Vol. Nº 8
Marzo/2021
www.csirt.gob.cl

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

Operación Renta 2021:
El SII y la TGR se preparan para enfrentar un mes clave

Ingenieria Social:
Cómo los ciberdelincuentes refinan sus ataques para una mayor efectividad

Cooperación Internacional
Brasil

Tendencias
Evolución y presente del Phishing

Comunidad Nacionales
Los grupos que inspiran y suman mujeres a la ciberseguridad

Legal
Engaños en línea y delitos: El Phishing

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

145 8712 7864
096 4321 5541

CSIRT es el Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile. Su misión es reducir los riesgos de la ciberseguridad en las redes del Gobierno de Chile, asesorando a las diferentes organizaciones que lo componen, actuando como socio estratégico en la defensa de las amenazas y colaborando para brindar mayor seguridad y robustez a las infraestructuras del Estado.

¿Cómo lo **hacemos?**

Contamos con un equipo multidisciplinario de profesionales y las tecnologías para proveer de asistencia técnica y logística a nuestros beneficiarios, así como prevenir la explotación de vulnerabilidades y actuar oportunamente frente a amenazas y ciberataques.

- MONITOREO DE LAS PLATAFORMAS DE INTERNET DE ORGANISMOS PÚBLICOS Y PRIVADOS **24/7**
- INVESTIGACIÓN Y CAPACITACIÓN PARA ENFRENTAR LAS AMENAZAS DEL FUTURO
- DETECCIÓN DE VULNERABILIDADES DE SITIOS Y SISTEMAS WEB DEL ESTADO
- GESTIÓN DE INCIDENTES Y DIFUSIÓN DE MEDIDAS PREVENTIVAS
- INCORPORACIÓN DE NUEVAS TECNOLOGÍAS Y HERRAMIENTAS DE SEGURIDAD INFORMÁTICA
- MEJORA CONTINUA DE LOS ESTÁNDARES DE CIBERSEGURIDAD DEL PAÍS

Alianza del Pacífico · FIRST · CSIRTamericas.org · MERIDIAN Connecting and Protecting

INDICE

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBER SUCESOS

Investigación, Tendencia y Concientización

cibersucesos@interior.gob.cl

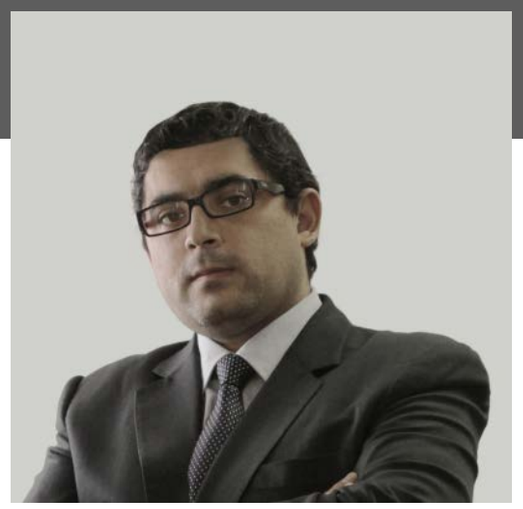
Director: Carlos Landeros Cartes

Jefa de contenidos y edición:
Katherina Canales Madrid

Colaboradores equipo CSIRT:
Ramón Rivera

Diseño y diagramación: Jaime Millán

EDITORIAL



Carlos Landeros Cartes
Director Nacional
CSIRT de Gobierno

Cada año, la Operación Renta se convierte nuevamente en un éxito para sus principales responsables, el Servicio de Impuestos Internos (SII) y la Tesorería General de la República (TGR). Ambos sistemas reciben en abril un volumen creciente de transacciones sin grandes problemas. Cómo lo logran y cómo proyectan el futuro de la digitalización de sus trámites, es nuestro tema central en este número, en la voz de sus líderes: el director del SII, Fernando Barraza, y la Tesorera General de la República, Ximena Hernández.

Lamentablemente, el que los contribuyentes debamos volcarnos a internet en abril, incluyendo a muchas personas que pueden no tener mucho manejo digital, vuelve a este período en un imán para los ciberdelincuentes. Más aún durante esta pandemia que ha obligado a realizar trámites por internet a personas que nunca antes lo había hecho, como muchos adultos mayores.

Por eso, el presente número de CiberSucesos se enfoca a explicar las características y técnicas de la ingeniería social, principal vehículo de las estafas realizadas a través de internet, y en especial de su exponente más común, el phishing. De hecho, la sección Tendencias la dedicamos en su totalidad a delinear las principales modalidades de este flagelo, las razones por las cuales la ingeniería social tiene tanto éxito y los pasos clave para evitar caer en ella.

Nuestra tradicional columna de Cooperación Internacional cuenta en esta ocasión con la participación de la doctora en Ciencias de la Información brasileña Elba Vieira, quien describe la realidad de su país como uno de los más afectados por el phishing en el mundo, especialmente tras el estallido del coronavirus, y detalla la política de Brasil para conseguir una mejor seguridad digital, la denominada Estratégia Nacional de Segurança Cibernética (E-Ciber).

Las Comunidades Nacionales representadas en esta edición coinciden en promover, cada una de forma diferente, una mayor participación de las mujeres en las ciencias, la tecnología y la ciberseguridad. Una labor que cobra mayor notoriedad en marzo, debido a la conmemoración del Día Internacional de la Mujer, pero que debería ser destacada todo el año.

Para finalizar, nuestra sección Legal recibe la opinión experta del abogado Renato Jijena, profesor de Derecho Informático de la Pontificia Universidad Católica de Valparaíso, quien explica la tipificación jurídica ya existente dentro de la cual se enmarcan delitos como el phishing.

