Delito en alza

Ciberdelito: Estafaron por millones a dos jubiladas

Durante la cuarentena y el aislamiento social, preventivo y obligatorio, crecieron los ciberdelitos. A veces pueden ser daños menores, como la pérdida temporal de la cuenta de una plataforma o la suscripción a un servicio premium del celular. Pero para algunas personas los daños pueden ser millonarios y generarle deudas por varios años.

“Los delitos y estafas online aumentaron al menos en un 70% durante el con namiento, muchos de los cuales implican la posibilidad de robo de credenciales y tarjetas de crédito y débito. La gente está más conectada y más sensible que nunca y lo que pasa en estos casos lamentablemente no es un tema tecnológico. Tiene que ver con concientización y educación”, explicó Gabriel Zurdo, especialista en ciber seguridad y CEO de BTR Consulting.
¿Cuál es el principal inconveniente? El desconocimiento de ciertos aspectos del home banking y los cajeros automáticos y la habilidad de los delincuentes para conseguir los datos necesarios y actuar antes de que la víctima pueda reaccionar.

Marcela Lesniowski y Viviana Díaz son dos docentes jubiladas, de Tigre, que cayeron en la trampa de los cibercriminales. No solo les robaron el dinero que tenían en sus cajas de ahorro sino que también sacaron préstamos de los bancos, con altas tasas de interés, que las damnicadas deberán pagar. Las dos son clientas del Banco Provincia, que por ahora les informó que ellas fueron las que entregaron las claves de acceso a sus cuentas.

“En casos como este recordamos el concepto del -cuento del tío-, que en el mundo de la informática lo llamamos -ingeniería socia-. Básicamente se genera un pretexto (más o menos creíble) para manipular o influir en una persona. En este caso, el engaño logró su cometido porque las víctimas quizás no tenían tanta educación o experiencia en temas digitales y se revelaron datos sensibles que deberían haber permanecido confidenciales”, armó Federico Kirschbaum, especialista enseguridad informática y fundador de Ekoparty.

La estafa a Díaz fue hecha de forma telefónica. “Me llamaron al celular, una persona que se identicó como Walter, que me dijo que trabajaba para ANSES y que estaba obteniendo el benecio del Ingreso Familiar de Emergencia (IFE). Primero le dije que no, porque yo sabía que ni mis padres ni yo lo teníamos que cobrar, pero ante la

insistencia me di cuenta que mi tía, que no tienen ninguna ayuda del estado, lo podía cobrar. Pensé que la habían anotado a ella y le dije que sí", relata la docente.

Después llegó el momento del robo de la cuenta. "Me empezó a explicar que la persona tenía que estar bancarizada, pero como ella no tiene cuenta podía usar la mía. Me aturdió con pedidos, personalmente hicieron que les de un código desde el cajero automático, que es con el que pudieron acceder a mi home banking", detalló Viviana.

"Primero pidieron un adelanto de sueldo, de 15 mil pesos, para que parezca que había cobrado el IFE. Pero después pidieron un préstamo de 447 mil pesos, con el sistema francés, que yo desconocía que tenía pre aprobado por el banco. Todo ese día estuvo bloqueado mi home banking, y por la pandemia, cuando fui al banco no me atendieron. Y en el cajero tampoco podía cambiar las claves porque estaban bloqueadas. Recién al otro día pude ir en persona y me dijeron que no podían hacer nada, porque yo les había dado las claves", agregó la mujer, que realizó la denuncia y espera una resolución por parte de una fiscalía de Tigre.

"Lo más doloroso es que terminé siendo yo la responsable, y me obligan a pagar un crédito que por ser sistema francés entrega 447 mil pesos pero terminó devolviendo más de un millón. Voy a estar los próximos seis años de mi vida pagando algo que yo no pedí", concluyó la docente.

La estafa a Marcela comenzó de otra forma: una página web que prometía conseguir un turno en el Banco Provincia, en el marco del Aislamiento social y obligatorio.

"Me comuniqué con la línea de atención telefónica para pedir un turno, para retirar dólares que tenía en mi cuenta. Me lo dieron para más de un mes después, 48 días. Pero al poco tiempo en Facebook me apareció una página, Bip Provincia, que decían poder gestionar turnos más rápido y operar desde la casa. Accedí y me dijeron que tenía que ir al banco, generar unas claves y enviárselas. Hicelo que me pidieron y lo mandé", explicó la mujer.

La sorpresa llegó en forma de correo electrónico, donde el banco le avisaba que habían hecho transferencias desde su propia cuenta, algo que ella no había hecho.

"Me volví a contactar con esta gente y me dijeron que estaban averiguando de dónde había sacado los dólares, porque ahora se estudiaba ese tema. Ahí empecé a sospechar y fui al banco, pero no me atendieron. Después de varias horas finalmente logró hablar con una persona del banco, que me dijo que yo les entregué el token de seguridad, que les -di la llave- y que llame al teléfono del Banco para solucionarlo. No me sentí contenida por la entidad", relató Marcela.

Además de vaciarle las cuentas también aprovecharon para sacar un préstamo personal, de 920 mil pesos, que ella deberá pagar con su sueldo. "Falta información: yo no sabía ni que tenía un adelanto de sueldo de 30 mil pesos ni un préstamo así, sin tener que firmar ni nada. Alguna vez que pedí algo parecido tenía

que cumplir un montón de requisitos, ahora lo hacen todo por Internet", agregó la mujer.

