UNIDOS POR LA CIBERSEGURIDAD FEBRERO 2022

PHISHING

EN AMÉRICA

Global Cyber

soluciones integrales en ciberseguridad

INTRODUCCIÓN

Podemos estar orgullosos de celebrar un día como el de la seguridad de la internet. Hemos avanzado mucho en poco tiempo. Nuestras sociedades son capaces de crear sistemas que garantizan que el intercambio de comercial y el tránsito de información entre los usuarios de los servicios en internet y las organizaciones sea seguro. También hemos logrado madurar entre las empresas e instituciones de nuestros países la necesidad de contar con estrategias de ciberseguridad.
Si bien no está todo resuelto -y en cuanto a la ciberseguridad en la internet, nunca estará todo resuelto-, nuestras sociedades están mostrando mayor resiliencia y están comenzando a fomentar la concientización entre los usuarios de internet, desde las edades más tempranas posibles, para que podamos entender que con esta poderosa herramienta de comunicación también hay asociado un riesgo.

La consigna en esta oportunidad es que entre todos podemos crear una internet segura. Estamos llamados a crear esfuerzos comunes para prevenir incidentes, crear conciencia y estar preparados para enfrentar a los desafíos que nuestra hiperconectada realidad. Las tecnologías de la información están cambiando al mundo, y debemos adaptarnos a esos cambios con ciberseguridad.

¿Qué es la Ingeniería social?

La Ingeniería social es la práctica de obtener información sensible a través de la manipulación de usuarios legítimos 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, las 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.

CONTACTO@GLOBALCYBER.CL

Global Cyber
soluciones integrales en ciberseguridad

¿Por qué somos vulnerables frente a un ataque de ingeniería social ?

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

1. La confianza de las personas en los demás, es la base de cualquier ataque de ingeniería social
2. El sentido de la obligación moral de las personas
3. La avaricia lleva a las personas a entregar información a cambio de una recompensa que no se va a concretar
4. El miedo a pérdidas mayores en caso de no cumplir con los requerimientos del atacante
5. 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

CONTACTO@GLOBALCYBER.CL

Global Cyber
soluciones integrales en ciberseguridad

¿Qué daños puede causar un ataque de ingeniería social?

- Pérdida de información personal de los miembros y usuarios de la organización: para las organizaciones, especialmente las de gran tamaño, perder información confidencial podría generar la pérdida de confianza de actuales usuarios y potenciales clientes en una organización o negocio, optando estos últimos por descontinuar los servicios con la entidad afectada.

- Pérdida de información crítica o confidencial: la información sensible de alguna operación podría ser utilizada por competidores para tener acceso a desarrollos y estrategias de la organización.

- Pérdidas económicas: la pérdida de confianza e información sensible, puede tener como consecuencia el retiro o cancelación de inversiones y la pérdida económica.

- Daño en la imagen pública: una entidad afectada por un ataque debe invertir mucho para mejorar su imagen pública para restaurar la confianza en sus productos y servicios.

CONTACTO@GLOBALCYBER.CL

Global Cyber
soluciones integrales en ciberseguridad

¿Por qué la ingeniería social es efectiva?

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

1. Porque a pesar de los protocolos, prevenir la ingeniería social tiene el desafío de que las personas son susceptibles a cambiar e impredecibles

2. Porque es difícil detectar una amenaza de ingeniería social

3. No existe un método que permita dar completa seguridad a una organización frente a un ataque de ingeniería social

4. No existe un software o hardware para defenderse contra un ataque de ingeniería social

5. Este tipo de ataque es relativamente sencilla de implementar y su costo es muy bajo

CONTACTO@GLOBALCYBER.CL

Fases de un ataque de ingeniería social

Investigar al objetivo	En esta fase, el criminal recolecta la información sobre la organización a la que quiere atacar. La información puede ser reunida a partir de datos públicos de la propia organización, información general de internet, datos de los miembros de la entidad y otros.
Seleccionar a la víctima	En esta etapa el atacante selecciona a una persona de la organización.
Establecer una relación	Esta etapa del ataque incluye generar una relación con la persona seleccionada, de tal modo que la víctima no pueda identificar las intenciones encubiertas. Mientras mayor sea el nivel de confianza, más sencillo será para el atacante obtener información de la víctima.
Explotar la relación	El atacante explota al máximo la confianza de la víctima y recolecta la mayor cantidad de información sensible de ésta, como el nombre de usuario, la contraseña, y otros detalles.

