un técnico o persona que pueda realizarlo.
- Tomar precauciones al elegir e instalar dispositivos conectables a internet (IoT), ya que pueden ser un canal de acceso a nuestra red y a nuestra información para posibles intrusos.
- Realizar mantenimiento preventivo de nuestras computadoras, evitando que se infecte con malware y funcione de forma incorrecta.

- Realizar copias de seguridad de nuestra información más importante en forma regular, definiendo qué archivos se resguardarán, dónde y cada cuánto tiempo se hará.
- Tomar precauciones cuando nos conectamos a internet desde una conexión wifi pública, evitando realizar operaciones sensibles si no se confía en la red o en el proveedor, o si se sospecha de algo.
- Considerar la protección y el resguardo físico de los dispositivos móviles cuando estamos de viaje, e implementar medidas de seguridad avanzadas (como la localización de equipos o el cifrado de disco).
- Integrar a los adultos mayores a la tecnología de forma gradual, ayudándolos a adaptarse para que puedan aprovechar sus beneficios sin correr riesgos innecesarios.

Capítulo 7

Consejos para padres y educadores

Los adultos tienen la enorme responsabilidad de ser constantemente una referencia para los niños y adolescentes en todos los ámbitos de la vida. Si bien no existe una forma única e indiscutida de encarar la educación con relación al uso de las nuevas tecnologías, es importante que tomemos un rol activo en nuestra capacidad de reacción y conocimiento de los temas para evitar que nuestros hijos corran riesgos innecesarios. Es importante, desde el rol de padres y docentes, saber qué debemos tener en cuenta con los menores a la hora del uso de la tecnología.

Comprender los riesgos

Los menores utilizan internet, dispositivos electrónicos y todo tipo de tecnologías de forma natural; crecen teniéndolos como parte de su entorno cotidiano. En la actualidad, resulta muy difícil hacer una separación entre las actividades diarias y su conexión con las redes e internet, ya que la vida social tiene hoy día un aspecto «conectado» en el que, de manera cada vez más intuitiva, se comparte información constantemente. Muchas veces, la toma de conciencia sobre la importancia de los datos personales y la información aparece como resultado de una experiencia negativa propia o de alguien cercano, por ejemplo, cuando fotos o videos indiscretos se hacen públicos. Por esto, es necesario tener en cuenta que los menores no son, en principio, conscientes de los riesgos a los que están expuestos por el solo hecho de relacionarse con su entorno digital y tener un manejo avanzado de las distintas tecnologías.

Entre los factores más importantes en la comprensión de los comportamientos de los menores está la diferencia generacional entre ellos y sus padres. Una de las preguntas que más surgen entre los padres es quién debe hablar con los niños sobre los temas de riesgos en el uso de las tecnologías. La respuesta es: los propios padres. Esta duda aparece debido a dos factores: primero y principal, el desconocimiento que muchos adultos tienen sobre cómo comunicarse acerca de ciertos temas con sus hijos; y segundo, el desconocimiento sobre los temas que deben abordarse. Debido a esto último es que, dependiendo de nuestra afinidad con la tecnología y de la edad de los menores, es posible que tengamos que hacer un esfuerzo y prestar atención al uso y riesgos existentes. Por otro lado, surge la pregunta de cuándo es el momento de hablar,

presuponiendo que hay una edad adecuada y una situación ideal. Pero nada más lejos de la realidad; muchos expertos coinciden en que el momento para hablar es ahora mismo. Claro que hay que buscar la mejor manera de comunicarse en función de las edades, prioridades y situaciones, pero nunca es bueno dilatar el momento para comenzar a abordar los temas.

Es responsabilidad de los adultos comprender los riesgos a los que están expuestos los menores debido al uso de la tecnología, para así poder encontrar la mejor forma de comunicárselo. Esto incluye un involucramiento cada vez mayor en el mundo de la tecnología, la prueba constante de dispositivos, software, servicios online, y hasta juegos y medios de entretenimiento. Así, aprendiendo a ser uno mismo consciente de los peligros existentes, puede determinarse con criterio propio cómo incidirá en los niños ese peligro, lo que permitirá encontrar formas de protegerlos.

Debemos considerar además que, en la actualidad, los viejos consejos de seguridad personal para manejarse en la calle y con extraños siguen siendo necesarios, pero ya no bastan para formar en la mente de un menor el sentido común que se requiere para enfrentar situaciones de potencial peligro. Muchos de los males que en persona podrían ser amenazas tienen su paralelismo en el mundo digital. Por ejemplo, el consejo de «no hablar con extraños» se puede extender a las redes sociales y mensajería (aunque pueda parecer exagerado), el «no aceptar cosas de desconocidos» podría aplicarse a aceptar recibir archivos o enlaces a sitios web; de igual manera, la cotidiana advertencia de «cuidarse al ir por la calle» bien podría tener su analogía con la navegación en internet, en donde es necesario cuidarse de los sitios que uno visita ya que algunos pueden ser peligrosos por tener contenido no apto para menores o programas dañinos.

Finalmente, no deben olvidarse las líneas principales que deben seguirse para fomentar un uso positivo y seguro de internet y las tecnologías digitales: la mediación activa (supervisar, acompañar y orientar) y la mediación restrictiva (establecer limitaciones para resguardarlos de riesgos), entre las que se debería encontrar un equilibrio según la edad y la madurez del niño.

Es necesario que los menores comprendan que, si bien normalmente el uso de las tecnologías es seguro, hay riesgos, y hay que conocerlos para ser precavido y saber la mejor manera de defenderse y actuar sin tener miedo.

Niños, tecnología y datos personales

En algún momento de la vida de los niños llega su primer teléfono celular, lo cual varía bastante entre países, ciudades, culturas y niveles socioeconómicos, pero ciertamente es un momento en el que los datos personales del menor comienzan a estar expuestos de forma más abierta. Al principio puede que los padres lo hagan para poder estar en contacto con los hijos, pero con el tiempo es probable que ellos comiencen a buscar su independencia, y es importante identificar cuándo llega ese momento.

Seguramente nuestros niños hayan usado previamente computadoras de escritorio, notebooks, tablets o consolas de videojuegos en casa y en la escuela. Sin embargo, el teléfono celular es el primer dispositivo electrónico individual y privado que tendrá en su vida, ya que allí reunirá datos de otros, compartirá los propios, se conectará a las redes sociales y a internet, y no siempre estará supervisado por un mayor.

En algún momento los niños comenzarán a tener su propia dirección de e-mail, cuentas de redes sociales y otros perfiles personales que formarán parte de una identidad digital que los acompañará el resto de su vida. Esto hace que sea importante la configuración inicial de las cuentas y el software para evitar, por ejemplo, que personas desconocidas entren en contacto con ellos.

En general, la edad mínima para registrarse en la mayoría de los sitios de internet serios está entre los 13 y los 14 años, cuando se trata de redes sociales, y de 18 años para aquellos sitios en los que se maneja dinero o contenidos específicos para mayores. Por ejemplo, en Facebook no es posible dar de alta un perfil para niños menores de 13 años, excepto que se mienta con la edad, lo que es algo común, por lo que los más pequeños terminan usando redes

sociales, quedando expuestos a posibles peligros. Es importante que el alta de tales perfiles se realice de la mano de un mayor, para evitar que el menor proporcione información personal o de la familia que pueda ser riesgoso de publicar y que quede al alcance de cualquier persona. En principio, solo deberían completarse los campos de datos obligatorios y dejar el resto para más adelante.

En este punto es fundamental destacar que los niños, *a priori*, no pueden definir qué datos podrían comprometer su integridad física o psicológica, por lo que es conveniente indicarles que información como el documento, la dirección de la casa, nombres de los familiares y ocupaciones, entre otros detalles, no debe ser brindada sin la autorización de un mayor. Es importante explicar por qué no deben ser compartidos esos datos personales para así ayudar al niño a ir comprendiendo los peligros relacionados con el uso de internet.

En los casos de los servicios que solicitan un nombre de usuario, es buena idea que los padres ayuden al menor a crear uno, ya que la elección de los niños suele agregar la edad o la fecha de nacimiento al nombre de usuario cuando encuentran que su nombre ya está ocupado por otro (mucho más común hoy en día que hace algunos años debido a la enorme cantidad de usuarios). La idea es que el nombre de usuario no permita identificar datos del menor, y si se evita recurrir a su nombre propio, mejor. Lo mismo aplica para la elección de contraseñas, donde se debe seguir las recomendaciones expuestas en capítulos anteriores.

Es importante considerar también que nunca se puede saber a ciencia cierta qué harán las empresas con nuestros datos personales y cómo esto incluye a los niños, por lo que debemos pensar dos veces antes de dar el alta compulsiva en sitios y crear perfiles innecesarios. En algunos países, por ejemplo, la ley obliga a las empresas a proteger estos datos, pero muchas de ellas están

ubicadas en otros territorios y no se les aplica la legislación local. Frente a la duda, siempre es posible consultar las condiciones de uso del servicio y la política de privacidad antes de proveer nuestros datos.

Algunos datos –y consecuencias posibles– sobre los que debemos educar a los menores a no proveer (o hacerlo de manera limitada y consciente) son los siguientes:

- El número de documento o pasaporte: puede originar que alguien cometa fraudes a nuestro nombre.
- Correo electrónico: aumenta la probabilidad de recibir correos basura (spam) y mensajes con intentos de estafa, fraude o engaños.
- Datos bancarios: puede producir pérdidas económicas.
- Ubicación geográfica del domicilio: tanto el lugar de vivienda como el de otros sitios que se frecuentan brinda información que podría hacer que alguien nos localice o conozca nuestra rutina, movimientos y hábitos diarios (incluyendo los horarios en que nos encontramos en casa y fuera de ella).
- Fotos y videos: permiten conocer mucha información sobre uno mismo, como los lugares donde vamos, quiénes son nuestros familiares y amigos, nuestro nivel socioeconómico, los gustos y preferencias, y mucho más.