OPERACIÓN RENTA 2021

El SII y la TGR se preparan para enfrentar un mes clave

La Operación Renta es cada año un imán para los ciberdelincuentes, convirtiendo al mes de abril en uno que ve una enorme alza de los ataques de phishing. Se multiplican los mensajes suplantando a la Tesorería General de la República (TGR) y al Servicio de Impuestos Internos (SII), como los organismos que lideran la Operación Renta, mensajes falsos que exigen a sus víctimas descargar archivos, hacer clic o entregar contraseñas para poder acceder a sus dineros o evitar deudas. ¿De qué forma se preparan estas importantes instituciones para hacer frente a los desafíos de la Operación Renta?

Las más altas autoridades de la TGR, tesorera general Ximena Hernández, , y del SII, director Fernando Barraza, explican que los desafíos de la Operación Renta son múltiples, ya que se combina un período de extrema demanda para los sistemas de ambos organismos, con una alta ocurrencia de estafas virtuales que se aprovechan del proceso tributario. "Cada año es un desafío contar con las capacidades tecnológicas para soportar el alto nivel transaccional y de procesamiento de datos en un corto período", explica Barraza. Más aún en 2021, agrega, con los nuevos sistemas y desafíos que ha traído la implementación de la boleta electrónica.

Hernández detalla que en la TGR, "nos corresponde no solo emitir los pagos correspondientes a cerca de 2 millones 800 mil devoluciones aprobadas por impuestos, sino también realizar los procesos de retención y compensaciones a los que están afectos estas devoluciones". Así, para el proceso del presente año, la tesorera general espera tener que realizar más de 70 mil devoluciones adicionales que en 2020, además de destacar que el 95% de las devoluciones de impuestos de la Operación Renta son hechas de forma electrónica.

Lógicamente, la pandemia también ha significado un mayor esfuerzo para ambos servicios. Este año en el SII "se proyecta un crecimiento de transacciones cercano al 40%, ya que muchos contribuyentes que habitualmente nitan presentar declaración de renta podrían tener que hacerlo este año, debido a los beneficios otorgados el año pasado producto de la pandemia", explicó Barraza.

¿Cómo se refuerzan estas instituciones para resistir tal incremento en la demanda? "Todos los años se realiza una revisión y pruebas exhaustivas a toda la plataforma tecnológica, con el fin de asegurar sus capacidades, disponibilidad, seguridad y tiempos de respuesta para asegurar una Operación Renta exitosa", indica Barraza. Esto incluye, explica, una serie de preparativos relacionados con la seguridad de la información y la ciberseguridad. El SII ha visto asimismo la incorporación de los denominados "asistentes web", indica el director del servicio, programas que ayudan a los contribuyentes a llenar las declaraciones juradas más complejas.

Por su parte, la TGR migró a la nube procesos como el correo electrónico y sus archivos compartidos, explica su máxima autoridad, lo que "nos permite flexibilizar y contar con mayor capacidad de respuesta cada vez que aumenta la demanda, como ocurre con la Operación Renta", detalla. Desde el punto de vista de la ciberseguridad, "la TGR cuenta con varios puntos de seguridad para el control y mitigación de amenazas como virus, spyware, ransomware, desastres tecnológicos y físicos", indica Hernández, esto por supuesto junto a una preocupación por la capacitación y concientización de funcionarios y contribuyentes.


0 0
0010
10 0
1
<!DOCTYPE html>
<html lang="en">
<head>
<title>My perfect website</title>
<meta charset="utf-8" />
<link rel="preconnect" href="//s3.mysite.com" />
<link rel="preconnect" href="//www.mysite.com" />
<meta name="viewport" content="width=640, initial-scale=1">
<script>
var mytag = mytag || {};
mytag.cmd = mytag.cmd || [];
(function() {
var gads = document.createElement('script');
gads.async = true;
gads.type = 'text/script';
var useSSL = 'https:' == document.location.protocol;
gads.src = (useSSL ? 'https:' : 'http:') + '//www.mytagservices.com/tag/js/gpt.js';
var node = document.getElementsByTagName('script')[0];
node.parentNode.insertBefore(gads, node);
})();
mytag.cmd.push(function() {
var homepageSquarySizeMapping = mytag.sizeMapping().
addSize([945, 250], [200, 200]).
addSize([0, 0], [300, 250]).
build();
mytag.defineSlot('/1023782/homepageDynamicSquare', [[300, 250], [200, 200]], 'reserved-div-1').

LOS DESAFÍOS **QUE VIENEN**

Ximena Hernández
Tesorera General de la Republica

Fernando Barraza
Director del Servicio de Impuestos Internos

“Este año seguiremos avanzando en la mejora de la disponibilidad y usabilidad de servicios y trámites a nuestros contribuyentes, esperando llegar a tener un 75% de nuestros trámites digitalizados”, explica Hernández. Esto contempla la inclusión de nuevos conceptos de pago y mejor control de la gestión financiera. La mandamás destaca que este proceso de digitalización fue acelerado por la pandemia, ya que antes de esta la cobertura de trámites digitalizados era del 60%.

La tesorera destaca la mejora constante de si sitio web, tgr.cl, el que permite resolver los trámites de los ciudadanos en cualquier lugar con conexión a internet, como “pagar contribuciones, suscribir un convenio o revisar el estado de un beneficio”, incluso a través de sistemas como el de PayPal, para facilitar la vida de los chilenos que viven en el extranjero. Por supuesto, la TGR tiene convenios con ChileAtiende y CajaVecina del BancoEstado para llegar a todos los rincones del país, complementa Hernández.
“Nuestro desafío este año es fortalecer la digitalización de nuestros usuarios y responder rápidamente a sus necesidades con un servicio seguro, confiable y, por ello, afianzar una cultura en ciberseguridad entre nuestros funcionarios y usuarios es fundamental”, concluye la tesorera.