CONTACTO@GLOBALCYBER.CL

¿Qué es el phishing?

El phishing es un tipo de ataque de ingeniería social en el que los cibercriminales engañan a las víctimas para que entreguen información confidencial o instalen malware.
En la mayoría de los casos, lo hacen a través de correos electrónicos maliciosos que parecen provenir de remitentes confiables.
Los atacantes registran dominios web falsos, crean sitios idénticos y luego envían el correo falso a cientos de personas.

Cuando un usuario hace click en un enlace, es dirigido al sitio falso, dónde el atacante convence a la víctima para compartir información sensible, personal, financiera o comercial. La persona, desprevenida de estar en un sitio de phishing, compartirá la información porque está convencido de que interactúa con una entidad legítima.

Una de las razones por la que un phishing es exitoso, es por la falta de conocimiento sobre esta amenazas entre los usuarios, el engaño visual del correo y del sitio fraudulento, y la falta de atención que las personas ponen en los detalles e indicadores de seguridad.

¿Sabías qué...? Diariamente

- 156 millones de correos electrónicos de phishing son enviados
- Se abren 8 millones de correos electrónicos de phishing
- Se hace clic en 800,000 enlaces de los correos electrónicos de phishing
- 80,000 personas son víctimas de estafa y entregan información personal a cibercriminales

CONTACTO@GLOBALCYBER.CL

Automatizar la detección y eliminación del phishing

Carlos Landeros Cartes
CoFundador y CEO en GlobalCyber

Los primeros en advertir sobre la existencia de un phishing en el ciberespacio suelen ser las personas que se encuentran con correos con mensajes, enlaces o archivos maliciosos adjuntos en sus bandejas de entrada, en cadenas de WhatsApp o por SMS en sus teléfonos móviles.

La suspicacia o habilidad de los usuarios para detectar un phishing, pero sobre todo para denunciarlo, suele ser la primera notificación para activar las respuestas entre los SOC y CSIRT en nuestra región. Entre las organizaciones y empresas, algunos de los equipos de seguridad más avanzados cuentan con capacidades para la extracción manual de logs y registros de phishing en plataformas antispam o de servidores de correos.

Y con posterioridad al inicio de la gestión de ciberseguridad, en muchos casos, los métodos que utilizan los equipos de seguridad TI para la supervisión del progreso en la mitigación de ese phishing sigue siendo manual, con el apoyo de tecnologías.

Hay una evidente necesidad de contar con herramientas y mecanismos automatizados para detectar y eliminar la amenaza del phishing antes de su distribución y redistribución entre los usuarios de servicios y el público en general.

Implementar soluciones para detectar y eliminar tempranamente un phishing es mucho mejor que notificar alertas sobre un incidente que se está mitigando. Y aunque crear habilidades entre los usuarios en general a través de campañas de concientización es muy importante, no está garantizado que sea más eficiente que la gestión anticipada de una bien implementada herramienta de seguridad.

Los tres conceptos esenciales que debemos tener en cuenta para adoptar esa solución tecnológica, en base a herramientas ya existentes, simples y sin costos de licenciamiento que pueden estar en cualquier SOC o CSIRT son:

• Detectar la creación de nombres de dominios intencionalmente semejantes a algunos ya existentes, que a futuro puedan alojar sitios fraudulentos para un phishing. Esta gestión se puede hacer en la etapa de inscripción de estos, en el registrador de nombres de dominio nacional o global.

• Detectar sitios web en el TLD nacional o global que ya están inscritos y que puedan ser utilizadas como sitios web para ejecutar el phishing a través de la identificación de parámetros comunes que tienen estos sitios ya desarrollados.

• Ejecutar procedimientos rutinarios de revocación de nombres de dominio de manera automatizada, tanto en su etapa inicial -en la inscripción del nombre de dominio-, como en la etapa de funcionamiento estable del sitio web en Internet.

Modernizar un SOC o CSIRT es posible siguiendo estas recomendaciones y los resultados, con conocimiento de causa, son rápidos y efectivos.

