**TECNOLOGÍA** De *hackers*, *crackers* y cibercrímenes en tiempos de pandemia.

# REDES CRIMNINALES

El aislamiento social ha acelerado nuestra vida *online*, pero ¿qué tanto sabemos sobre las seguridades e inseguridades de nuestros datos y cuentas almacenados en el ciberespacio?

KATHERINE SUBIRANA ABANTO

¿Se imagina que, de la nada, muchos cajeros automáticos a la vez empiecen a expulsar billetes y ocasionen —literalmente— una lluvia de dinero? No lo imagine, pues esto pasó en 2016 en más de una docena de países europeos, cuando un grupo de *hackers* programó, de forma remota, a decenas de estos aparatos para que a determinada hora expulsaran billetes sin control. Ellos solo "pasaron casualmente por ahí" cuando sucedió.

Esta escena es buena para recordar que, aunque el *hacking* —acto de vulnerar un sistema informático— no es una broma, nació como tal. Fue en la década de los sesenta, en el Instituto Tecnológico de Massachusetts, cuando los miembros del Laboratorio de Inteligencia Artificial se realizaban bromas entre sí instalando en las computadoras programas piratas con el objetivo de demostrar una superioridad técnica (o solo porque sí). Esas bromas se llamaban *hacks*, y quienes las hacían empezaron a llamarse *hackers*.

Los sistemas de cómputo y las redes se volvieron cada vez más complejos, y los caminos de los *hackers*, también. Gracias a ellos existen internet y la World Wide Web, y coinciden en la defensa y creación de *software* libre. También está Anonymous, abanderado de la lucha por un internet libre que extendió sus acciones al apoyar causas políticas y sociales al liberar información que revela delitos de toda índole. Pero la moneda tiene dos caras, y la menos amable la ocupan quienes usan su conocimiento para vulnerar sistemas informáticos y cometer delitos de distinta naturaleza, buscando su beneficio personal, como son la clonación de tarjetas o el robo de datos personales.

Para evitar confusiones, los *hackers* se dividen en dos grupos: los de sombrero blanco, que afirman que son solo ellos los que merecen el título de *hackers*, pues los otros, los de sombrero negro, son, en realidad, *crackers*. Camilo Galdos, jefe del área de investigación de la empresa peruana Deep Security, lo define así: "El *hacker* actúa por curiosidad y el *cracker*, por obtener un beneficio más allá del conocimiento". Entonces, hablemos con *hackers* sobre las trampas de los *crackers*.

**—La millonaria que no tiene herederos—**

A mediados de los años 90, en los albores de la popularización de internet en el Perú, los usuarios de correo electrónico vieron con sorpresa llegar a su bandeja de entrada mensajes del tipo "Bill Gates va a donar cinco mil dólares; solo tienes que entrar a este enlace y dejar tus datos" o "Soy millonaria, tengo cáncer, voy a morir y quiero dejarte mi herencia porque no tengo familia". Que levante la mano quien no le dio clic a uno de esos enlaces alguna vez. Basándonos en la definición de la compañía de seguridad informática Kaspersky, si usted lo hizo, fue víctima de *phishing*; es decir, le cedió a un tercero su correo electrónico para usos poco benévolos.

El *phishing* no ha desaparecido; más bien, se ha sofisticado. Si hace 20 años lo único que se podía perder era una cuenta de correo en la que recibía tarjetas de gusanito.com, hoy el panorama



ILUSTRACIÓN: VÍCTOR AGUILAR RÚA

**ÉTICA *HACKER***
La ética *hacker* se basa en el acceso libre a la información y a los computadores, la rebeldía y la no discriminación.

***HACKTIVISMO***
Se llama así al uso de técnicas *hackers* en causas sociales, ecológicas, humanitarias o de cualquier otra índole social.



*"El* hacker *actúa por curiosidad y el* cracker, *por obtener un beneficio más allá del conocimiento".*

SEGURIDAD PERUANA

## Sobre la Ley de Delitos Informáticos

En 2013 se publicó la Ley de Delitos Informáticos N.° 30096 con el objetivo de prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos, la indemnidad y libertad sexuales, la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública, en los cuales el delincuente utiliza la tecnología actual para cometer actos ilícitos.