En líneas generales, la mayoría de los servicios solicitarán información del tipo personal del usuario, y si bien cuando los niños son pequeños esa información es proporcionada por los padres, hay un momento en el que es importante permitir que ellos comiencen a tener sus propios entornos digitales, con su información y configuraciones. Esto, como dijimos, debe continuar siendo

supervisado por un adulto, hasta que los niños estén en condiciones o en edad de generar lo propio sin ayuda.

En los sitios web que requieren demasiada información personal, cuando el servicio no sea algo de uso indispensable o importante, se puede proveer datos falsos para proteger la información personal del menor.

Distintas medidas para distintas edades

Las nuevas generaciones de niños y adolescentes nacieron en un contexto ya muy tecnológico, por lo que se los llama «nativos digitales». Esta generación de jóvenes tiene una fuerte dependencia de la tecnología y se orienta con comodidad al relacionarse por medio de lo virtual, lo que algunos temen que podría derivar en una disminución de las habilidades sociales presenciales, aunque se vinculen a través de comunidades online sin siquiera conocerse personalmente.

La tecnología también provocó que la inmediatez sea parte de la realidad cotidiana de las nuevas generaciones, lo que derivó en el desarrollo de personalidades más impacientes que sus antecesores, característica aprovechada por el mercado de consumo para ofrecerles lo que quieren: velocidad, simplicidad y comodidad. No obstante, ser nativos digitales no los convierte automáticamente en competentes digitales, ya que eso incluiría habilidades para utilizar herramientas tecnológicas de forma segura y prudente.

En ese sentido, podemos separar las franjas etarias en distintos grupos:

- 2 a 5 años: en esta primera etapa se les debe permitir el uso de los dispositivos conectados a internet solo en presencia de un adulto, presentarles aplicaciones y juegos simples, crearles cuentas especiales en los dispositivos y sistemas, inculcarles la importancia de la privacidad, no dejarlos utilizar las cuentas de los mayores, y pedirles que, si se sienten mal con algo que ocurra, lo comuniquen a un mayor inmediatamente.

- 6 a 12 años: en esta etapa los niños comienzan realmente a usar de forma más independiente internet, por lo que se les debe enseñar normas de conducta en la red, continuar supervisándolos de forma consensuada, hacer hincapié en la importancia de la seguridad y privacidad, evitar el contacto con desconocidos, adecuar los videojuegos a la edad y dar pautas del uso de teléfonos móviles en caso de que se les brinde uno.
- 13 a 16 años: a esta edad comienzan a tener sus primeras cuentas de redes sociales y otros servicios, por lo que es importante conversar sobre lo que ocurre en esos contextos y sus riesgos. En algunos hogares se escribe un documento de buenas prácticas a modo de compromiso familiar y recordatorio. También se debe comunicar los riesgos de los archivos descargados y los sitios web que se visitan, y transmitir que no todo lo que se dice en internet es necesariamente cierto.
- 17 y 18 años: esta es la edad en la que comienza la madurez para identificar los peligros y protegerse de forma autónoma. En caso de haber hermanos mayores, es útil que haya intercambio de ideas con los más pequeños. Los temas de riesgos, privacidad y seguridad deben continuar estando en agenda, apuntando siempre a tener una comunicación fluida para promover la confianza.

Por supuesto que estas recomendaciones son generales y pueden no reflejar el nivel exacto de acciones a tomar, en tanto ellas dependen más del nivel de madurez de los menores que de su edad biológica. Lo que sí puede tomarse como referencia es la variación entre los más chicos y los más grandes, ya que todos atravesarán –de una u otra forma– las mismas etapas, independientemente de que cada consejo se adapte a su edad del momento.

Riesgos para niños y adolescentes

Si bien los niños y adolescentes se encuentran expuestos a los mismos peligros en internet que los adultos, también lo están a riesgos que los afectan a ellos específicamente y no a los mayores, en tanto los menores carecen de experiencia en la vida y son más vulnerables ante distintas situaciones. Conociendo estos riesgos, los adultos pueden guiar y enseñar a los menores cómo actuar y estar prevenidos.

Ciberbullying

Una de las preocupaciones más relevantes de los padres suele ser la violencia que los niños ejercen con sus pares, lo que hoy día extiende su manifestación al entorno online. Entre estas prácticas (que muchas personas adultas han padecido en su etapa escolar) se encuentra la que se ha denominado bullying, la cual refiere al acoso entre menores (o a veces de un niño mayor hacia uno menor). El uso de medios digitales para realizar esto se conoce como ciberbullying, lo que no es más que una extensión de los medios tradicionales a los modernos.

Esta conducta caracterizada por insultos, agravios y chantaje emocional hacia las víctimas puede suponer también el uso de información difamatoria propagada por distintos canales como mensajes de texto, e-mail, mensajería instantánea y redes sociales. Además, puede incluir la publicación de videos y fotos con el fin de ejercer violencia emocional y psicológica sobre el niño; un escenario que, a su vez, da origen a páginas de Facebook, cuentas de Instagram o blogs destinados a publicar material difamatorio y agresivo para la persona. Lógicamente, el servicio o red social

desconoce el objetivo, por lo que solo pueden actuar a partir de la recepción de una denuncia.

La versión digital del bullying tiene como daño colateral que la publicación de contenidos en internet hace que las pruebas visibles del acoso permanezcan online por tiempo indeterminado, incluso hasta más allá del momento en el que deja de ser utilizada para su fin original.

Existen motivos por los que el ciberbullying está tan difundido. Uno de ellos es la sensación de anonimato de internet; es decir, la facilidad de ocultar o falsear la identidad online ofrece una suerte de anonimato que aumenta la sensación de poder por parte del acosador. Además, saber que tras una pantalla pareciera imposible devolver el daño incrementa aún más la actitud abusiva. Incluso, cuando se trata de acoso de varias personas hacia una sola, el comportamiento grupal produce una disminución de la autoconciencia individual, ya que los niños se encuentran defendidos y protegidos por el mismo grupo. Por otro lado, existe una dificultad natural para percibir el daño provocado, lo que se daría de no existir el anonimato, puesto que la propia distancia que ofrece la tecnología debilita las limitaciones sociales, al tiempo que facilita la desinhibición del comportamiento. Asimismo, la inmediatez dada por la velocidad de las comunicaciones produce formas de actuar más impulsivas que motivan la continuidad del incremento de los problemas en base a las reacciones de cada lado.

Es muy importante para los padres detectar temprano los posibles casos de acoso que estén sufriendo sus hijos. Para eso, deben estar atentos a algunos síntomas que podrían permitir identificarlo:

- Cambios físicos y emocionales: manifestaciones de dolencias frecuentes (dolores de cabeza o estómago), cambios de

estado de ánimo, estados sostenidos de tristeza o apatía sin razón aparente, ansiedad inusual, comportamientos agresivos.

- Cambios conductuales y en su interacción con otros: alteraciones de comportamiento en sus actividades habituales, modificaciones en los hábitos alimenticios y de sueño, cese de uso de dispositivos o redes sociales, lesiones autoinfligidas, cambios de grupos de amigos.
- Cambios en su desempeño escolar: involucramiento en incidentes dentro de la escuela, menor capacidad de concentración o atención, falta de interés en temas de su preferencia, baja en el rendimiento estudiantil, pérdida de pertenencias y útiles, lesiones físicas inusuales.

Asimismo, existen algunas recomendaciones de prevención útiles, tanto para los padres de un niño acosado como de uno acosador:

- Educar en habilidades digitales: es fundamental incorporar en la educación del hogar los conceptos y herramientas de uso cotidiano, así como sus riesgos y peligros.
- Establecer reglas claras: el comportamiento de los menores se modifica cuando saben que están bajo un marco de reglas y que, además, están siendo supervisados (esto variará según la edad).
- Mantener una buena comunicación familiar: esto facilita que los problemas tengan una forma más fácil de ser abordados cuando surgen y aumenta las posibilidades de colaboración mutua en entornos cercanos.
- Educar en conciencia y sensibilidad: es fundamental transmitir valores relacionados con el respeto por el otro, tanto para el

acosador como para quienes están al tanto y no actúan por miedo o desconocimiento.

- Enseñar a determinar las consecuencias de los actos: esto es crítico en general, pero, además, debe enseñarse a inferir qué información es verdadera o creíble y cuál no. También se les debe explicar que muchas conductas pueden llevar a consecuencias en el ámbito familiar, la escuela y, en el peor de los casos, a nivel social (delitos).

Grooming

El grooming implica el engaño de una persona adulta a un menor por medio de distintas vías de contacto, por lo general, con el objetivo de obtener imágenes de contenido sexual del menor, que luego el acosador utilizará para extorsionarlo. En una situación más extrema, el mayor intentará tener un encuentro personal con el niño, lo que puede tener consecuencias graves para su integridad física y psicológica. En pocas palabras, es un tipo de abuso sexual que se desarrolla, en principio, virtualmente. La relación generada pasa del engaño a la extorsión, bajo la amenaza de publicación de material obtenido o de difusión del material a amigos y familiares.

El grooming cae en la categoría de abuso como el ciberbullying, solo que en el primero existen propósitos de índole sexual, en tanto el otro caso se limita al ámbito social y no incluye esos fines.

El proceso del grooming atraviesa varias fases:

- Contacto: al inicio el adulto simula ser un menor de edad cercana a la edad de la víctima y busca crear lazos de confianza por medio de causas comunes, gustos, preferencias y cualquier otra supuesta coincidencia. En esta etapa no se produce violencia ni diálogos dudosos, por lo que el menor no suele sospechar. Por ejemplo, si la víctima es un niño, el

adulto puede hacerse pasar por una niña interesada en el niño o viceversa.

- Relación: el acosador obtiene acceso a información personal y familiar del menor, con lo que empieza el intercambio de confidencias, secretos e intimidades a fin de lograr el afecto o admiración por parte del menor. También se intenta generar una dependencia emocional que el niño puede confundir con empatía y amistad, lo que hace que no dude de su acosador. Por ejemplo, el acosador puede llevar al menor a entrar en una relación virtual de «amigovios».
- Acción: al ganar la confianza del menor, el acosador procede a la obtención de imágenes y videos de carácter sexual explícito, por medio de la cámara web o del teléfono celular. En esta instancia, el menor queda comprometido fuertemente con su acosador y le es muy difícil escapar. Luego de esto, el adulto podría concretar el abuso sexual o la agresión, lo que deriva en secuelas graves para el menor. Por ejemplo, el acosador puede incentivar al menor a encontrarse personalmente en algún lugar, yendo más allá de la relación virtual que venían manteniendo.