Desde el SII, su director menciona varias tareas entre las que la institución planea realizar en el corto a mediano plazo. Entre ellas, señala la necesidad de realizar mayor análisis de datos, en el contexto del denominado “big data”, ampliando el uso de algoritmos de “machine learning”, con tal de “optimizar el monitoreo del comportamiento tributario de los contribuyentes, a través de productos como el radar tributario y el detector de fraudes”.
Además, Barraza menciona como otra tarea digital a desarrollar el conseguir mayor interoperabilidad con otros organismos públicos, “en base a servicios de datos e integración de sistemas, promoviendo el uso de la clave tributaria para contribuyentes empresas y el uso de API para acceder a datos tributarios”.
Finamente, el director del SII también declara la intención de su servicio de acelerar la adopción de servicios en la nube y de alcanzar un 100% de digitalización de trámites tributarios.

La Operación Renta genera en abril de cada año un aumento de la circulación de amenazas de ingeniería social como el phishing, riesgo que se ha visto acrecentado desde el año pasado gracias a las campañas maliciosas que se aprovechan de la pandemia y la vacunación para diseminar malware o robar datos".

CIBERCONSEJOS DE SEGURIDAD
OPERACIÓN RENTA 2021

Los phishing más comunes en la Operación Renta

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

ATENTO A LAS SEÑALES DE **PHISHING!**

- **Revisa** el remitente si recibes un correo electrónico relacionado a la devolución de impuestos o Coronavirus.
- **Nunca** ingreses tus contraseñas si no confías de un sitio.
- **Revisa** el contenido, que no sea alarmante o tenga faltas de ortografía.

Para estar preparados, te presentamos los phishing y sitios fraudulentos sobre la Operación Renta de los últimos años.

PHISHING 1
Supuesto remitente: **Tesorería Genera de la República**

Mensaje: El correo informa de obligaciones impagas, por lo que envía un enlace para descargar un formulario del Servicio de Impuestos Internos.


Tesoreria General de la República (TGR)

TGR
Tesorería General de la República

Estimado(a) Contribuyente

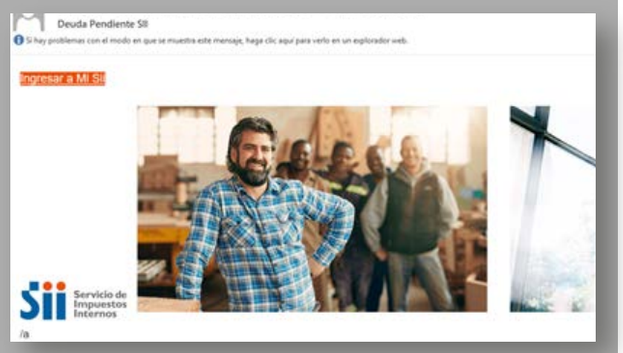
Tesoreria General d e la República (TGR): Le informa que existen obligaciones, producto de una liquidación tributaria que se encuentra impaga. Una liquidación tributaria corresponde a la determinación de diferencias de impuesto detectadas por el SII. Puede descargar el informe generado por el SII en el siguiente enlace:

Descargar Informe

¡ATENCIÓN! Esta entidad nunca envía e-mails solicitando descargar archivos y tampoco mensajes para que los usuarios entreguen datos personales.

PHISHING 2
Supuesto remitente: **Tesorería Genera de la República**

Mensaje: El correo informa de obligaciones impagas, por lo que envía un enlace para descargar un formulario del Servicio de Impuestos Internos.



¡ATENCIÓN! El SII no envía documentos adjuntos, excepto cuando el contribuyente lo ha solicitado.

PHISHING 3
Supuesto remitente: **Tesorería Genera de la República**

Mensaje: El correo informa de una multa e invita al cliente a descargar la restitución de declaración.

¡RECUERDA! El SII nunca solicitará datos personales, ni rut o contraseña secreta.


CASINO

INGENIERIA **SOCIAL**

La Ingeniería social es la práctica de obtener información sensible a través de la manipulación de usuarios para que éstos la revelen al atacante. Los atacantes utilizan esta técnica con el propósito de acceder en sistemas informáticos que les permitan realizar acciones para perjudicar, utilizar o exponer a las personas, organismos o comunidades que se ven comprometidos en el ataque.

El correo electrónico es el principal medio utilizado por los cibercriminales para cometer sus ataques utilizando esta técnica. No obstante, pueden utilizar otros canales de comunicación además del email, entre ellos se cuentan las llamadas telefónicas, los mensajes de texto y las redes sociales.

Los ataques de ingeniería social son, por lejos, la práctica más utilizada y exitosa para cometer delitos informáticos, lo que revela el descuido o la escasa importancia que las personas asignan a la información que poseen.

En un ataque de ingeniería social, los cibercriminales explotan condiciones básicas de la naturaleza humana como:

- La confianza de las personas en los demás, lo que es la base de cualquier ataque de ingeniería social
- La avaricia, la cual lleva a las personas a entregar información a cambio de una recompensa que no se va a concretar
- La ignorancia sobre el valor de los datos que las personas poseen o rol que desempeñan, convierten a una organización en un blanco fácil de ataque

¿Por qué la **ingeniería social es efectiva**?

- Porque a pesar de los protocolos, prevenir la ingeniería social tiene el desafío de que el comportamiento humano es impredecible
- Porque es difícil detectar una amenaza de ingeniería social
- No existe un método que permita dar completa seguridad a una organización frente a un ataque de ingeniería social
- No existe un software o hardware para defenderse contra un ataque de ingeniería social
- Este tipo de ataque es relativamente sencillo de implementar y su costo es mínimo

PRINCIPALES ATAQUES **ASOCIADOS A INGENIERÍA SOCIAL**

PHISHING:

Técnica por la cual el ciberdelincuentes mandan mensajes de correo electrónico con mensajes falsos, haciéndose pasar por empresas legítimas o personas de confianza para la víctima e instándole a hacer clic en enlaces, descargar archivos o enviar información personal sensible, como contraseñas.

SMISHING (PHISHING DE SMS):

Se trata del envío de mensajes de texto (SMS) o WhatsApp para comprometer a los usuarios a una interacción instantánea en la que, con el pretexto de ser un mensaje legítimo, guían a las personas a descargar un malware, visitar un sitio fraudulento o llamar a un teléfono falso, dónde requieren que éste divulgue información personal y detallada de sus cuentas.