Fátima Toche, abogada especialista en el área de tecnología y delitos informáticos, considera que el principal vacío en la ley es no contar con jueces y fiscales especializados en delitos informáticos. "Es una disciplina que requiere especialización y no todos los abogados, jueces y fiscales la tienen. Muchos casos se caen porque jueces y fiscales no saben valorar las pruebas y no entienden la tecnología. Más que conflictos regulatorios, yo veo un problema en que no hay expertos en informática forense que puedan hacer el análisis técnico informático de los casos. Es una cuestión de recursos humanos especializados y ni qué decir de la precariedad en la que trabaja la División de Investigación de Delitos de Alta Tecnología (Divindat), que por falta de gente y tecnología no realiza los patrullajes cibernéticos que debería hacer para la prevención del delito".

Y añade: "Nadie habla de la educación digital. Si en la escuela formaran en ciudadanía digital y peligros de internet, menos gente caería en *phishing* y otros fraudes virtuales".

es distinto. La cantidad de datos personales que almacenamos en la red (número de documento de identidad, firmas digitales, tarjetas de crédito, etc.) puede exponernos a riesgos mucho mayores: podemos ver nuestras actividades expuestas y ser sujetos de fraudes bancarios.

Los ciberdelincuentes han optado también por el *phishing* segmentado y atacan cuentas de correo de adultos mayores aprovechando el poco manejo que estos suelen tener de la tecnología. También es muy usada ahora la modalidad de *smishing*, es decir, los mensajes de texto que vienen de números telefónicos desconocidos que usan el nombre de instituciones conocidas, pero cuyos enlaces son falsos. Al darles clic, lo dirigen a una página de *phishing* o insertan en su dispositivo móvil un código malicioso.

Lo más común es que estos mensajes roben datos de cuentas bancarias y, por supuesto, dinero. Por ello, las entidades financieras realizan campañas para que sus clientes no ingresen a enlaces que llegan en mensajes poco seguros o que los redirigen a páginas que solicitan datos personales. Pero ¿qué pasa si un cliente cae en una de estas estafas? Los bancos en el Perú manejan más o menos las mismas políticas: asumen el costo total de la pérdida en determinadas circunstancias: si el robo de dinero se produjo después de que el usuario bloqueara su tarjeta, si el robo fue por una vulneración al sistema del banco que nada tuvo que ver con el cliente o si el delito involucra el mal manejo de los datos personales del usuario por parte de los trabajadores de la entidad bancaria.

Surge la siguiente pregunta: ¿Por qué los bancos ofrecen seguros de protección para las tarjetas en caso de robo o fraude? ¿Significa que están reconociendo que sus sistemas no son seguros? Camilo Galdos responde de forma sencilla: "En caso de robo, obviamente no es responsabilidad del cliente, pero, en caso de fraude, puede que el cliente lo haya facilitado al dar clic en enlaces peligrosos o dejar sus datos personales en páginas maliciosas". Los seguros están orientados a ello.

En el Perú, el *phishing* está penalizado hasta con cuatro años de pena privativa de libertad. El artículo 1 de la Ley de Delitos Informáticos N.° 30096 señala que el que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años, y con treinta a noventa días multa.

**—Seguridad en tiempos de *e-commerce*—**
El informe "Consumidores y marcas en tiempos de COVID-19", elaborado por Llorente y Cuenca en marzo de 2020, pinta el panorama actual: divertirnos, comunicarnos, comprar o trabajar es prácticamente imposible sin sumergirnos en el mundo digital, por lo que la pandemia aceleró el cambio en áreas como la digitalización,

los servicios bajo demanda y el desarrollo del *e-commerce*.