El proceso puede durar hasta varios meses. En general, el contacto inicial se da por medio de redes sociales, para luego pasar a medios más directos, como la mensajería instantánea. En algunos casos, el acosador obtiene la contraseña de alguna cuenta de e-mail o redes sociales de su víctima y la utiliza para manipularlo por medio de chantaje y extorsión.

Por lo general, los niños se dan cuenta de la situación cuando es bastante tarde, aunque para un adulto habría sido evidente la intención del interlocutor. Por esto, es recomendable que los primeros contactos que realice el niño en una red social estén

supervisados por un mayor, a fin de reducir el riesgo de contacto para fines de grooming.

Los síntomas que pueden manifestarse en el menor que es víctima de grooming son equivalentes a los mencionados para los casos de ciberbullying que ya fueron descriptos.

En cuanto a las maneras de combatir el grooming, se busca evitarlo de forma preventiva aumentando los esfuerzos para educar y entrenar a los niños en cómo detectar y reaccionar ante los posibles agresores, ofreciéndoles siempre un canal abierto de comunicación para esto y sin juzgarlos. Es recomendable aprovechar las situaciones en las que un caso de grooming aparece en los medios de comunicación para tomar el tema y hablarlo con los menores, de forma que puedan notar que se trata de un peligro real y no solo de una preocupación de sus padres.

Si la situación de contacto entre el menor y su agresor ya se produjo, es fundamental tomar acciones de inmediato, comenzando por hacer la denuncia a la entidad correspondiente. Debe recopilarse todas las pruebas posibles del contacto establecido, desde historiales de chat hasta capturas de pantalla, así como información del perfil de usuario del acosador y, sobre todo, proteger al niño de toda relación futura con este, dándole la tranquilidad de que no debe temer por su integridad y sin culpabilizarlo por los hechos ocurridos.

Sexting

Se le llama sexting al envío de contenidos de tipo sexual (fotografías y videos) generados a partir de teléfonos celulares o cámaras web y enviados por la propia persona a otra por algún medio de comunicación en internet (normalmente a través del teléfono celular, aunque es extensivo a cualquier otra vía).

El sexting es una práctica cada vez más común entre jóvenes y adolescentes, aunque también los adultos suelen estar envueltos en

ella. Sus orígenes datan del año 2005, cuando los sistemas de mensajería comenzaron a permitir el envío de contenidos visuales además de texto. Desde 2009 fueron apareciendo sitios web ilegales dedicados a recopilar y explotar comercialmente los contenidos sexuales de producción privada, muchos de los cuales provienen del sexting. De hecho, el Departamento de Justicia de Estados Unidos alertó desde un principio sobre el fenómeno del sexting, reconociendo que podía dar lugar a nuevos delitos.

La práctica del sexting implica desde riesgos psicológicos y legales hasta la posibilidad de que sea comprometida la integridad física de forma indirecta. Si bien en un principio puede parecer algo curioso y hasta divertido, cuando se toma fuera de contexto puede generar muchos perjuicios para los usuarios. Por ejemplo, gran cantidad de artistas y famosos se han visto envueltos en casos en los que videos o fotos que se habían producido en la intimidad llegaron a millones de personas. En ocasiones, no se toma conciencia en el momento porque no es fácil notar sus posibles consecuencias; pero pasado el tiempo, los resultados pueden ser dramáticos y avergonzar a quienes estuvieron involucrados. Las principales razones por las que se realiza sexting incluyen noviazgos, coqueteo, popularidad, presión, venganza e intimidación.

Dado que los jóvenes tienen tendencia a la curiosidad y la rebeldía, es importante conversar con ellos acerca de esta práctica, advirtiéndoles que el hecho de compartir fotos o videos en situaciones sexuales o sugerentes podría llegar a ser peligroso en un futuro para su identidad, ya que nunca se logra determinar en manos de quién puedan caer esas imágenes o videos y qué intenciones motivar a quien los posea.

Las recomendaciones respecto a la práctica del sexting son sencillas y evidentes: no producirlo, no compartirlo y no pedirlo. Hay que tener en cuenta que el solo hecho de producir el material ya es

un riesgo en caso de que el teléfono celular sea hackeado, perdido o robado. El riesgo se agrava mucho más cuando fotos o videos salen del teléfono hacia otro dispositivo (es enviado), ya que en ese momento el contenido dejó de estar bajo el control de quien lo creó. El receptor podrá compartirlo con otras personas voluntariamente, o incluso de manera involuntaria si su teléfono (u otro dispositivo) fuera hackeado, perdido o robado.

Los motivos por los que los jóvenes practican sexting dependen de varios factores:

- El hecho de creer que la foto o video estará segura en el teléfono celular o computadora del receptor, sin considerar posibles robos, pérdidas, bromas o hasta malas intenciones.
- La confianza en la discreción del receptor del contenido por falta de experiencia en la forma en que pueden comportarse las personas.
- La presión de los grupos de pertenencia para lograr destacarse o lograr notoriedad o aceptación en el período de la vida relacionado con el despertar de las prácticas sexuales.
- Los modelos sociales existentes y los medios de comunicación, lo que hace que no se perciba como algo de mayor gravedad por estar naturalizada la aparición y exhibición de desnudos por doquier.
- La falta de consideración de las consecuencias que puede traer a futuro para su vida, incluyendo el futuro lejano, cuando se transformen en adultos y busquen trabajo, tengan familia, etcétera.
- La falta de sensibilización ante el riesgo natural de la adolescencia y la actitud transgresora que la acompaña, lo que

deriva en que la práctica sea vista como un desafío o una diversión.

En suma, al sacarse una fotografía y enviarla a un contacto por medio de una red social o sistema de mensajería instantánea, como WhatsApp, Telegram o Snapchat, se pierde el control de ese material. Asimismo, al tomarle una foto a otra persona, es fundamental contar con su permiso y tener en cuenta las mismas cuestiones, especialmente por si llegaran a ser robadas o copiadas. El respeto mutuo, además, debe ser promovido y fomentado desde la familia y la escuela.

En caso de recibir –de forma privada o en un grupo de mensajería– una foto o video de otra persona (especialmente si es alguien que se conoce), no se debe colaborar en su difusión, para evitar las consecuencias que podría tener para ese individuo. Pensemos que cada uno de nosotros querría que los demás actuaran con la misma prudencia si la víctima fuéramos nosotros. Más allá de esto, tampoco debemos solicitar este tipo de fotografías o videos, ya que, aunque no tengamos malas intenciones, podríamos tener algún problema con nuestra computadora o teléfono celular y el material podría quedar en manos de terceros que ni siquiera conozcamos.

Como si esto fuera poco, el sexting puede ser causante de situaciones de acoso y extorsión a menores de edad para que el material no sea publicado, lo que es motivo suficiente para que no incurramos en la práctica y motivemos a los menores a que tampoco lo practiquen.

Contenidos inapropiados y mediación parental

Internet se nos presenta de manera libre y abierta, sin prohibiciones. Dependiendo de la edad del usuario, algunos contenidos podrían considerarse inapropiados (por ejemplo: imágenes y videos con desnudos, violencia, entre otros). El hecho de restringir un material puede ser complicado, ya que la limitación depende, por lo general, del dispositivo utilizado. De esta manera, si un menor accede desde otra computadora o dispositivo (ya sea mediante una conexión pública, de un amigo o de la escuela) no encontraría esas restricciones. En este sentido, no es posible aislar tan fácilmente a los menores de los contenidos inapropiados.

Algunos servicios incorporan filtros para que cuando se inicie una determinada sesión las restricciones se mantengan en el tiempo. Por ejemplo, los motores de búsqueda como Google y Bing cuentan con opciones de configuración para evitar que se muestren contenidos determinados (para adultos). Aun así, es posible que aparezcan ventanas emergentes mientras se navega, lo que puede ser producto del tipo de sitios web que se visita o de la existencia de algún tipo de programa malicioso en el equipo, por lo que es fundamental mantener el sistema libre de estos.

Lo apropiado o no de los contenidos dependerá de la madurez del niño, de su edad, de su educación, su religión y otros factores, por lo que solo existen unos pocos criterios universales. Finalmente, es importante instruir a los menores sobre qué hacer si llegan a visualizar contenidos inadecuados.

Por este y otros motivos es que se habla del concepto de mediación parental, definido como el proceso por el que los adultos acompañan al menor en su proceso de alfabetización digital, educándolo para que haga uso responsable de las nuevas

tecnologías, velando por reducir los riesgos y ofreciéndoles soluciones si estos llegaran a materializarse.

Se consideran básicamente cuatro estilos de mediación parental, cada uno con sus ventajas y desventajas en términos educativos: el estilo autoritario (normas rígidas y sin negociación), el estilo permisivo (con escaso control o exigencias), el estilo indiferente (poco implicado, desconociendo riesgos), y el estilo democrático (límites definidos en conjunto y búsqueda de la autonomía). En general, todo se trata de cómo se establecen los límites y normas, sobre los que se recomienda incluir los siguientes aspectos:

- Definir horarios y situaciones en los que se podrá conectar a internet, ya sea en un dispositivo u otro y tanto en la casa como fuera de ella. Aquí se tienen en cuenta los horarios de descanso, tareas escolares, actividades familiares y demás. También se contempla la cantidad de horas de conexión para evitar adicción o sobreexposición.
- Definir la edad a las que se permitirá tener un teléfono celular, tablet, computadora propia; y la edad a la que se le autorizará el acceso a internet, a las redes sociales, cuentas de correo electrónico y otros servicios. Esto obedece, en parte, al sentido común, y también al momento que se esté viviendo.
- Definir el software, juegos y sitios web a los que se aceptará ingresar según la edad, considerando que muchos contenidos informan la edad recomendada mínima de uso.
- Definir qué datos, imágenes y videos no deben subirse a internet, tal como se aclaró anteriormente.