VISHING:

Consiste en la suplantación a través de tecnología de voz (puede ser una llamada, un mensaje de voz), en la que se trata de engañar al individuo para revelar información crítica. En estas llamadas los delincuentes buscan engañar a los usuarios, haciéndoles creer diversas historias y situaciones que relatan a través del teléfono o mensaje.

RECOMENDACIONES PARA NO CAER EN EL **CUENTO DEL TÍO VERSIÓN DIGITAL**

DESCONFÍA de los correos y SMS que provienen de fuentes desconocidas.

CUIDADO con las ofertas que recibes. Si son muy buenas, duda.

NUNCA ingreses tus contraseñas si no confías en un sitio.

REVISAR que el enlace coincide con la dirección a la que apunta. Y, en cualquier caso, ingresar la url directamente en el navegador, sin copiar y pegar

NO ABRAS archivos ni utilices enlaces que estén dentro de un correo enviado por un remitente desconocido.

REVISA el contenido, que no sea alarmante o tenga faltas de ortografía.

COMPRUEBA el número de teléfono desde el que te hace una llamada antes de responder. Muchas compañías móviles, ya incluyen la posibilidad de bloquear llamadas no deseadas y de filtrar el spam, marcando cuando un número es sospechoso.

NINGUNA institución financiera o empresa te enviará un mensaje de texto en el que te pide que actualices la información de tu cuenta o que confirmes el código de tu tarjeta de crédito o cajero automático.

CONTACTA rápidamente a tu banco si revelaste información y cambia tus contraseñas inmediatamente.

Curiosidades: **Cada día**

- 156 millones de correos electrónicos de phishing son enviados
- Se abren 8 millones de correos electrónicos de phishing
- Se les da clic a 800 mil enlaces de correos electrónicos de phishing
- 80 mil personas son víctimas de estafa y entregan información personal a cibercriminales que intentan suplantar la identidad

Aunque el Phishing deber ser conocido para ti, existen otros ataques que tienen como fundamento la Ingeniería Social como:

1.– Baiting o Carnada

Consiste en tender una trampa y dejar un dispositivo de almacenamiento infectado -como un pendrive- en un lugar estratégico como lugares públicos con mucha afluencia de personas, para conseguir que los curiosos conecten este dispositivo infectado en sus equipos para ejecutar malware con el que pueden robar nuestros datos personales y/o tomar control del equipo, infectar la red y llegar al resto de dispositivos.

2.– Shoulder Surfing

Es una técnica mediante la que el ciberdelincuente consigue información de nosotros, como usuarios, mirando "por encima del hombro" desde una posición cercana, mientras que utilizamos los dispositivos sin darnos cuenta.
Puede darse en lugares públicos, como cafeterías o centros comerciales, y en transportes, mientras utilizamos nuestro equipo, o en cajeros automáticos.

[¿Sabías que 9 de cada 10 intentos de ataque por medio del shoulder surfing, fueron exitosos?]

3.– Dumpster Diving

Hay un dicho famoso que la mayoría seguro ha escuchado: «La basura de un hombre es el tesoro de otro».
Eso significa que lo que una persona considera inútil podría ser de gran valor para la otra. El concepto de Dumpster Diving se basa en esto. Indagar por información en la basura, tal como se señala en la traducción, se trata de acceder a elementos eliminados en la basura por la víctima, como borradores de documentos, información de contactos, códigos, etc.

Los usuarios de internet le hemos hecho el trabajo más fácil a los delincuentes, ya que, en general, publicamos una gran cantidad de información sobre nuestra identidad, rutinas y familias a través de las redes sociales. Gracias a eso, los delincuentes pueden hacerse pasar por familiares o jefes de la persona objetivo, revistiendo a sus mensajes de urgencia y autoridad.

De eso se trata la ingeniería social, de un grupo de técnicas que hay que tener particularmente en cuenta durante marzo y abril, ya que la Operación Renta del Servicio de Impuestos Internos (SII) genera un aumento de los casos de phishing, íntimamente relacionado con este fenómeno.

PHISHING: BRASIL PRINCIPAL OBJETIVO DE ATAQUE EN EL MUNDO

Brasil es uno de los países que más ataques de phishing sufre en la región, y la doctora Elba Vieira nos explica por qué y cómo ha afectado la pandemia a su popularidad. Asimismo, detalla las principales acciones contenidas en la estrategia brasileña de ciberseguridad, E-Ciber, para combatir los riesgos existentes en el mundo digital

Elba Vieira : Doctora en Ciencias de la Información de la Universidad Federal da Bahia y fundadora de la consultora Solare.

Las nuevas tecnlogías son cada vez más usadas por los criminales para dificultar su identificación y la defensa contra sus ataques. Junto con ello, utilizan técnicas para explotar la fragilidad humana y sentimientos como miedo, curiosidad, empatía, pena y tantos otros. Como indica Kevin Mitnick, la ingeniería social es un "arte teatral" y a través de ella es posible "hacer que las personas hagan cosas que normalmente no harían para un extraño". El experto agrega una frase que se ha hecho famosa: "el factor humano es el más débil de la seguridad".

En este contexto se enmarcan el phishing y su éxito. Al inicio de la pandemia, en abril de 2020, pudimos observar el avance de los números relacionados con ataques cibernéticos en los países de América Latina. Según números de Kaspersky, tan solo en ese mes, Brasil recibió más del 60% de los ataques identificados por la empresa en América Latina.

Y este mes de marzo, la firma rusa publicó que "los brasileños son los principales objetivos de ataques de phishing en el mundo", debido, entre otros motivos, al mayor uso de las redes sociales, el aumento las personas trabajando de forma remota (y con recursos propios) y una búsqueda intensa de información respecto de la pandemia.