CONTACTO@GLOBALCYBER.CL

Cifras alarmantes

- Google registró 2,1 millones de sitios de phishing en 2021, un 27% más que en 2020
- El PDF fue el tipo de archivo adjunto más utilizado en un ataque de phishing
- EL 24% de los correos de phishing contienen archivos maliciosos adjuntos
- Al menos una persona hace clic en un enlace de phishing en el 86% de las organizaciones
- Las credenciales, los datos personales y registros médicos son los tres principales tipos de datos comprometidos en un ataque de phishing
- Los servicios financieros sufrieron 60% más de ataques de phishing que cualquier otra área en 2021
- El 91 % de los ataques exitosos reportados, comenzaron con un correo malicioso
- En un 62% aumentaron las campañas de phishing tras la implementación del trabajo remoto
- En promedio, los trabajadores de las empresas reciben 14 correos maliciosos al año
- 96% de los ataques de phishing son a través de correos electrónicos, 3% por sitios maliciosos y 1% vía smartphone

Fuentes: Reportes de Tessian, Cisco, Microsoft y Verizon

Global Cyber
soluciones integrales en ciberseguridad

CONTACTO@GLOBALCYBER.CL

El informe Data Breach Investigations Report de VERIZON de 2021 muestra que el phishing sigue siendo la principal acción de amenaza utilizada en las filtraciones exitosas. Los ciberdelincuentes robaron credenciales de acceso en el 85% de las violaciones relacionadas con la ingeniería social.

Principales servicios suplantados por pishing

·Entidades y servicios bancarios
·Compañías telefónicas, eléctricas, de agua, gas o cualquier otro servicio.
·Empresas de mensajería
·Administración Pública
·Redes sociales
·Plataformas de compraventa o de subastas, tiendas online.
·Servicios de pago online
·Juegos online
·Servicios de correo y almacenamiento en la nube
·Soporte técnico

Frecuentemente vemos casos de Phishing por correo electrónico, siendo el de mayor impacto para las empresas el **ataque BEC (Business Email Compromise)** que busca suplantar la identidad de un alto ejecutivo de la organización.

CONTACTO@GLOBALCYBER.CL

Global Cyber
soluciones integrales en ciberseguridad

PHISHING EN AMÉRICA

Este informe es un testimonio del trabajo que muchos países de América Latina están realizando para enfrentar el phishing en cada una de nuestras sociedades. Pero también es un manifiesto sobre la voluntad que tenemos para coordinar ese trabajo.

Las sociedades estamos avanzando en esa coordinación mucho más rápido de lo que nuestras legislaciones lo hacen. Los equipos de seguridad TI en organizaciones y empresas están cada vez más abiertos a compartir información de inteligencia entre ellos. Lo que necesitamos es crear más instancias para fomentar ese intercambio y madurar nuestras estrategias de ciberseguridad con esos contenidos.

A ello debemos sumar los esfuerzos por crear concientización entre los usuarios y perspectivas ágiles de gestión en el trabajo de nuestros equipos, para que podamos hacer frente a las amenazas cibernéticas.
El phishing es una amenaza que trasciende a las sociedades a nivel planetario. Las iniciativas para enfrentarla siempre serán insuficientes sino estamos unidos y bien coordinados.

Nuestro objetivo es fomentar una comunidad que madure para enfrentar a los ciberatacantes, atenuar su acción en América Latina y mitigar el impacto que pueda generar entre nuestras organizaciones.

Queremos agradecer a grandes amigos y profesionales que aceptaron la invitación ha colaborar en este trabajo.
Sus diferentes perspectivas y énfasis sobre el escenario del phishing en cada uno de los países de América son un aporte muy relevante en el desafío que estamos enfrentando para mejorar nuestra ciberseguridad.

Global Cyber
soluciones integrales en ciberseguridad

Phishing en Chile

Katherina Canales Madrid
Especialista en estrategias de Ciberseguridad
CoFundadora y COO en Globalcyber

La importancia de la concientización en ciberseguridad se define en la habilidad que tienen las personas para reconocer que están frente a una amenaza. A pesar de que las organizaciones son las responsables finales de gestionar el riesgo cibernético y mitigar un incidente, son las personas las que están directamente expuesta a los ciberataques, eso porque el phishing sigue siendo la principal amenaza a la ciberseguridad.