Además, se les debe enseñar a los menores a no responder a provocaciones y malas maneras de los demás, y a la vez explicarles las posibles acciones ante esa situación (eliminar o bloquear

usuarios, por ejemplo). Finalmente, es importante promover el ocio no tecnológico para que no tengan siempre la sensación de que la única forma de entretenimiento y aprovechamiento del tiempo libre es mediante el uso de la tecnología.

El software que permite que el acceso a sitios web y otras acciones dentro del sistema pueda ser controlado y supervisado por un tercero (adulto) es justamente la herramienta de control parental. Esta se basa en el uso de dos métodos de filtrado. Por un lado, implementación de listas negras en donde se enumeren los sitios web que serán bloqueados, y, paralelamente, listas blancas donde figuren aquellos sitios a los que se pueda acceder. Por el otro lado, a través de la detección de palabras clave que permitan que se bloquee el acceso a sitios que cuentan con cierto contenido escrito.

Si bien hay distintas herramientas de control parental disponibles en el mercado, hoy en día los sistemas operativos más modernos (sean de teléfonos, tablets, computadoras o consolas de videojuegos) ya traen herramientas que incluyen la funcionalidad descripta anteriormente. También permiten la posibilidad de configurar límites de tiempo y horarios para el uso de un dispositivo, además de restricciones de qué aplicaciones se podrán usar, entre otras opciones. Estas herramientas son muy útiles y fáciles de utilizar; solo se debe investigar cuáles están disponibles según el sistema operativo de los dispositivos empleados.

Consejos para educadores

El educador moderno es, cada vez más, un guía en el proceso de aprendizaje antes que una referencia definitiva o una figura de autoridad en el conocimiento, lo que los obliga a adaptarse y a adquirir nuevas habilidades, entre las que se debe encontrar la comunicación de temas vinculados a los riesgos en el uso de la tecnología.

Para el caso de los colegios que tengan Informática o Computación como asignatura, debe instruirse a los profesores para que aborden las temáticas relacionadas con los riesgos del uso de las tecnologías, aprovechando los espacios en grupo para dialogar con los alumnos sobre los temas sensibles, estimulándolos a un debate e intercambio de ideas y opiniones.

En el caso particular de los adolescentes, es necesario transmitirles las consecuencias y responsabilidades que pueden devenir del mal uso de las tecnologías. Por ejemplo, actualmente la mayoría de las consultoras de búsqueda laboral y las áreas de Recursos Humanos de las empresas realizan búsquedas en internet y redes sociales durante el proceso de análisis de candidatos a un puesto de trabajo. Esto lo hacen, incluso, antes de una entrevista, a fin de comprobar si la persona –pese a lo que indique su currículum– tiene hábitos o comportamientos poco adecuados para el perfil que espera la organización. Por esto, es importante alentar a los jóvenes y adolescentes a que aprendan a cuidar su presente, porque en el futuro será parte de su pasado, y en muchos casos no podrán cambiar lo que hayan generado.

Por otra parte, un educador no puede desconocer ciertas cuestiones del uso de las redes sociales y otros espacios virtuales, como el manejo de las configuraciones de seguridad y privacidad,

las buenas prácticas de uso y sus funcionalidades básicas. Particularmente, Facebook cuenta con una serie de directivas y recomendaciones para adultos y docentes que pueden ser muy bien aprovechadas.

Hoy sabemos que la forma más efectiva de conseguir buenos resultados es la concientización y la sensibilización en vez del control, ya que, a medida que los menores aprenden a reconocer el riesgo, deja de ser necesario el control invasivo. Lamentablemente, esto no resuelve cuestiones de corto plazo, por lo que, en caso de estar sobre un problema puntual, deben tomarse medidas técnicas y continuar la concientización en simultáneo.

Para los docentes que suelen tener alumnos de la misma edad cada año, es recomendable mantenerse actualizados en cuanto al uso que ellos hacen de las tecnologías. También es fundamental hablar en las reuniones de padres sobre los riesgos que estas acarrean, a fin de que las reglas y principios generales puedan estar lo más alineados posible entre el hogar y la escuela, al tiempo que permite alertar a muchos padres que no tienen conocimiento de los peligros existentes.

Es importante respetar la privacidad de los alumnos en caso de que la institución utilice software de monitoreo de actividades, ya que las mejores relaciones que se pueden establecer con los menores están basadas en la confianza y no en la autoridad o el poder.

Se debe promover entre los alumnos la práctica del respeto mutuo a fin de prevenir casos de bullying que puedan afectar su integridad y autoestima, haciéndolo extensivo al trato online.

Para aquellas escuelas o instituciones educativas que no cuenten con políticas formales de uso de la tecnología, es bueno poner el tema en la agenda de las autoridades y de los demás docentes para fomentar su uso prudente.

En definitiva, la escuela es un entorno que define –en buena medida– la vida de los niños, por lo que todo aquello que se les pueda enseñar y transmitir durante su paso por ella jugará un rol importante en su futuro. Por sobre todas las cosas, debemos tener siempre presente que la mejor forma de enseñar es a través del ejemplo. En este sentido, las recomendaciones para educadores coinciden en gran medida con las que se aplican a los padres, por lo que es importante tenerlas en cuenta.

Importante recordar

- No negarles a los menores el acceso a internet ni el uso de dispositivos, ya que no conviene privarlos de conocer y disfrutar de un medio de comunicación y aprendizaje tan vasto, y que al utilizarlos están adquiriendo nuevas habilidades que serán clave en su desarrollo para el futuro.
- Es recomendable controlar qué hacen nuestros hijos cuando navegan en internet sin invadir su privacidad; para ello conviene utilizar herramientas de control parental, en especial para niños pequeños.
- Los menores pueden conocer más que un adulto de cierta tecnología, pero no sobre los riesgos en internet, por lo que se les debe transmitir como parte de su educación.
- Regular el tiempo que están frente a los dispositivos e internet.
- Enseñarles a los menores sobre el uso prudente de la mensajería instantánea y redes sociales; pedirles que informen acerca de cualquier ocurrencia de acoso o pedidos que no sean de su agrado o que les resulten extraños.
- Motivar a los adolescentes a evitar toda forma de sexting y circulación de material de contenido privado. Esto implica sus tres aspectos: no producirlo, no compartirlo y no pedirlo.
- Transmitirles a los niños y adolescentes que deben aprender a cuidar su presente, porque en el futuro será parte de su pasado, y si ese pasado se encuentra en internet, cualquiera podrá revisarlo.

- No debemos olvidar que el principal ejemplo para los menores somos los adultos, por lo que es importante que nuestras acciones en redes sociales –donde pueden vernos nuestros hijos– sean consistentes con lo que les transmitimos.
- Instruir a los menores a no compartir información que pueda identificarlos, especialmente direcciones, teléfonos, colegios e instituciones, entre otros.
- Evitar promover en los menores la realización de operaciones monetarias en internet hasta que, en base a su edad, estén capacitados para realizarlas sin riesgos.
- Mantener el diálogo abierto en el entorno familiar y escolar en cuanto a las experiencias de los menores en internet y lo que ven cotidianamente.
- Colocar la computadora en un área común de la casa en lugar de ubicarla en el dormitorio del niño, para que su uso pueda ser supervisado con facilidad (especialmente el de los más chicos); además, garantizar que la cámara web esté desconectada cuando no sea necesaria.
- Crear usuarios para los menores y no permitirles la utilización de usuarios administradores en ningún software ni sistema que manejen, dejando esto para un adulto.
- Configurar a conciencia las opciones de privacidad y seguridad en las redes sociales que utiliza el niño.

Capítulo 8

Qué hacer si nos hackean

Aunque interactuemos de forma preventiva, posiblemente en algún momento suframos un incidente o seamos hackeados por un hacker malicioso. En estos casos, es necesario saber qué hacer y cómo comportarse para evitar que el problema sea aún mayor.

En este capítulo veremos cómo actuar ante diversas circunstancias de este tipo.

Los delitos informáticos

Sabemos que la ley y la tecnología no se han llevado bien históricamente, más aún con el crecimiento exponencial de esta última, separando la brecha más fuertemente. Es difícil todavía hacer que un problema de índole personal común llegue a la justicia, pero existen algunos canales que es bueno conocer con antelación. Por este motivo es importante conocer primeramente cuáles son los delitos informáticos que podemos considerar.

En líneas generales y de forma breve, se entiende por delito informático cualquier acción en contra de los principios de la seguridad de la información (confidencialidad, integridad y disponibilidad) que afecten sistemas, redes y datos. Existen distintos tipos de delito informático según aquello que afecte:

- Delitos en contra de los principios de la seguridad sobre datos y sistemas: esto es, por ejemplo, el acceso no autorizado a sistemas informáticos, la intercepción de datos en redes de comunicaciones, la interferencia en el funcionamiento de un sistema, o el abuso de dispositivos y equipamiento que facilite la concreción de un delito.
- Delitos vinculados al contenido: esto es, por ejemplo, la producción, oferta, difusión o adquisición de contenidos prohibidos a través de un sistema informático, o la posesión de contenidos de esa naturaleza en sistemas o medios digitales de almacenamiento.
- Delitos de fraude informático: esto es, por ejemplo, la falsificación mediante la introducción, eliminación de datos

informáticos y el fraude mediante la introducción, alteración o eliminación de datos, o la interferencia en sistemas.

- Delitos relacionados con la propiedad intelectual: esto es, por ejemplo, la copia y distribución de software, y la piratería informática en general.

Esta clasificación de delitos proviene del Convenio de Ciberdelincuencia del Consejo de Europa, firmado en 2001. Posteriormente, se promulgó un protocolo adicional (2008) a fin de incluir actos de racismo y xenofobia a través de medios informáticos, incluyendo entre otros la difusión de material xenófobo o racista, los insultos o amenazas con motivación racista o xenófoba, y la negociación, minimización, aprobación o justificación del genocidio o de crímenes de lesa humanidad.

Con estas conceptualizaciones como guía, podemos determinar si un comportamiento o acción está enmarcado dentro de lo que es considerado delito según la ley, y por esto es tan importante tenerlo en cuenta, ya que muchas veces estamos frente a delitos sin darnos cuenta.