Así, de acuerdo con Kaspersky, "la emergencia sanitaria protagoniza muchos de los ataques de phishing,

que buscan robar información como datos personales, credenciales de cuentas online y, principalmente, contraseñas bancarias. Las maniobras usadas por los criminales fueron desde ofertas de máscaras y alcohol gel a falsas inscripciones para programas de auxilios sociales, registro para el sistema de pagos PIX y, más recientemente, páginas fraudulentas de inscripción para recibir la vacuna".
La misma firma rusa indicó en otro estudio que "la tendencia general de crecimiento de los ataques dirigidos contra el sector corporativo continuará el próximo año, aún más porque el modo de trabajo remoto, cada vez más popular, vuelve a los funcionarios más vulnerables".

Las nuevas tecnologías son cada vez más usadas por los criminales para dificultar su identificación y la defensa contra sus ataques. Junto con ello, utilizan técnicas para explotar la fragilidad humana y sentimientos como miedo, curiosidad, empatía, pena y tantos otros. Como indica Kevin Mitnick, la ingeniería social es un "arte teatral" y a través de ella es posible "hacer que las personas hagan cosas que normalmente no harían para un extraño". El experto agrega una frase que se ha hecho famosa: "el factor humano es el más débil de la seguridad".
En este contexto se enmarcan el phishing y su éxito. Al inicio de la pandemia, en abril de 2020, pudimos observar el avance de los números relacionados con ataques cibernéticos en los países de América Latina. Según números de Kaspersky, tan solo en ese mes, Brasil recibió más del 60% de los ataques identificados por la empresa en América Latina.
Y este mes de marzo, la firma rusa publicó que "los brasileños son los principales objetivos de ataques de phishing en el mundo", debido, entre otros motivos, al mayor uso de las redes sociales, el aumento las personas trabajando de forma remota (y con recursos propios) y una búsqueda intensa de información respecto de la pandemia.
Así, de acuerdo con Kaspersky, "la emergencia sanitaria protagoniza muchos de los ataques de phishing, que buscan robar información como datos personales, credenciales de cuentas online y, principalmente, contraseñas bancarias. Las maniobras usadas por los criminales fueron desde ofertas de máscaras y alcohol gel a falsas inscripciones para programas de auxilios sociales, registro para el sistema de pagos PIX y, más recientemente, páginas fraudulentas de inscripción para recibir la vacuna".
La misma firma rusa indicó en otro estudio que "la tendencia general de crecimiento de los ataques dirigidos contra el sector corporativo continuará el próximo año, aún más porque el modo de trabajo remoto, cada vez más popular, vuelve a los funcionarios más vulnerables".

La concienciación **es clave**

No hay una solución mágica para resolver este problema. Es importante aplicar medidas con eje en las personas, los procesos y las tecnologías, para aumentar la superficie de protección de las organizaciones. Entender por qué las personas erran es una de las mejores tácticas para construir programas de concientización.

Un estudio de la Universidad de Stanford explica algunos de los factores psicológicos tras el éxito del phishing. Un **25% de los funcionarios** encuestados dijo haber hecho clic en un email de phishing en el trabajo, con un 34% de hombres señalando que hicieron clic en un link de un email de phishing contra **17% de las mujeres.**
Asimismo, la distracción y el trabajo remoto colaboran. Según el estudio, 45% de los entrevistados citaron la distracción como el principal motivo de caer en un phishing, mientras que un **57% de los trabajadores** admitió distraerse más trabajando en casa que en la oficina.

La respuesta de Brasil

En Brasil se observa un movimiento de preocupación de las organizaciones hacia la prevención del crimen cibernético. Recientemente, el Conselho Monetário Nacional (CMN) actualizó sus reglas para las instituciones financieras brasileñas en lo respectivo a seguridad cibernética y contratación de servicios de procesamiento y almacenamiento de datos y de computación en la nube, debiendo además establecer y documentar criterios ante crisis causadas por ataques cibernéticos.

Además, la propia Autoridade Nacional de Proteção de Dados (ANPD), responsable de velar por la protección de datos en el país, definió en su planificación estratégica el fortalecimiento de las organizaciones brasileñas y de los ciudadanos, incentivando y promoviendo eventos de capacitación sobre temas de protección de datos personales y, por consecuencia, de ciberseguridad.

Brasil posee algunos instrumentos robustos relacionados con el tema de la ciberseguridad. Una de ellas es la Estratégia Nacional de Segurança Cibernética (E-Ciber), que además de llenar vacíos en el marco normativo del país, tiene como visión para Brasil "convertirse en un país de excelencia en ciberseguridad. Y entre sus objetivos estratégicos está volver a Brasil más próspero y confiable en el ambiente digital, aumentar la resiliencia del país ante amenazas cibernéticas y fortalecer el actuar de Brasil en el escenario internacional.

E-Ciber formaliza diversas acciones estratégicas, que deben ser aplicadas por las organizaciones. Ellas incentivan el fortalecimiento de medidas de gobernanza cibernética, la colaboración público-privada y con la sociedad, una elevación del nivel de protección de las infraestructuras críticas, el uso de soluciones innovadoras en ciberseguridad y una ampliación de la cooperación internacional, entre otras importantes medidas.

De esta forma, la parte I de E-Ciber contiene un diagnóstico donde nota que, en ataques cibernéticos recientes, grupos de hackers han tenido a los sistemas del gobierno como objetivos, y que entre los principales tipos de amenaza contra la administración pública están precisamente los phishing, junto a ataques DDoS, liberación de datos privados, espionaje y terrorismo cibernético e interrupción de servicios.
Por lo anterior, las organizaciones públicas y privadas deben establecer políticas y procedimientos de ciberseguridad que sean mejorados periódicamente, junto a la capacitación continua de todos los colaboradores.