A nivel global, el 90% de las infracciones de seguridad detectadas en las organizaciones durante 2021, se iniciaron por un clic desprevenido en un enlace o archivo malicioso. Esto es producto de una combinación entre la siempre insuficiente concientización y el aumento de la superficie de ataque por la implementación del trabajo remoto.

Y aunque las organizaciones han mejorado mucho sus capacidades con respecto al inicio de la pandemia, el phishing sigue siendo la principal amenaza a la ciberseguridad, porque los atacantes supieron mutar más rápido que los expertos para explotar los escenarios de incertidumbre en los que el mundo se vio envuelto.

Reflexionar sobre el estado del phishing en Chile es -y será- siempre pertinente al hablar de ciberseguridad. Pero seguirá siendo una discusión cualitativa o especulativa mientras nuestro país no cuente con una legislación que permita crear o formalizar las instancias para gestionar los incidentes y acumular inteligencia sobre cada tipo de amenaza.

CONTACTO@GLOBALCYBER.CL

Global Cyber
soluciones integrales en ciberseguridad

Si se trata de evaluar lo que se ve y lo que subyace, podemos decir que los titulares sobre incidentes de ciberseguridad han disminuido en los últimos meses. La conclusión lógica es que las empresas y organizaciones son capaces de responder gestionar el riesgo, pero entre líneas podemos especular que son capaces de mitigar el impacto de los ataques de los que han sido víctimas, al menos lo suficiente para que no sean notorios más allá de las propias organizaciones.

Por un lado, es inevitable pensar que estamos bien si no hablamos de la amenaza. Pero si la estadística global dice que 9 de cada 10 personas dentro de las organizaciones hacen clic en un enlace malicioso, quizás estamos evitando dar testimonios sobre lo que realmente pasa en las organizaciones por el costo que esto significa en el prestigio de la marca.

De todas formas, necesitamos madurar, al menos entre las organizaciones, para crear espacios de discusión sobre como estamos enfrentando la ciberseguridad y amenazas como el phishing. Necesitamos construir encuestas con datos confiables y representativos de las organizaciones -con el debido anonimato de éstas- para tener una fuente de inteligencia que nos permita no solo enfrentar la amenaza anticipándonos a ella. Necesitamos autoevaluarnos y compartir experiencias. Pero, sobre todo, necesitamos dar mayor importancia a la educación y la concientización de las personas que utilizan los sistemas dentro de las organizaciones, para que dejen de ser los vectores de entrada y se conviertan en la primera línea de protección de las organizaciones.

Phishing en la República Dominicana

Carlos Leonardo
Director CSIRT Nacional
República Dominicana

Al igual que en resto del mundo, en la República Dominicana la conducta de ingeniería social ha tomado un giro más organizado por parte de los ciberdelincuentes, donde se toman más tiempo para estudiar la victima potencial y concentrar los esfuerzos de ataque a objetivos que generen una mayor cantidad de ingresos.

El perfil del delincuente cibernético en República Dominicana ya no es la típica persona con conocimientos avanzados en computación, si no personas con antecedentes delictivos en crímenes comunes que ha evolucionado a la utilización de tecnología para cometimiento de hechos con fines de lucro económico.

En una perspectiva general pudiéramos apreciar como estos delitos han sido más sofisticados en cuanto a la persuasión a los usuarios y no tanto así en el uso de nuevas herramientas tecnológicas.

Los tipos de víctimas de ciberataques más afectados son los las personas, con más del 70% del total de las denuncias. Las modalidades más frecuentes que son utilizadas por los ciberdelincuentes están relacionadas con estafas, engaños, amenazas o suplantación de identidad quienes utilizan medios informáticos para llegar a sus víctimas y cometer el ilícito.