Es importante tener en cuenta que cada país tiene distintas leyes relacionadas a los delitos informáticos, como así también definiciones de lo que se considera delito de este tipo. Debido a esto, es importante que cada uno investigue las leyes de su país o consulte con un especialista en la materia.

Cómo reaccionar ante los delitos informáticos

Luego de haber comprendido este tipo de delitos, debemos saber qué hacer en un caso real. Ante todo, y según lo recomendado por las entidades idóneas, debemos tener en cuenta algunas acciones importantes que no podemos olvidar:

- Los NO: no eliminar ni reenviar. Es decir, no borrar ni destruir o modificar la información relativa al incidente, a fin de garantizar al máximo la integridad de esa información. Nunca reenviar mensajes constitutivos del delito, como correos electrónicos y de mensajería instantánea.
- Los SÍ: denunciar y guardar. Es decir, realizar lo antes posible la denuncia ante la dependencia policial más cercana al domicilio (comisaría) o en una fiscalía, teniendo en cuenta que esta tiene la obligación de tomar la denuncia; se recomienda presentar allí todas las pruebas posibles, además de guardarlas para su correcta protección. Por supuesto, luego de realizada la denuncia, se deberá proceder como el investigador de la causa lo indique.

Estos consejos tienen como objetivo evitar que el usuario reaccione de forma incorrecta y están pensados para facilitar la tarea de los investigadores, los abogados y el personal policial, ya que tienen en cuenta los principios básicos de los procedimientos de investigación.

Luego de seguir estas recomendaciones básicas, debemos acudir a las autoridades correspondientes según el tipo de delito y la zona geográfica, lo que depende del país y ciudad.

Servicios gratuitos y sus limitaciones

Muchos de los servicios que utilizamos en internet son gratuitos desde el punto de vista económico (es decir, no debemos pagar por ellos con dinero), pero no lo son tanto con respecto a la información personal. Estamos «pagando» esa gratuidad económica con información sobre nosotros, nuestros hábitos y nuestras preferencias, lo cual luego es vendido a terceros o utilizado para ofrecernos servicios y productos. Como ejemplo de esto tenemos muchos de los mismos servicios que mencionamos a lo largo del libro, como el correo electrónico de Gmail, Microsoft Outlook o Yahoo! Mail, sus buscadores asociados (Google, Bing y Yahoo!), las redes sociales como Facebook, Twitter, Instagram, Pinterest o LinkedIn, sistemas de mensajería y comunicaciones como WhatsApp y Telegram, y plataformas como YouTube y Spotify, entre otras.

Desde el punto de vista de la seguridad, entonces, se recomienda no proveer demasiada información a las empresas que ofrecen estos servicios, de manera tal que nuestra privacidad no se vea tan comprometida en el futuro.

Podemos notar que antes de comenzar a utilizar estos servicios se nos presentan los términos y condiciones que debemos aceptar para acceder a su uso. Dicho texto (generalmente largo, para desalentar su lectura) incluye los detalles sobre cómo serán tratados nuestros datos, para qué se los podrá utilizar y todos los consentimientos que estamos dando al aceptar el uso del servicio en cuestión. Es recomendable leerlos –incluso si ya hemos recurrido hace tiempo a tal servicio– para conocer los alcances y límites sobre lo que la empresa explica respecto a la privacidad de sus usuarios.

En este punto sería interesante preguntarnos qué sucedería si, de un día para el otro, cualquiera de estos servicios cambiara sus condiciones o términos de uso, si decidieran cobrar por funcionalidades que eran gratuitas o, en el peor de los casos, si dejaran de brindarnos su prestación por cualquier motivo. Situaciones como estas han ocurrido en algún momento con grandes empresas y servicios, y que por su envergadura no parecía que pudieran modificar estos aspectos, mientras los usuarios suponían que las mantendrían por mucho tiempo.

Dado que no sabemos cuál será el futuro de las empresas en cuestión, conviene hacer algún ejercicio mental que nos permita plantear escenarios posibles. Por ejemplo, podemos preguntarnos: ¿qué pasa si mañana no puedo acceder más a este servicio? Si la respuesta implica que tendremos muchos problemas, deberemos tener siempre copia de seguridad de la información que guardamos en ese servicio para no extraviarla ante una eventual pérdida de acceso al servicio. La recomendación es aprovechar la funcionalidad de copia de seguridad de perfiles que poseen algunos servicios, los cuales permiten descargar un paquete de archivos con el contenido de todo lo que hayamos generado sobre esa plataforma.

Adicionalmente, debemos saber que los servicios en internet operan según la ley de su país de origen, por lo que –ante cualquier problema– todo estará sujeto a estas y no a las que rigen en nuestro país.

De haber sufrido un robo de nuestra cuenta o perfil de algún servicio, hay que acudir a su prestador a través de los canales provistos por este para tener alguna posibilidad de recuperarlos. Por ejemplo, supongamos que perdimos acceso (por un robo de cuenta) a nuestro correo electrónico y nos contactamos con la empresa mediante algún formulario de contacto, teléfono o e-mail de soporte. Al respondernos, nos solicitarán información personal de la cuenta –

como la fecha de creación estimada, el contenido de los últimos correos electrónicos, remitentes conocidos, nombres de carpetas, reglas existentes, etiquetas y datos personales– a fin de verificar si somos realmente el dueño y no un impostor que se hace pasar por nosotros. Al ser un servicio gratuito, las posibilidades de que nos respondan rápido y que obtengamos una buena solución son bajas, ya que los pedidos que reciben son innumerables.

En algunas redes sociales y servicios online están comenzando a tomarse medidas que incluyen la asignación de un segundo usuario administrador del perfil o la provisión de doble factor de autenticación para evitar la usurpación y también permitir la recuperación de nuestra cuenta. Es recomendable aprovechar tales medidas siempre que estén disponibles, a fin de aumentar nuestras probabilidades de recuperación de cuentas en caso de que nos suceda algo indeseable.

Qué NO hacer

Decenas de veces me ha sucedido que personas que me conocen, o incluso desconocidos, me consultan si podría hacerles «un favor» porque los han hackeado o se han olvidado la contraseña de un servicio y no pueden ingresar y quieren que los ayude a recuperar el acceso «de alguna forma». La mayoría desconoce que ese favor que solicitan es algo ilegal si no se realiza por los medios que dispone el proveedor de ese servicio. Incluso en el caso de las cuentas que son hackeadas, si uno sabe quién lo hizo o quiere saber quién fue, tampoco se debe recurrir a medios ilegales para hacerlo y recuperar la cuenta, ya que estaría exponiéndose a una serie de inconvenientes de índole legal. Por lo tanto, algo que no debe hacerse nunca es utilizar el hacking ilegal para recuperar o lograr acceso a un servicio si no se quiere tener problemas con la justicia.

Hay que tener presente que si ingresamos sin autorización a la cuenta de cualquier servicio (e-mail, Facebook, Instagram, etcétera) que no sea nuestro estamos haciendo algo ilegal y podemos meternos en serios problemas. A veces esto sucede con parejas o exparejas; uno de los dos accede a un servicio del otro sin autorización (es común en separaciones y divorcios problemáticos), lo que puede terminar con una denuncia, sumado a las consecuencias que ello acarrea.

Una vez, un conocido me llama para contarme (bastante perturbado y avergonzado) un incidente que había tenido; alguien le había hackeado su computadora y robado fotos comprometedoras, y le pedía dinero a cambio de no publicarlas. Esta persona estaba muy preocupada ya que, aunque le pagara al extorsionador, nada podía garantizar que no las publicara de todas maneras. Al tratarse de un reconocido empresario, si esas fotos

se hacían públicas, era consciente del gran impacto que eso tendría en su vida, causándole muchísimos problemas.

Desesperadamente me solicitó si podía hacerle el favor de hackear la computadora de la persona que lo estaba extorsionando y borrar todas las fotos comprometedoras. Pero, aunque lo que había hecho la otra persona era ilegal, no podía hacer eso que me pedía, porque también era ilegal, y quien tendría inconvenientes sería yo. Le recomendé que hiciera la denuncia a la policía y que no tuviera fotos comprometedoras en ningún dispositivo para evitar futuras situaciones similares. Al final, parece que tuvo que pagarle al chantajista, quien, afortunadamente, nunca publicó las fotos.

Importante recordar

- Debemos conocer los actos relacionados con la informática que se consideran ilegales en el país en el que nos encontremos, ya que, de lo contrario, podríamos estar cayendo en una acción contemplada por la ley como delito sin saberlo.
- En caso de estar ante un delito informático, hay que realizar, lo antes posible, la denuncia en la dependencia policial o fiscalía más cercana al domicilio, y no olvidar guardar todo aquello que pueda servir como prueba.
- No eliminar ni reenviar información relativa a un incidente, como correos electrónicos o mensajería instantánea.
- Evitar, en la medida de lo posible, proveer demasiada información a las plataformas de servicios web, redes sociales y demás para preservar al máximo nuestra privacidad.
- Leer los términos y condiciones de uso de los servicios que más frecuentamos para conocer sus alcances y el manejo que pueden hacer de nuestros datos.
- Aprovechar la funcionalidad de copia de seguridad de perfiles de los servicios y redes sociales que la ofrecen para tener un resguardo de la información de nuestras cuentas en caso de sufrir un problema grave.
- Activar la mayor cantidad de medidas de seguridad que ofrecen los servicios online, como los factores adicionales de autenticación, la provisión de datos de recuperación y la

asignación de un usuario alternativo de administración, entre otras.

- No hay que confiar en que la ley protegerá nuestras cuestiones de privacidad; hay que tomar un rol activo en la prevención y la protección contra cualquier tipo de incidente.

Capítulo 9

Inteligencia artificial

Desde hace décadas, el concepto de inteligencia artificial (IA) fascina a la gente, ya que es donde el ser humano intenta reproducir la forma en que trabaja su propio cerebro. Las grandes capacidades de procesamiento y almacenamiento que nos ofrece la tecnología hicieron que la IA pudiera ir más allá de lo imaginado, al punto que hoy existen aplicaciones como ChatGPT que, de una forma u otra, pueden «pensar», sacar conclusiones, crear texto, imágenes, sonidos y videos a partir de la información provista.