Consciente de ello, la Organización Mundial del Comercio elaboró y presentó en mayo el documento "*E-commerce*, comercio y pandemia" en el que aborda la necesidad de proteger al consumidor en línea, pues se han registrado prácticas fraudulentas en la venta y problemas de ciberseguridad. Los principales fraudes informáticos que se pueden cometer en el *e-commerce* son la clonación de tarjetas, transferencias electrónicas fraudulentas, compras por internet mediante información de tarjetas de crédito o débito, *smishing*, y *phishing*, explica Óscar Zevallos Prado, abogado del Estudio Muñiz, en un texto publicado en su portal.

Es claro que los fraudes se cometían antes de la pandemia, pero es cierto que, a partir de la declaratoria de emergencia nacional, los centros comerciales y establecimientos medianos y pequeños y casi la totalidad de consumidores se han visto obligados a ingresar al mundo del *e-commerce*. ¿Están preparados para ello?

Los usuarios deben estar prevenidos, ya que las estafas no solo se realizan mediante intrincados enlaces web. La clonación de tarjetas de crédito también es un riesgo. ¿Cómo se realiza? Óscar Zevallos pone un ejemplo: usted puede realizar una compra por *delivery* y pasar su tarjeta por un POS modificado que extrae los datos de la tarjeta de crédito. Luego, los delincuentes clonan dicha tarjeta, y efectúan compras por internet u otros canales digitales.

Además de procurar consumir en establecimientos de confianza, ¿cuáles son las precauciones por tomar al realizar una transacción virtual? Camilo Galdos da algunas recomendaciones: "La única forma de no ser vulnerado por atacantes es usar la tarjeta de crédito en sitios fiables y de alta reputación. Para sitios de *e-commerce*, una buena alternativa sería usar un *proxy* de pago como PayPal o Pago Efectivo, o usar el sistema que redirija el pago a la web de la tarjeta de crédito (Visa, Mastercard, etc.), pues el riesgo ocurre al entrar a una web desconocida que, al momento de hacer la compra, pide que se ingresen los datos de la tarjeta".

SHUTTERSTOCK



**La figura de Anonymous se ha convertido en el símbolo de los *hackers* y del *hacktivismo*.**

> *¿Los pequeños comercios están preparados para ingresar adecuadamente al mundo del e-commerce?*

**—Teletrabajo y ciberseguridad—**

Ante la necesidad de implementar el teletrabajo, la empresa debe tener en cuenta los protocolos de seguridad necesarios para que este se realice en un entorno digitalmente seguro. Charter of Trust, asociación que promueve la seguridad informática, reportó que, en 2019, se registraron casi 200 millones de ataques de *ransomware* en el mundo y se teme su aumento. ¿Qué es el *ransomware*? Se trata de un ataque en el que los cibercriminales instalan en las PC un *malware* (*software* malintencionado) para sustraer información. Este 2020, los ataques pueden aumentar, pues el teletrabajo ha hecho que algunas empresas relajen sus protocolos de seguridad informática para que los trabajadores accedan más fácilmente a los sistemas.

Los expertos de Allianz Global Corporate & Specialty elaboraron una serie de recomendaciones para protegerse de cualquier tipo de ciberataque, por ejemplo, mantener el *software* actualizado, utilizar antivirus y tomar precauciones al compartir datos personales. También recomiendan mantener los dispositivos de trabajo en la oficina y no llevar a casa los que no sean necesarios; usar navegadores web actualizados; utilizar distintas contraseñas y que estas sean seguras; proteger los datos mediante cifrados; descargar datos solo de fuentes de confianza; realizar periódicamente copias de seguridad; no mezclar usos personales y laborales; y ser especialmente cuidadoso ante correos o adjuntos sospechosos, sobre todo de remitentes desconocidos.

Al respecto, Camilo Galdos comenta: "El principal problema de seguridad en las empresas son los trabajadores. Se pueden comprar *firewalls* de cientos de miles de dólares, pero, si no capacitan al personal para entender de ciberriesgos, es muy probable que la empresa sea atacada". Ciertamente. Al final, cualquier tipo de estafa cibernética depende únicamente de la decisión correcta o incorrecta que tomemos nosotros, los seres humanos.