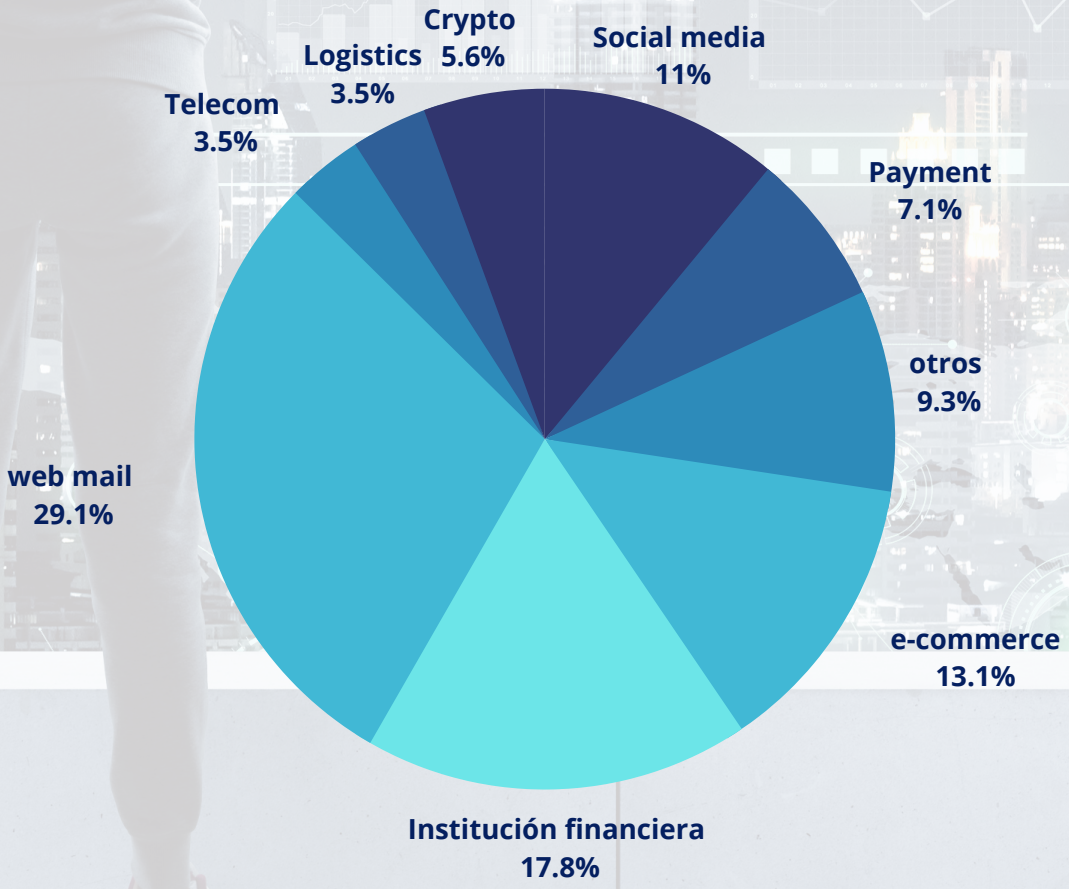
Los ataques de los ciberdelincuentes no se centran en las vulnerabilidades de los sistemas informáticos que utilizan los usuarios sino que pretenden atacar las fragilidades del ciudadano mediante las cuales puedan conseguir datos personales o cualquier información de utilidad para cometer sus crímenes. Es por esto que el uso responsable de las tecnologías de la información y de las comunicaciones, así como el cuidado de los datos personales han sido componente principal de las compañas de concienciación que ejecutamos con frecuencia. Para nosotros impera realizar los esfuerzos en desarrollar una cultura alrededor de los riesgos en el uso de los medios informáticos y las buenas prácticas para identificarlos y mitigarlos.

CONTACTO@GLOBALCYBER.CL

Phishing en el Perú

Aldo Villaseca Hernández
Cyber Security Consultant Base4 Security

La existencia del Phishing no es una amenaza nueva para los usuarios sin embargo los ciberdelincuentes utilizan diversas técnicas de ingeniería social para lograr ataques exitosos y robo de credenciales.
Según el reporte APWG Phishing Activity Trends Report el número de ataques de Phishing se ha duplicado desde principios de 2020, los sectores más afectados se pueden apreciar en el siguiente gráfico:



Global Cyber
soluciones integrales en ciberseguridad

CONTACTO@GLOBALCYBER.CL

En el caso de Perú las estadísticas presentadas por KASPERSKY "Panorama de Amenazas en América Latina 2021" señalaron algunos datos relevantes:

- 06 de cada 10 peruanos no reconocen mensajes que puede ser estafas cibernéticas.
- 61% de los peruanos no sabe qué son los mensajes maliciosos.
- El 40% de ataques de phishing son de índole financiero.