La IA actual utiliza los llamados modelos de lenguaje grande (*large language models*), los cuales procesan, entienden y generan texto similar al humano. Estos modelos son entrenados con grandes cantidades de datos, con los cuales se identifican patrones y aprenden para luego poder predecir y generar texto de manera similar al humano. Es importante destacar que la IA actual no entiende como un ser humano, sino que simula comprender en base a patrones que ha identificado durante su entrenamiento. Por otro lado, tenemos los llamados modelos de difusión (*diffusion models*), que son entrenados con grandes cantidades de datos visuales

(imágenes, videos) y sonoros (sonidos, música). Estos modelos son los utilizados para la creación de imágenes, videos, sonidos y música.

Estos modelos descriptos trabajan en conjunto y forman parte de lo que se conoce como inteligencia artificial generativa, la cual permite generar textos, imágenes, videos y música nuevos a partir de datos de entrenamiento simulando creatividad humana.

Constantemente se producen nuevos avances en IA y también nuevas aplicaciones, lo cual contribuye a que cada vez sea más utilizada esta tecnología, tanto en el ámbito personal como en el de las empresas, para distintos tipos de tareas, que van desde lo más sencillo hasta lo más complejo.

La IA puede aplicarse a problemas concretos y puntuales e incorporarse como un software que va «aprendiendo» de las acciones del usuario, de los datos que recopila o de cualquier entrada de información que se le provea. Actualmente la IA está inserta en las distintas soluciones tecnológicas que utilizamos en nuestra vida diaria, siendo algo transparente para nosotros, como ser en Siri en dispositivos de Apple y Alexa en tecnología de Amazon. También plataformas de streaming como Netflix y Spotify usan IA para aprender de nuestros hábitos y hacer recomendaciones personalizadas de música. Las redes sociales también utilizan IA para mostrarnos contenidos que determinan lo más relevante para nosotros, basados en nuestros gustos, que aprende de todos los datos que recopila cuando usamos estas mismas redes. Podemos afirmar que hoy la IA ya está integrada en nuestras vidas ya que es un componente importante de la tecnología que utilizamos diariamente.

Los riesgos

Si bien podría pensarse que la IA no implica riesgo alguno, debemos entender que las tecnologías son solamente herramientas y que el uso que se les da depende exclusivamente de la intención de las personas.

Así como la IA potencia personas y empresas para realizar más cosas en menor tiempo y de mejor manera, lamentablemente, también puede potenciar lo malo cuando alguien con malas intenciones tiene al alcance y disposición herramientas de IA. Debido a esto, varias de las amenazas descriptas en este libro se pueden potenciar y ser aún más peligrosas. Por ejemplo, los ataques de phishing pueden ser más automatizados, masivos y personalizados, siendo mucho más difíciles de detectar debido a que los engaños se asemejan mucho más a lo real; o el uso de *deepfakes* o *fakes* (falsos), en los que se utiliza IA generativa para crear videos, audios o imágenes falsas de una persona de manera súper realista. Con solo proveer una imagen de una persona o una muestra de su voz grabada, se puede construir distintos contenidos multimedia (audio, imagen, video) cuya falsedad es cada vez más difícil de detectar. Esto tiene un buen uso y lo vemos aplicado en el mundo del entretenimiento, como ser en series, películas, etc., y en el marketing, en las publicidades, por ejemplo, pero también tiene un mal uso cuando lo que se busca es engañar haciendo pasar como real el contenido multimedia generado. Debido a esto, es común que en las redes sociales circule este tipo de material multimedia para engañar a la gente y generar controversias y discusiones. Esto también se puede utilizar para estafas y robo de información, ya que las víctimas, al recibir un mensaje de voz, videollamada o llamado telefónico, al pensar que se trata de alguien conocido, puede ser

engañada y proveer información sensible (nombre de usuarios y contraseñas, códigos, etc.), así como realizar acciones que la terminen perjudicando de alguna manera, como transferir dinero o criptomonedas, etc. Este es un nuevo tipo de amenaza, facilitado por la IA, del cual tenemos que saber cómo protegernos. Lo mejor que podemos hacer al recibir algún mensaje de audio, videollamada o llamada telefónica de alguna persona que conocemos, pero que nos pide algo fuera de lo común o si notamos algo raro, es preguntar algo que solo esa persona y nosotros conozcamos, o algo que no sea público o fácil de conocer. Por ejemplo, el audio o video es de un primo que nos solicita urgentemente dinero; podemos preguntarle: «¿te acordás la última vez que nos vimos, cuándo fue?». De esta forma, si no es nuestro primo real, no sabrá cómo respondernos y podremos identificar el engaño. Otra opción es tener palabras secretas entre familiares, así cuando se comunican uno puede preguntar por esa palabra secreta para asegurarse de que realmente sea su familiar y no un *deepfake*.

A principios de 2024 ocurrió un grave incidente que terminó con un robo de 25 millones de dólares a una empresa de Reino Unido. Un empleado de la empresa de la sede de Hong Kong fue engañado a través de una videollamada donde se le solicitó que transfiriera de forma urgente 25 millones de dólares a un par de cuentas bancarias para poder realizar un importante negocio. Como en la videollamada el empleado vio a uno de los directivos de la empresa y a colegas suyos, no sospechó que se trataba de un engaño y procedió a transferir el dinero. Luego se supo que criminales habían realizado un sofisticado ataque utilizando *deepfake* para verse igual a empleados reales de la empresa en la videollamada, generando confianza y engañando a la víctima para que transfiriera el dinero a las cuentas de los criminales.

Los desafíos

En un futuro cercano algunos sistemas que usan IA podrían tomar decisiones en forma autónoma, y en caso de haber algún error, tales determinaciones podrían llegar a originar problemas, incluso de importante gravedad. Por ejemplo, si un sistema de IA es utilizado para organizar el aterrizaje de aviones en un aeropuerto, cualquier error –por más pequeño que sea– podría ocasionar una tragedia.

Algunas incógnitas del tipo filosóficas surgen respecto al uso de la IA, como si alguna vez las máquinas podrán pensar mejor que el ser humano, lo que algunos expertos dicen que podría ocurrir en los próximos años.

Algo preocupante es la falta de ética, empatía y distintas emociones humanas en la IA, que puede llevar a que esta opere de manera extrema y perjudicial para el ser humano por carecer de esas emociones. Las decisiones que toma la IA siempre tienden a optimizar resultados de la mejor manera posible y de esa forma cumplir con su objetivo. Entonces, al carecer de emociones humanas puede pasar, por ejemplo, que ante un problema de hambre por escasez de alimentos decida que la mejor forma de solucionarlo es reduciendo la cantidad de humanos, en vez de buscar cómo producir más comida.

Otro punto controversial es el uso militar de la IA. Con el rápido crecimiento de la aplicación de la última tecnología en armas cada vez más autónomas (o sea, que no son directamente manejadas por personas) –como drones, tanques, robots, etcétera–, el agregado de IA para hacerlas completamente independientes podría llegar a ser catastrófico, porque, de esta manera, se decidiría en forma automática sobre las vidas de las personas. Actualmente hay varios

expertos que se oponen al uso de la IA para lo militar debido a las posibles graves consecuencias.

Probablemente en el futuro, mucha de nuestra interacción con el mundo pase a través de un sistema de IA, y seguramente ni lo notemos, aunque quizás no sea conveniente dejar que nuestro esfuerzo por pensar sea reemplazado cada vez más por lo que un sistema puede hacer. Un caso que ilustra esto es la utilización de las calculadoras de mano, que facilitaron la realización de cuentas matemáticas reemplazando otras técnicas que, pese a ser más lentas, tenían la ventaja de que «obligaban a pensar». Hoy nadie negaría el uso de una calculadora, pero el hecho de que hayamos perdido parte de la capacidad de hacer ciertas operaciones matemáticas es, tal vez, un terreno perdido, y desconocemos el impacto que tendrá. Al ir cediendo terreno a la IA para que resuelva todos nuestros problemas, además de volvernos más dependientes, posiblemente iremos relegando, cada vez más, nuestra capacitad intelectual.

Otra de las discusiones acerca de la IA es que reemplazar las tareas que son ejecutadas por personas implicaría un impacto considerable en el mercado laboral, dejando a muchos sin trabajo y obligándolos a adquirir nuevas competencias profesionales para permanecer competitivos y encontrar nuevas ocupaciones.

El tiempo dirá si la IA termina siendo más beneficiosa para la humanidad, o generará problemas más graves que los que soluciona.

Importante recordar

- La IA es una tecnología muy útil que nos permite hacer cosas antes impensadas.
- La IA ya está integrada en nuestra vida ya que la tecnología que utilizamos a diario utiliza IA.
- Como toda herramienta, la IA puede usarse para bien o para mal.
- Lamentablemente, la IA potencia las amenazas descriptas en este libro haciéndolas más peligrosas.
- Los *deepfakes* son una nueva amenaza de la cual debemos aprender a protegernos.
- La IA carece de emociones humanas, por lo tanto, al tomar decisiones, podría elegir algo perjudicial.
- Darle mucha autonomía a la IA podría ser muy peligroso, especialmente en el ámbito militar.

Capítulo 10

Amenazas (no tan) futuras

Las nuevas tecnologías incluyen riesgos inherentes a su uso, y debemos conocerlos, estudiarlos y prevenirlos, porque, en mayor o menor medida, ya están apareciendo entre nosotros. Algunas presentan grandes desafíos, y otras no tanto, pero es importante conocer los peligros que acarrean; ya son aplicadas en múltiples contextos, y pronto pasarán a formar parte de nuestra cotidianidad.

Realidad aumentada

La realidad aumentada es una de las herramientas de las cámaras digitales incorporadas en los dispositivos móviles que, gracias a su alta capacidad de procesamiento, pueden agregar información a un espacio o elemento que está siendo captado. Consecuentemente, si apuntamos la cámara de nuestro teléfono celular para que capte la calle que transitamos, a través de esa función una aplicación puede agregar información de los comercios en esa calle y resaltarla sobre la imagen que nos brinda la pantalla en tiempo real.