E-Ciber es una importante herramienta y guía para que las organizaciones direccionen sus estrategias y planes a la pregunta de la ciberseguridad. Finalizando con una cita de Bruce Scheiner, "todos se deben esforzar: usuarios y consumidores, gobiernos y reguladores, empresas e inversionistas. Un futuro de éxito para nuestras economías digitales depende de la integración de los principios de ciberseguridad, como privacidad y seguridad por diseño desde el inicio del desarrollo de la tecnología".

Tendencia Digital

EVOLUCIÓN Y PRESENTE **DEL PHISHING**

El phishing es hoy el modo más extendido de ataque cibernético y el principal exponente de la ingeniería social. ¿Qué debemos tener en cuenta para no caer en sus redes y convertirnos en una nueva presa de los ciberdelinucuentes?

Con un nombre inspirado por la “pesca” (“fishing”, en inglés) que realizan de sus víctimas, el phishing es un tipo de ataque se disemina generalmente por correo electrónico, ofreciendo como “carnada” mensajes aparentemente urgentes o beneficiosos, diseñados para parecer fuentes confiables para la víctima, como empresas y familiares o amigos.

La “pesca” se concreta cuando la potencial víctima realiza la acción deseada por los atacantes, como puede ser el hacer clic en sitios que descargan malware, el enviar datos personales a los delincuentes, o el realizarles una transferencia de dinero.

Fases de un ataque **de ingeniería social**

INVESTIGAR EL OBJETIVO:
El criminal recolecta información sobre la organización o persona a la que quiere atacar, la que puede ser reunida, por ejemplo, a partir de datos públicos de las organizaciones o en internet.

SELECCIONAR A LA VÍCTIMA:
El atacante elige a su objetivo. En una organización, por ejemplo, un trabajador frustrado es un buen candidato.

ESTABLECER UNA RELACIÓN:
Aquí se genera un vínculo con la víctima elegida, para que confíe en el atacante y sea más fácil aprovecharse de ella.

EXPLOTAR LA RELACIÓN:
El criminal usa el vínculo cimentado con la víctima para obtener la mayor cantidad de información sensible y datos personales, o hacer que descargue un archivo malicioso.

Claves para **identificar un Phishing**

Técnicas identificables como lo que hoy se conoce como phishing han existido por al menos 30 años, y en todo este tiempo, por supuesto, no han dejado de evolucionar.

Entre los ejemplos destacados está el famoso fraude del príncipe nigeriano, o estafa 419, que tiene antecedentes en similares engaños efectuados antiguamente a través de cartas.

En esta modalidad, los delincuentes distribuyen un email donde una persona, supuestamente un príncipe millonario, explica que necesita ayuda para sacar su fortuna del país. Y si el receptor le ayuda, le dará una parte. Para lograrlo, la víctima debe realizar un pago (relativamente pequeño, en comparación con la recompensa) por adelantado a este supuesto príncipe, lo que por supuesto no es más que la consumación de la estafa.

Un truco clave usado por los malhechores para el spear phishing es el denominado spoofing, cuando se registra la dirección de correo electrónico con un nombre falso en el área que se despliega como nombre del remitente. Por eso, es clave siempre fijarse en la dirección real de quien envía el email (y particularmente el dominio, la parte que va después del @). Si no coinciden con el nombre que aparece como “from” o remitente, se trata muy seguramente de un correo malicioso.

Otra tendencia importante es que cada año los ataques de phishing se concentran en fechas donde las personas realizan transacciones online, como la Operación Renta, la Navidad y, recientemente, los retiros de fondos previsionales.

ALGUNAS VARIANTES **DEL PHISHING**

Spear phishing: Variante del phishing donde el destinatario es una persona en específico, a la cual se debe investigar previamente de forma exhaustiva.

Pharming: Es un phishing a gran escala, a través de redirigir el tráfico de una web hacia un sitio fraudulento, ya sea a través del uso de malware en el equipo de la víctima, o de comprometer un servidor DNS.

Whaling: Phishing cuyo objetivo son los "peces gordos" dentro de una organización (por eso "whaling", "caza de ballenas"), como el gerente general, altos funcionarios públicos y políticos o celebridades.

Repackaging: El cibercriminal incluye malware en una aplicación legítima, para difundir su programa malicioso entre quienes creen estar descargando un programa seguro.

PARA FIJARSE Y **SOSPECHAR**

1.– Nadie le ofrecerá dinero por realizar una simple transacción o por hacer clic en un enlace.

2.– Nunca envíe dinero por adelantado ante una solicitud por email.

3.– Desconfíe cuando se le llame a actuar rápido para aprovechar una oportunidad o por un supuesto riesgo.

4.– Sospeche si el remitente solicita confidencialidad, pide ayuda urgente o apela al fervor religioso.

5.– Tenga cuidado con fotos y documentos, son fáciles de falsificar, no son prueba de la autenticidad.

6.– No haga clic en mensajes que prometan imágenes de fotos íntimas o videos morbosos.

7.– Los correos de phishing suelen ser impersonales, a "cliente" o "usuario", en vez del nombre del destinatario.

8.– Atención con mensaje que esté redactado de forma incorrecta o con palabras equivocadas.

9.– Tener especial cuidado con fechas como la Operación Renta como Navidad o el "Cyber Monday".

10.– Nunca hacer clic en enlaces de bancos o tiendas. Visite sus páginas escribiendo sus direcciones en el navegador.

LOS GRUPOS QUE INSPIRAN **SUMAN MUJERES A LA CIBERSEGURIDAD**

Las mujeres continúan su batalla por ocupar una mayor proporción de los puestos de trabajo en aquellos sectores que siguen dominados por los hombres. Un área donde esta diferencia es muy notoria es precisamente en el mundo de la ciberseguridad. Por eso cada día se forman más grupos e iniciativas para incluir más mujeres en este ámbito laboral. Estos son algunos de ellos.

HACKADA

Hackada es una comunidad nacida a mediados del año pasado, a partir de mujeres que, hasta ese momento, compartían dentro de otros grupos de ciberseguridad e informática dominados por hombres. Su objetivo fue formar una comunidad solo para mujeres, donde existiera un espacio seguro y empático donde compartir experiencias y apoyarse mutuamente ante cualquier dificultad que encontraran en sus lugares de trabajo, casi exclusivamente masculinos.

