EL *BOOM* DE LOS DELITOS INFORMÁTICOS

Términos como *phishing*, estafa informática o *skimming* ya son palabras que han salido de la órbita jurídica para pasar al lenguaje coloquial, y es que casi todos quienes contamos con una casilla de correo electrónico o redes sociales hemos recibido, aunque sea una vez, un mensaje de dudosa procedencia con fines sospechosos: recibir los datos de nuestras tarjetas o cuentas bancarias, contraseñas de cuentas e incluso solicitando que depositemos dinero en determinada cuenta bancaria del exterior.

La tasa de los delitos informáticos ha crecido exponencialmente y hoy en día cualquiera puede llegar a ser una víctima si no se toman los suficientes recaudos a la hora de navegar la red. Esto sucede porque a los notables avances tecnológicos de los últimos 20 años se le sumó una pandemia mundial que generó todos los elementos para crear un ambiente más que fértil para que se propagara el cibercrimen.

El virus que azotó al mundo hace casi dos años nos impulsó a todos —incluyendo a los criminales— a tener que reinventar los aspectos más básicos de nuestra vida, como relacionarnos con nuestros seres queridos y trabajar. Según datos oficiales del FBI, durante 2020 los delitos informáticos aumentaron un 69 % con respecto a 2019, especialmente las estafas cibernéticas y el *phishing*. Los delincuentes se aprovecharon directamente de la crisis económica y humanitaria, tendiendo trampas para cuantos más blancos pudiesen acaparar, desde personas en situación de necesidad hasta empresas de gran porte.

Ahora bien, ¿cómo evitamos ser blancos fáciles de los ciberdelincuentes? ¿Qué precauciones se pueden tomar para no ser ciberestafados o que nuestros datos sean robados?

En primer lugar, siempre es importante contar con un antivirus de calidad, ya que de esa manera protegemos a nuestra computadora de que sea invadida por *malware* o *hackers* que puedan buscar introducirse en el sistema para sacar datos personales o empresariales,

o incluso espiarnos a través de la cámara *web*.

Además de un antivirus, también es muy aconsejable contar con un *firewall*: un instrumento que funciona como pared entre la red pública y la red privada, controlando que el tráfico que pasa de una a otra cumpla con ciertas reglas predeterminadas y así impedir el paso de intrusos. Siempre debemos tener cuidado al momento de instalar un *software* o aplicación; debemos asegurarnos de que el programa es original y su creador es confiable.

Por otra parte, tampoco es seguro conectarse —y mucho menos realizar operaciones bancarias o manejo de datos importantes— por medio de redes de Internet públicas (de restaurantes, hoteles, espacios públicos) ya que no cuentan con la suficiente seguridad y son fácilmente intervenibles por los delincuentes.

Una medida adicional, sencilla y efectiva es implementar el cambio regular de contraseñas, procurando incluir mayúsculas, signos de puntuación y la letra ñ (que no se encuentra en teclados de otros idiomas).

Ahora bien, corresponde hablar de las figuras más habituales en la actualidad y las precauciones para estas. Si bien hoy en día las estadísticas demuestran que la gran mayoría de los ciberdelitos denunciados se encuadran en la hipótesis de la estafa informática, la estrella de los últimos años es el *phishing*. La etimología de esta palabra proviene de la fusión entre *password* y *fishing*, su traducción sería "pescar contraseñas". El delincuente arroja un anzuelo virtual en busca de pescar datos personales de la víctima (especialmente contraseñas) que le permitan acceder a los datos personales y bancarios. El *modus operandi* del cibercriminal es de lo más variado: puede enviar correos electrónicos haciéndose pasar por una empresa que le ofrece servicios a la víctima (Microsoft, Netflix, Spotify, Mercado Libre, Amazon, Apple) solicitando que renueve sus datos o diciendo que cierta compra no quedó bien realizada; puede hacerse pasar por un representante de su entidad bancaria y más, el límite es la imaginación del ciberdelincuente.

Para evitar ser víctima de *phishing* siempre tenemos que comprobar la dirección de correo electrónico del remitente, además, debemos tener en cuenta que por lo general los grandes proveedores de servicios —como las mencionados— no nos van a solicitar jamás los datos de nuestra tarjeta por medio de un *mail* o redireccionándonos a páginas de dudosa confiabilidad. Ante la duda, es mejor no responder los *mails* que solicitan este tipo de datos o antes contactarse por teléfono con el proveedor.

También son comunes en el mundo de las estafas informáticas los timos por los cuales se intenta convencer a la víctima de que un familiar del exterior necesita una ayuda económica, que se ha ganado alguna clase de premio o incluso que existe una herencia en el exterior a su favor. Este tipo de engaños suelen hacer caer a los usuarios menos experimentados.

Es evidente que con el correr de los años los ciberdelincuentes han perfeccionado sus tácticas y que lo seguirán haciendo, siguiendo el ritmo del desarrollo tecnológico, por lo tanto, es importante mantener los ojos abiertos; chequear los detalles de los *mails* que llegan a nuestro correo electrónico —la forma de redacción y la existencia de faltas ortográficas pueden delatar a un delincuente haciéndose pasar por una institución empresarial—; no clicar sobre *links* que llegan de *mails* desconocidos ni brindar datos de tarjetas o cuentas bancarias a ningún sitio que no sea a todas luces seguro y confiable; la suficiente diligencia a la hora del uso de la red y equipos informáticos puede llegar a salvarnos de una gran pérdida económica. Y, lo que es más importante, contribuye con la lucha contra la ciberdelincuencia que, día a día, amenaza una herramienta tan útil y maravillosa para la humanidad como lo son las tecnologías de la información y la comunicación.

Por María Paz Bonilla
Integrante del Estudio Jurídico Scelza & Montano