Las aplicaciones son innumerables y están principalmente asociadas a mejorar la experiencia de usuario. Por ejemplo, en ámbitos educativos, un libro de texto o una imagen podría darle más información a un estudiante e incluso modificarla en otros momentos o para las distintas personas que lo visualicen. Lo que se busca es que nuestra percepción contextual se incremente, mejorando nuestras posibilidades de interactuar y teniendo más datos al respecto.

Tal como podemos suponer, al tratarse de la combinación entre mecanismos de sensado y el software que interactúa con ellos, también podrían ser objetivos de potenciales atacantes, los cuales –mediante acciones ofensivas– podrían hackear las aplicaciones y los dispositivos, alterando así lo que el usuario recibe como información. Esto podría ser sencillo y no afectar la integridad de la víctima, o también complejo y llevar a un nivel de gravedad alto a la persona.

Por ejemplo, el parabrisas inteligente de un vehículo (que de por sí cuenta con varios sistemas informáticos y computarizados) está programado para ofrecer información agregada sobre distancias, carteles, interpretación de sucesos, clima, velocidades y frenado,

entre otras. Pero si un atacante modificara su comportamiento, estaría en peligro la vida de quienes viajan en el vehículo, ya que actuamos basándonos en la información que recibimos; por lo tanto, si esa información fuera falsa, tomaríamos decisiones equivocadas que podrían tener consecuencias de distinta gravedad.

Realidad virtual

La realidad virtual implica el uso de la tecnología para producir una experiencia que permita a la persona tener la sensación de estar presente e inmersa en esa realidad aparente simulada por computadora. Dicha tecnología se basa en la experiencia visual y auditiva, aunque también puede agregar movimiento y sensaciones olfativas.

Esta tecnología avanzó mucho en los últimos años, ayudada por los teléfonos celulares, que, de forma básica, han permitido acceder a sus experiencias mediante el uso de dispositivos sencillos.

La realidad virtual está principalmente provista por un casco o anteojos que la persona se coloca y que le permiten sentirse inmerso en ese universo y aislado del entorno. Las experiencias pueden ser realmente fascinantes y cada día se avanza más en ese sentido, al punto que existen aplicaciones para celulares y cientos de videos subidos a YouTube que tienen la posibilidad de ser reproducidos en dispositivos de realidad virtual simples, como los llamados *cardboards* (anteojos con armazón de cartón), que están al alcance de todos.

Los riesgos derivados de la realidad virtual son los relativos a la posibilidad de que el dispositivo que la provee sea transformado por un hacker malicioso y pase a modificar la experiencia del usuario, especialmente en aquellos equipos a los que se puede acceder por medio de conexiones inalámbricas como wifi o bluetooth. Estas alteraciones podrían ser tan sutiles que el usuario podría no darse cuenta de que está siendo intervenido y ser víctima de contenidos explícitos que modifiquen los resultados de la experiencia.

Holografía

La holografía es una técnica fotográfica que se basa en la creación de imágenes tridimensionales utilizando la luz. La forma básica de holografía consiste en grabar con un láser una película fotosensible que, al ser iluminada de la manera adecuada, proyecta una imagen que se percibe en tres dimensiones. Esta técnica fue inventada en 1948, y evolucionó hasta nuestros días, permitiendo, cada vez más, características y usos como el entretenimiento, la educación y todo contexto en el que una proyección tridimensional pueda servir para agregar información al entorno.

Con los hologramas en 3D, es enviar una proyección de nuestra imagen tridimensional, tal como hoy lo hacemos con el video en dos dimensiones. También puede llevarse la experiencia al usuario que visualiza, como sucede con el dispositivo Microsoft HoloLens, el cual permite ver en 3D objetos que no están realmente allí, combinando realidad aumentada con un dispositivo *wearable* más la técnica de la holografía.

Los riesgos asociados van en la misma línea que otros ya mencionados: la posibilidad de que los dispositivos sean hackeados para alterar su funcionamiento, haciendo que se proyecten imágenes distintas a las que se desean, cambiando lo que el usuario ve. Nuevamente, algunas alteraciones podrían ser inocentes, pero otras podrían poner en riesgo la salud o la vida de las personas. Por ejemplo, si la holografía es utilizada para representar a una persona real en una operación quirúrgica realizada a distancia mediante un robot, cualquier problema con la imagen holográfica podría costarle la vida al paciente, ya que los médicos estarían viendo una imagen incorrecta, lo que los llevaría, posiblemente, a cometer errores.

Dado, entonces, que esta tecnología será otra de las que tendremos a nuestro alrededor en los próximos años, no debemos dejar de considerar la seguridad a nivel de su software y su hardware, y exigirles a los fabricantes que realicen diseños que cumplan con estándares de seguridad adecuados.

Tecnología *wearable*

La miniaturización de la tecnología llegó en los últimos años a un punto difícil de creer para aquellas personas ajenas a los avances tecnológicos. Esa mayor portabilidad inauguró una nueva tendencia: la tecnología «vestible» (*wearable*) implica que se incorpora en nuestra vestimenta para adicionar algún beneficio. Los dispositivos se clasifican normalmente en: salud, deporte, entretenimiento, industriales y militares.

Así aparecieron los smartwatches (relojes inteligentes), que pueden comunicarse con el teléfono móvil para complementar y ampliar sus funciones; el calzado deportivo con capacidad de proveer estadísticas del ejercicio físico y conectarse con el reproductor de música para ajustar los ritmos; las mochilas y camperas con celdas solares que actúan como baterías para recargar otros dispositivos, y los lentes que proveen información adicional al campo visual, entre otros tantos desarrollos tecnológicos.

Como en el caso anterior, los riesgos existentes pueden provenir de las malas intenciones de hackers o de las fallas de los dispositivos. Es decir, si contamos con una determinada funcionalidad de una prenda, por ejemplo, y esta falla sin que tengamos una alternativa, nos veremos perjudicados de distintas formas.

También podría ocurrir que un dispositivo sea hackeado y se comporte de manera errática o bajo el control de otra persona, quien podría enviar información falsa haciendo que responda según su conveniencia para alterar la experiencia de uso. Esto se torna más grave a medida que tales dispositivos incluyen mayores capacidades de procesamiento y la posibilidad de conectarse de

forma inalámbrica con otros –e incluso a internet–, lo que funcionaría como un canal de acceso para ser atacado remotamente.

En definitiva, siempre tenemos ventajas al usar tecnologías que facilitan nuestras actividades o complementan las tareas cotidianas, pero no debemos olvidar que cuanto más tecnológicas sean las prendas y accesorios que utilizamos, más probabilidades existen de ser susceptiblemente afectados por un hacker malicioso y por problemas de seguridad.

Un caso particular que merece ser ampliado respecto de los *wearables* es el de los dispositivos biomédicos tecnológicos, que en algunos casos se utilizan adosados al cuerpo por fuera (como sensores de caídas, registradores de pulsaciones cardíacas, dispensadores de insulina) y otros por dentro, a través de intervenciones quirúrgicas que los insertan (como los marcapasos cardíacos o los cardiodesfibriladores internos). Estos, tal como los demás, podrían ser atacados por hackers maliciosos para provocar su mal funcionamiento y poner en peligro la vida de la persona. De hecho, aunque parece de película, ha sido demostrado que los marcapasos electrónicos pueden ser hackeados remotamente y provocar un ataque cardíaco al paciente. Es por esto que un exvicepresidente de Estados Unidos ha ordenado deshabilitar la función de acceso inalámbrico a su marcapasos para evitar la posibilidad de que un hacker lo ataque y hasta pueda matarlo.

Robots y nanorrobots

La idea que las personas tienen de los robots está mucho más asociada a las máquinas con forma humana que a lo que la tecnología realmente ha creado hasta el momento. Un robot es cualquier máquina o entidad electromecánica o virtual que permite realizar alguna tarea de forma automatizada. Por ejemplo, las fábricas utilizan máquinas robotizadas para ensamblar productos y, en un ámbito más personal, las aspiradoras robóticas permiten recorrer un espacio físico de forma automática para realizar la limpieza. Esto está muy vinculado a la IA, ya que se intenta combinar la automatización, la repetitividad de las acciones y la capacidad de tomar decisiones.

Quizás la pregunta más formulada en la historia de la robótica haya sido: ¿qué pasaría si los robots pudieran realmente pensar por sí mismos? Lo cierto es que no lo sabemos, aunque hay quienes han propuesto que se podrían volver en contra del hombre, su creador. La literatura de ciencia ficción y el cine se han encargado de crear escenarios futuristas nada buenos para el ser humano, que sirven de ilustración de lo que podría suceder.

En un futuro, es probable que los robots «personales» que brindan asistencia a la gente tomen más relevancia en nuestras vidas, y en ese momento deberemos preguntarnos cuánto estamos dependiendo de una tecnología cuyo funcionamiento no comprendemos y que, como en otros casos, solo los especialistas pueden crear, modificar, programar y reparar. Esto sin contar la posibilidad de que un hacker malicioso tome control sobre los robots, acceda remotamente a sus componentes, los reprograme y les haga causar daños a personas y cosas. Habría que preguntarse seriamente si confiaremos en la tecnología tanto como para dormir

con los robots encendidos o si los apagaríamos para dormir tranquilos.

El uso de robots también está creciendo en el ámbito de la seguridad (sea policial, militar u otro), la medicina, la industria, el entretenimiento, el hogar, etcétera, lo que indica que nuestra dependencia de la robótica irá creciendo continuamente y pronto los robots se volverán muy comunes.

Hace un tiempo, junto con mi colega Lucas Apa realizamos una investigación sobre varios robots y descubrimos que son muy inseguros y fáciles de hackear. De continuar la falta de seguridad en los robots, podría tener graves consecuencias; al tratarse de computadoras con manos y patas o ruedas, el impacto al ser hackeados es enorme debido a su potencial uso para dañar tanto a personas como a cosas.

Los robots hackeados también se pueden utilizar para espiar, ya que tienen cámaras y micrófonos. Un hacker malicioso puede controlar remotamente un robot moviéndolo a voluntad para ver y escuchar todo lo que esté a su alcance.