"Ahora puse un abogado especializado en ciberdelitos, y por una medida cautelar no me están descontando. Pero todavía no me llamaron a declarar, aunque sea por videollamada, de la fiscalía de Tigre, que es la que está a cargo del caso", concluyó la docente víctima del delito cibernético.

Desde el Banco Provincia respondieron a la consulta de TN Tecno por estas estafas.

"Los casos consultados son estafas perpetradas a través de la modalidad conocida como ingeniería social. Esta forma de delito es utilizada por los delincuentes para explotar la confianza de una persona a fin de obtener información confidencial que les permita realizar un delito posterior u obtener dinero en forma directa", explicaron.
Desde la institución también remarcaron el crecimiento de estos casos durante la pandemia. "Las situación de aislamiento, producto de la pandemia de COVID-19, propició que los delincuentes potencien la utilización de la ingeniería social ya que es más fácil engañar a alguien para que revele sus datos confidenciales que vulnerar la seguridad de los sistemas que administra el Banco", detallaron, para agregar que están colaborando para tratar de encontrar a los culpables: "Banco Provincia colabora de forma constante y permanente con las investigaciones judiciales que se desarrollan en virtud de las denuncias de las eventuales víctimas, y estos casos en particular no han sido la excepción. Se contestaron las requisitorias que la Fiscalía interviniente cursó, a fin de ayudar a la identicación de los responsables de la estafa".

Desde la institución, además, compartieron una serie de recomendaciones de seguridad para evitar este tipo de estafas, además de recordar que desde la entidad nunca solicitan claves de acceso y/o datos personales por correo electrónico o llamados telefónicos.

- No compartir ni divulgar claves.
- Usar contraseñas fuertes mezclando mayúsculas, minúsculas y números.
- No usar la misma clave para distintas aplicaciones, cuentas, plataformas, etc.
- Leer con cuidado los emails que se reciben. Vericar que los sitios remitentes sean legítimos.
- Cuando por teléfono se ofrezcan premios, préstamos o benecios importantes, no dar datos de cuentas, tarjetas, y frente a la duda consultar a alguien de confianza.
-No usar equipos públicos o de terceros para acceder a las aplicaciones o sitios de bancos.
- No usar redes de wi-fi públicas para acceder a sitios que soliciten contraseñas.

La palabra de los expertos

Con la pandemia por el COVID-19 los ataques de tipo phishing se hicieron cada vez más frecuentes. “Consiste en un engaño que representa el 45% de los ataques de seguridad. En algunos casos, los estafadores crean sitios o cuentas falsas en redes sociales imitando sociales. Usan los mismos logos y la dirección de correo de la empresa dentro de la página o el mensaje que envían a sus víctimas. Por ejemplo, les ofrecen una solución o les anuncian de algún presunto inconveniente y les solicitan su información privada con el falso propósito de ayudarlas”, resumió Zurdo.
Kirschbaum, también destacó a la pandemia como un factor determinante en este tipo de delitos: “Mucha gente comenzó a usar herramientas digitales que antes no usaba, y por supuesto los atacantes aprovechan esta situación y la falta de conocimiento en medidas de protección”.

El sistema utilizado en la estafa a las jubiladas de Tigre, con llamadas telefónicas, se llama “vishing”o “phishing por voz” . “Es una forma de ingeniería social, donde la gente no sabe que está hablando con un impostor. Piensan todo el tiempo que estuvieron hablando con una persona de soporte técnico de un banco o del ANSES. Es una vieja técnica que se ha reutilizado y optimizado en los últimos tiempos”, confirmó Zurdo, que aclara que siempre hay que “prestar atención si recibimos un mensaje a través de Instagram, WhatsApp o SMS donde el estafador se hace pasar por una entidad oficial".

“El foco debería estar en la educación, en comprender los riesgos y cómo protegerse de ellos, en concientizarse sobre el phishing, los engaños y otras técnicas de ingeniería social que podrían poner en peligro la identidad y la información de las personas. La tecnología es imprescindible en la vida cotidiana, por lo cual, la clave está en usarla de forma responsable”, resumió Kirschbaum, que aconseja ser prejuiciosos con los vínculos acortados, con los que llegan por correo electrónico o por redes sociales y siempre actuar con cautela a la hora de compartir datos sensibles.
“Debemos desconfiar de soluciones o -regalos- en las redes sociales. En esta estafa se trata de utilizar cuentas impostoras en las redes para engañar a los usuarios. Cuando nos invitan a entrar aalgún sitio, debemos observar muy bien la URL de cada página. En este sentido, una vez que identiquemos la página real, deberíamos guardarla en Favoritos y entrar por allí, en lugar de usar los resultados de búsqueda”, recomienda Zurdo, que también propone crear contraseñas únicas para cada sitio. “Las contraseñas universales son cómodas, sin embargo, asumimos un riesgo al utilizar la misma para muchos sitios web. Si un pirata informático obtiene nuestra contraseña en un sitio web, nuestras otras cuentas serían igualmente vulnerables a los ataques”.
¿Sobre quién recae la responsabilidad en casos como estos? “Es difícil determinar de quién es la responsabilidad y quién debe hacerse cargo. En general, el banco se hace cargo de compensar a la víctima, siempre y cuando se cumplan ciertas

condiciones. Creo que se necesita un esfuerzo conjunto entre el espectro de usuarios, que deben comprender la importancia de educarse; y las organizaciones, que deben fortalecer los controles. En este caso, la vericación de identidad o los requisitos necesarios para poder sacar un crédito", concluyó Kirschbaum.

(Fuente: El Esquiú)