Desde entonces, el grupo ha crecido y hoy está conformado por 118 participantes, quienes comparten sus conocimientos con el resto de las chicas y realizan actividades para visibilizar a la mujer en ciberseguridad y empoderar a las chicas interesadas en entrar a este rubro.

WOMCY
LATAM Women in Cybersecurity

Womcy es una organización que ofrece asesorías en ciberseguridad enfocadas en minimizar la brecha de género en ciberseguridad en toda América Latina. Ofrece varios programas distintos, para públicos empresariales, universitarios y escolares, uno de estos últimos enfocado en niñas entre 14 y 17 años, llamado Womcy Girls. Asimismo, mujeres interesadas en compartir sus experiencias en el rubro con las chicas pueden postular para convertirse en conferencistas.

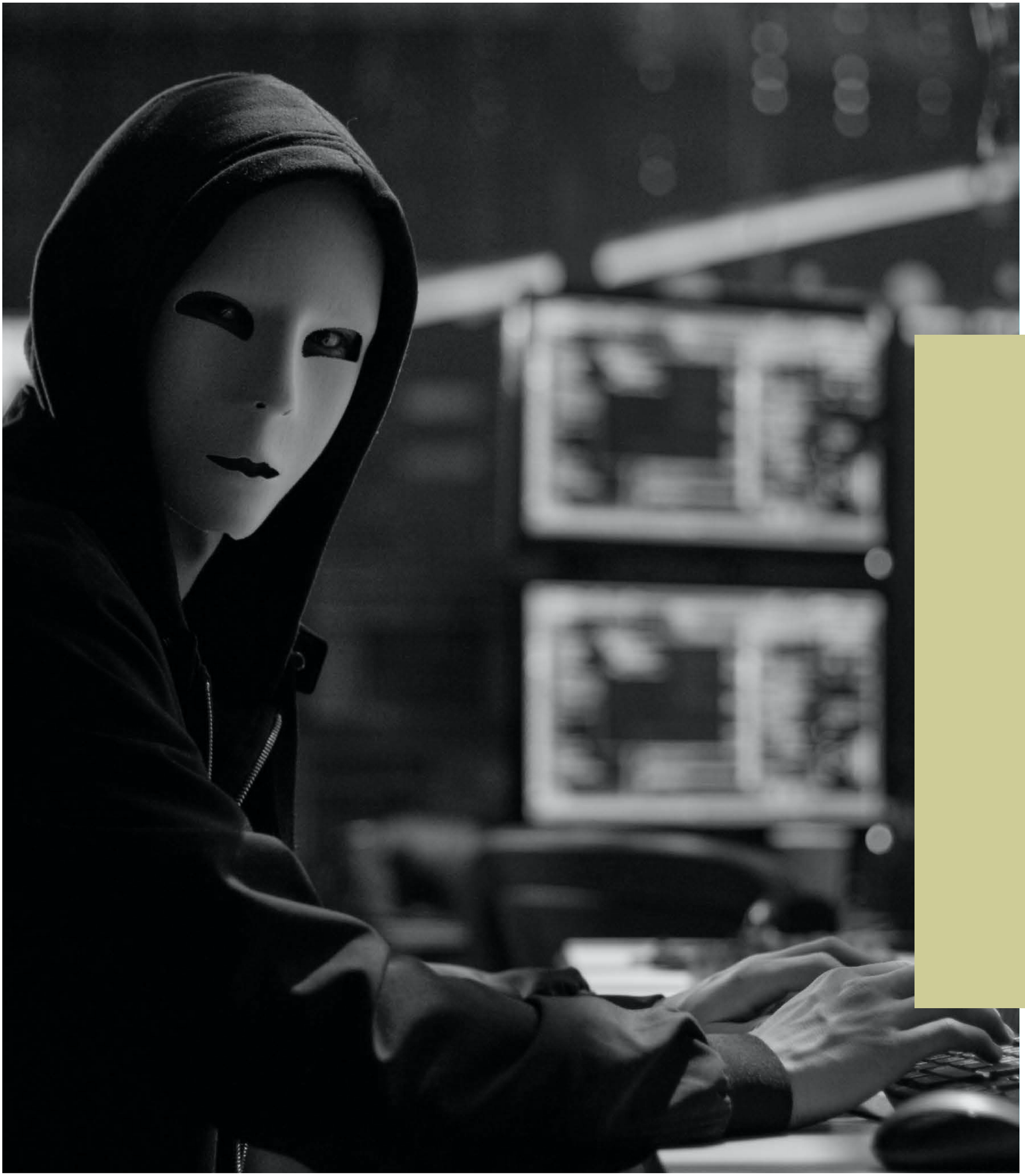
Inspiringgirls

Inspiring Girls tiene como norte la eliminación de estereotipos en la tecnología, resaltando la presencia de mujeres en campos como la biotecnología, a través, entre otros métodos, de programas de habilidades STEM para niñas y de actividades en colegios por parte de mujeres profesionales de estas áreas, que actúan como embajadoras voluntarias.
También hacen cursos para desarrollar habilidades sociales en las chicas, gestionar sus emociones y generar autoestima, seguridad personal, y generar capacidades de comunicación digital, entre muchos otros.

TECHNOVATION
Girls Chile

Technovation Girls Chile es una fundación que realiza actividades de motivación en habilidades STEM (ciencia, tecnología, ingeniería y matemáticas) y habilidades digitales para niñas entre 10 y 18 años, con el objetivo declarado de fomentar que, en algunos años más, más mujeres sean parte del mundo laboral en los campos relacionados con la ciencia y la tecnología.
Su actividad más destacada es el Technovation Challenge, que desafía a las niñas a trabajar en equipo y competir por desarrollar la mejor app.