El caso de los nanorrobots es una tendencia más moderna que combina las acciones de un robot con la nanotecnología, una tecnología del orden de magnitud de los nanómetros (una milmillonésima parte de un metro). Estos robots diminutos están conformados por partes mecánicas y biológicas, y su uso principal está centrado en la medicina, para que puedan, por ejemplo, ingresar en el cuerpo humano a reparar tejidos dañados, destruir células cancerosas, proveer nutrientes específicos, y mucho más.

Es bastante evidente pensar en los riesgos de los nanorrobots, ya que, así como pueden ser creados para salvar vidas, también podrían ser utilizados para crear problemas en el cuerpo humano. Al estar basados en computadoras, solo es necesario modificarles sus

programas para que realicen acciones destructivas en lugar de sanadoras.

Ciudades inteligentes

Una tendencia en crecimiento es la aplicación de tecnologías al funcionamiento de la infraestructura de las ciudades, creando las llamadas ciudades inteligentes, o *smart cities*. Esto implica combinar e interconectar sistemas de transporte, de suministro de servicios, de comunicaciones y otros para mejorar la experiencia de vida en una ciudad, haciendo más eficiente el uso de los recursos y dándole más comodidad a la gente. El desarrollo urbano de las ciudades inteligentes está basado en la sostenibilidad, pudiendo responder a las necesidades de empresas y de la ciudadanía en los aspectos económico, operativo, social y ambiental.

Dado que se busca compartir datos entre servicios para lograr interconexión de sistemas, aparecen los temas vinculados a la protección de los datos y la privacidad, que podrían comprometer a toda la población. Además, estas tecnologías están relacionadas con algunos sistemas de infraestructura crítica, que, en caso de ser afectados por un ataque terrorista o incidente, pueden poner en riesgo la vida de la gente y causar desde pequeños problemas hasta caos en una ciudad.

A las ciudades inteligentes se suman los edificios y casas inteligentes, que, a través de la conectividad –como hemos visto en internet de las cosas–, se encuentran expuestos a posibles ataques por el solo hecho de estar conectados a internet, aunque también podrían ser atacados desde otras edificaciones cercanas debido a que muchos de sus sistemas utilizan comunicación inalámbrica para interconectarse.

Un ejemplo muy resonante y representativo es el sistema de tráfico «inteligente», que permite que los semáforos sepan cuándo cambiar según el tráfico, lo que hace más eficiente la circulación.

Este sistema funciona en base a sensores que se encuentran en las calles (bajo el pavimento) y se comunican vía inalámbrica con aparatos que gestionan el sistema.

En una investigación[3] –que tuvo repercusión mundial– descubrí que era posible alterar la comunicación de los sensores, generar datos falsos y, en definitiva, afectar todo el sistema. Para esto, el atacante solo necesita estar en las proximidades de esos sensores, lo que puede hacer en persona, a través de drones o utilizando medios de transporte. Los riesgos de esta tecnología son muy altos ya que podrían generarse accidentes de tránsito difíciles de evitar, con pérdidas económicas y de productividad de personas y empresas, además de embotellamientos forzados y otras acciones maliciosas contra el bien público.

Mediante otra investigación también demostré que la mayoría de las nuevas tecnologías utilizadas en las distintas ciudades del mundo son inseguras y están expuestas a ciberataques. Esto es muy preocupante y, de seguir en este estado, los sistemas de las ciudades podrían ser hackeados, perjudicando a la población de distintas maneras.

Como ciudadanos debemos exigir a nuestros gobernantes que realicen pruebas de seguridad antes de empezar a utilizar tecnologías que afecten a la población y que no se imponga la funcionalidad por sobre la seguridad. Esta última tiene que ser lo primero a considerar para evitar serias consecuencias relacionadas con el uso de tecnologías inseguras, como ya hemos visto. También es importante que contribuyamos con nuestra opinión en cuanto a las necesidades que tenemos como ciudadanos y al tipo de soluciones que las empresas y gobiernos nos proveen, de forma tal que al involucrarnos formemos parte de la solución.

Big data

El término *big data* se refiere a los grandes volúmenes de datos, y por grandes estamos diciendo «muy» grandes, tanto que hasta una mínima variación en un conjunto de datos puede ser utilizada para extraer estadísticas de interés sobre aquello que se recopila.

El concepto *big data* surgió a partir de que la capacidad de almacenamiento de los medios informáticos se hizo más y más grande, pasando en pocos años de unos cuantos gigabytes (miles de millones de bytes) al orden de los terabytes, que en las grandes empresas ya se están transformando en petabytes, lo que, por ejemplo, equivale a millones de millones de archivos de música.

El *big data* puede ser utilizado para obtención de datos científicos, a tal punto que una rama de la ciencia se ha dedicado a estudiarlo en profundidad: la ciencia de los datos (*data science*). De hecho, lo que ha permitido que el *big data* tenga tanta utilidad en el mundo actual es la posibilidad de ser analizado y procesado.

Como en todos los casos, debemos comprender qué riesgos introduce para nosotros la posibilidad de almacenar y analizar estos gigantescos volúmenes de datos. Lo más evidente es la posibilidad de que pueda quedar guardada tanta información personal. Es decir, pensemos en un servicio de correo electrónico o en una red social –para entender que continuamente se produce mucho contenido–, que está siendo almacenado y archivado cada segundo. Por ejemplo, se estima que se suben a YouTube más de cuatro millones de videos por día. En Facebook se hacen más de 4000 millones de comentarios diarios, mientras que en servicios de correo electrónico se envían a lo largo de 24 horas más de 200.000 millones de e-mails. Sin dudas, las cifras son increíbles, pero lo más sorprendente es que en cada una de esas acciones viaja nuestra información

personal, nuestras palabras, fotos, videos y más; todo factible de ser analizado con las nuevas tecnologías de software e inteligencia artificial aplicada.

El análisis de estos datos puede ayudar a obtener información sobre nosotros que nunca hayamos hecho pública. Por ejemplo, el análisis de *big data* podría determinar nuestra orientación sexual, política, religiosa, etcétera, basándose en nuestra actividad en internet y preferencias sin que nosotros lo hayamos mencionado abiertamente. De esta misma manera, se pueden obtener distintos tipos de información sobre nosotros que podrían ser usados de diversas formas sin nuestra autorización.

Es posible que, en el futuro, la información que internet tenga de nosotros sea difícil de controlar, pero por el momento tenemos la oportunidad de seleccionar y pensar bien qué publicamos, qué compartimos y qué decimos en internet, ya que la mayoría de las acciones que producen contenidos personales son voluntarias.

En el futuro, es probable que si alguien (gobierno o gran organización) quiere obtener información sobre una persona, encuentre los medios para hacerlo sin que esta pueda evitarlo, pese a los esfuerzos para mantener cierto nivel de anonimato. En este sentido, dentro de algunos años, cuando hayamos olvidado la foto subida a Facebook o el mensaje que enviamos en Twitter, la tecnología podría recuperarla y ser utilizada a favor o en contra nuestro.

Con este panorama, debemos tener muy en cuenta la importancia de ser prudentes con el manejo de nuestra información, ya que, si bien puede ser utilizada para cosas beneficiosas, también podría afectar nuestra privacidad el hecho de que una empresa conozca más de nuestros propios hábitos que nosotros mismos.

Importante recordar

- Siempre es recomendable averiguar si los fabricantes de los productos tecnológicos que estamos adquiriendo aplican pruebas de seguridad informática a sus dispositivos. En general, esta información no la ofrecerán los vendedores, sino que tendremos que averiguarlo nosotros mismos a través de los medios de información que se encuentran en internet. De no hacerlo, estaremos confiando ciegamente en los productos.
- Debemos ser cuidadosos con la calidad y cantidad de información que «le damos» a internet, ya que será almacenada a través de los años y no sabemos para qué ni cómo podría ser utilizada en el futuro.
- Es recomendable conocer las alternativas de funcionalidad que nos ofrecen las tecnologías *wearables* y tratar de no depender de ellas, para, en caso de falla, no incurrir en riesgos innecesarios.
- Como buena práctica debemos elegir, en la medida de lo posible, productos tecnológicos que ofrezcan actualizaciones de seguridad o cuenten con medidas de protección para reducir los riesgos asociados.
- Es importante aprender a utilizar las nuevas tecnologías y generar otras competencias profesionales, ya que, en muchas tareas, los robots y los algoritmos implementados en el software lograrán reemplazar –tarde o temprano– a las personas.
- Debemos exigirles a los gobiernos locales y nacionales que no excluyan la seguridad cuando se trate de implementación de

tecnologías en ciudades, ya que estarían poniendo en riesgo la vida de los ciudadanos.

- No debemos esperar que ninguna empresa o entidad se encargue de nuestra privacidad y seguridad. Tenemos que ser prudentes en el uso de las tecnologías y aprender sobre ellas para no ser víctimas de problemas evitables.

---

[3] archive.nytimes.com/bits.blogs.nytimes.com/2015/06/10/traffic–hacking–caution–light–is–on/

Agradezco, a todos los que colaboraron, de distinta manera, para que este libro sea una realidad.

César Cerrudo ha sido hacker profesional por más de 20 años realizando diferentes trabajos e investigaciones en ciberseguridad. Ha ayudado a diversas empresas –Microsoft, Oracle, Twitter, IBM y muchas otras– a proteger sus tecnologías identificando cientos de problemas de seguridad que afectaban a millones de personas. Ha presentado en importantes empresas y conferencias alrededor del mundo el resultado de sus variadas investigaciones. También estas han sido cubiertas por los principales medios internacionales, como *The New York Times*, *Time*, *Bloomberg Businessweek*, *The Guardian*, CNN, NBC, Fox News, *Financial Times* y *The Wall Street Journal*, entre otros.

Logró fama mundial por haber hackeado los semáforos de Nueva York luego de publicar una de sus tantas investigaciones.

César es actualmente asesor de ciberseguridad para gobiernos, empresas e instituciones, y también es CEO de Argeniss Software, entre otras cosas.

Contactá a César Cerrudo:

https://linktr.ee/cesarcer

Créditos

ISBN: 978-9915-9834-3-1
Producción editorial: Mariana Zabala Diseño de ebook: Felipe Correa / https://about.me/felipe.correa