Legal



ENGAÑOS EN LÍNEA Y DELITOS: **EL PHISHING**

Antes que el fraude actualmente masificado donde un SMS falso nos pide el reenvío de un código de autenticación de Whatsapp, fue y sigue siendo práctica recurrente recibir un correo electrónico supuestamente de nuestra entidad financiera, pidiendo conectarnos a su sitio web para actualizar o verificar las contraseñas y claves de acceso. En derecho, se trata de una conducta intencional y dolosa donde, mediando un engaño o la simulación de ser una petición bancaria, se busca que el sujeto pasivo al cual se le acceden o "pescan" las claves de autenticación realice una conducta concreta, que a la postre le ocasionará un perjuicio patrimonial al realizarse una transferencia bancaria no autorizada a un tercero.

Renato Jijena Leiva
Profesor Derecho Informático PUCV

Se olvida que siempre hay dos víctimas afectadas en su patrimonio, la inmediata o directa que es el titular de la tarjeta o de la cuenta corriente que entrega sus claves, y la mediata o indirecta que es el administrador del sistema bancario cuyo patrimonio y confidencialidad tecnológica se vulnera, y por eso son jurídicamente cuestionables sentencias de los tribunales de mal fundamento jurídico y construidas en base a entelequias, atribuyendo siempre y a priori la responsabilidad a los bancos sólo porque son depositarios de los fondos debitados.

Es un mito jurídico mayor declarar que se trata de conductas no sancionables en Chile y que debemos apurar una nueva tipificación de delitos informáticos. En una modalidad de "concurso de delitos" son aplicables tres tipos penales diversos que "subsumen" cabalmente el ilícito, a saber: el tipo penal de fraude o engaño del Código de 1875; el tipo de acceso indebido a la información de un sistema del artículo 2° de la ley 19.223, que es una figura amplia y genérica; y el tipo penal nuevo de la ley 20.009 que castiga al que mediante cualquier engaño o simulación obtenga o vulnere la información y medidas de seguridad de una cuenta corriente bancaria, de una cuenta de depósito a la vista, de una cuenta de provisión de fondos, de una tarjeta de pago o de cualquier otro sistema similar, para fines de suplantar al titular o usuario y efectuar pagos o transacciones electrónicas.

Desde la perspectiva de la ingeniería social que nos convoca..., si un porcentaje mayoritario de los chilenos teme que las transacciones financieras en línea, sin presencia de plástico, son vulnerables, delitos informáticos como el engaño "espejeando" y simulando la conexión a un sitio web bancario lo explican. Es una percepción que se despeja cultural, técnica y legalmente, pero especialmente desde la perspectiva técnica de la Seguridad de la Información. ¿Será invirtiendo cifras millonarias en sistemas, auditorías, certificaciones y capacitaciones en seguridad física y lógica?, pues no, más que un tema de monto de recursos es un problema acerca de la idoneidad de las medidas técnicas y organizativas que se implementen para resguardar la integridad, la disponibilidad y la confidencialidad de un sistema de gestión en línea de fondos o valores.

La seguridad de sistemas es esencialmente prevención y en menor medida reacción ante las contingencias. Sólo previniendo se es diligente y se demuestra la responsabilidad debida, para así aminorar la posibilidad de que los riesgos inherentes se traduzcan en perjuicios indemnizables, y eso debe trabajarse en conjunto con las áreas de riesgo, de tecnología y jurídica o de Fiscalía. Pero estas últimas siguen en una especie de divorcio profesional que creíamos superado.

La respuesta concreta ante el phishing desde la óptica de los SGSI o de la ciberseguridad provino diligentemente de los responsables: además de la clave de acceso inicial al sistema bancario, para una transferencia siempre se pide una segunda clave o coordenada aleatoria y una tercera que se remite al celular del usuario, es decir, al sujeto activo del delito ya no le es suficiente conseguirse sólo el RUT y el password de la víctima. Y bueno, si además del mensaje estándar de que "el banco nunca le pedirá sus claves" un sistema así de verificación de identidad en tres niveles no se ha implementado, si podríamos imputar con fundamento negligencia grave al banco y exigir indemnizaciones de perjuicios.

Desde otra perspectiva. Cuando un prestador de servicios ofrece usar Internet para transacciones o pagos electrónicos, y su cliente acepta la oferta de la mano de un contrato de adhesión para el uso de canales digitales, debe hacerlo bajo el paraguas del artículo 23 de la ley del consumidor, es decir, garantizando -a priori- que no actuará con negligencia o causando menoscabo por fallas y deficiencias de seguridad. Pero en la otra orilla del contrato entonces, el cliente y consumidor también debe asumir una carga de diligencia o cuidado de sus claves de acceso y mecanismos de autenticación, bastante menor, más pasiva, de menor costo, pero necesaria y exigible por seguridad, para la fiabilidad del sistema y en equidad. Y en definitiva si el equilibrio necesario además de cultural y técnico también debía ser normativo o legal, además de un tipo penal específico para sancionar al sujeto activo del delito, de la mano de herramientas como la misma ley 20.009 desde el año 2005 se ha limitado la responsabilidad de los usuarios de tarjetas, articulándose en Chile un sistema obligatorio -para bancos y casas comerciales- de avisos y bloqueos en casos de hurtos, robos y extravíos, y estableciéndose de cargo del proveedor demostrar que el propio tarjetahabiente no realizó la transacción fraudulenta.

CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

CSIRT
https://www.csirt.gob.cl/

Teatinos 92 piso 6
Santiago, Chile

CONTÁCTANOS
+(562) 2486 3850

registra un incidente

Síguenos

Twitter de CSIRT
https://twitter.com/csirtgob/

LinkedIn
https://www.linkedin.com/company/csirt-gob/

Youtube
https://www.youtube.com/channel/UCua0E5Jz9V1Rn-VtLHPP4Nw/

Instagram
https://www.instagram.com/csirtgobcl

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Teatinos 92 piso 6
Santiago, Chile
www.csirt.gob.cl