Los casos frecuentes en el Perú que vemos se presentan desde marzo 2020 con el inicio de la emergencia sanitaria por pandemia del COVID19 utilizando el correo electrónico, mensajes de texto (SMS) y WhatsApp son los relacionados a entidades financieras, bonos del gobierno para familias más vulnerables otorgados como ayuda por la Pandemia y de supuestas retenciones bancarias hechas por la SUNAT (Superintendencia Nacional de Aduanas y de Administración Tributaria).
En este contexto las estadísticas de denuncias presentadas a la DIVINDAT División de Investigación de Delitos de Alta Tecnología) de la Policía Nacional son robos a cuentas bancarias utilizando técnicas de phishing.

Ante estos hechos y el crecimiento exponencial del Phishing tal como lo señalan diversos reportes y estadísticas es necesario definir y establecer una Estrategia de ciberseguridad mediante la cual se logra implementar una serie de controles conformados por 03 componentes:

- Documentos que gobiernan la Ciberseguridad,
- Herramientas tecnológicas de Seguridad informática con configuración segura
- Programas continuos de Capacitación y Concienciación sobre Ciberseguridad con indicadores (KPI) definidos para medir eficacia.

Considero que sin todos estos 03 componentes señalados líneos arriba no será posible conseguir tener un nivel de seguridad en el cual las amenazas y riesgos sean mitigados y por consecuencia minimizados a un nivel aceptable para nuestras organizaciones.

.

CONTACTO@GLOBALCYBER.CL

Phishing en Uruguay

Mateo Martínez
Master en Seguridad Informática
Gerente de Krav Maga Hacking

El phishing en Uruguay sigue creciendo y ya no solo buscando obtener datos financieros, sino que el engaño se ha extendido a varias verticales de negocio e inclusive a afectado múltiples personas que han sido engañadas, sus credenciales e identidad digital robadas y utilizadas en forma maliciosa. Si bien existen diversas campañas desde el gobierno nacional como **"Seguro te Conectás de Agesic"** y además varios bancos locales han realizado varias campañas de educación y concientización a sus usuarios, aún queda mucho trabajo por hacer.

De todos modos es interesante observar como inclusive las personas más mayores ya son conscientes de estos engaños y dudan frente a mensajes sospechosos. Pero siempre existe el momento oportuno que aprovechan los delincuentes y con envíos dirigidos, utilizando el lenguaje de negocio o haciéndose pasar por personas cercanas, logran sus objetivos y logran infiltrarse y robar información. Han caído empresas en fraudes muy importantes de transferencia de fondos a cuentas falsas luego de robos de credenciales de personal de las gerencias financieras o directivos de organizaciones así como personas que han tenido transacciones financieras no autorizadas por ellos.

El phishing si bien es uno de los temas principales en las campañas de educación y concientización, aún es muy difícil de detectar inclusive por usuarios expertos.

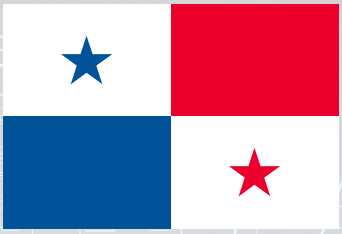
CONTACTO@GLOBALCYBER.CL

Global Cyber
soluciones integrales en ciberseguridad

Los delincuentes cada día perfeccionan sus técnicas y los errores comunes que se veían antiguamente como faltas de ortografía, correos o nombres de otras regiones ahora han sido reemplazados por correos muy precisos y perfectos que hablan el idioma del negocio, conocen los apodos de la familia y muchas veces son el resultado de campañas muy extensas de ingeniería social.

Así que la recomendación para todos sigue siendo estar atentos, no caer en estafas, no creer en los premios de concursos de los que no participamos y validar siempre con controles administrativos.

CONTACTO@GLOBALCYBER.CL



Phishing en Panamá

Silvia Batista
Coordinadora de CSIRT Panamá

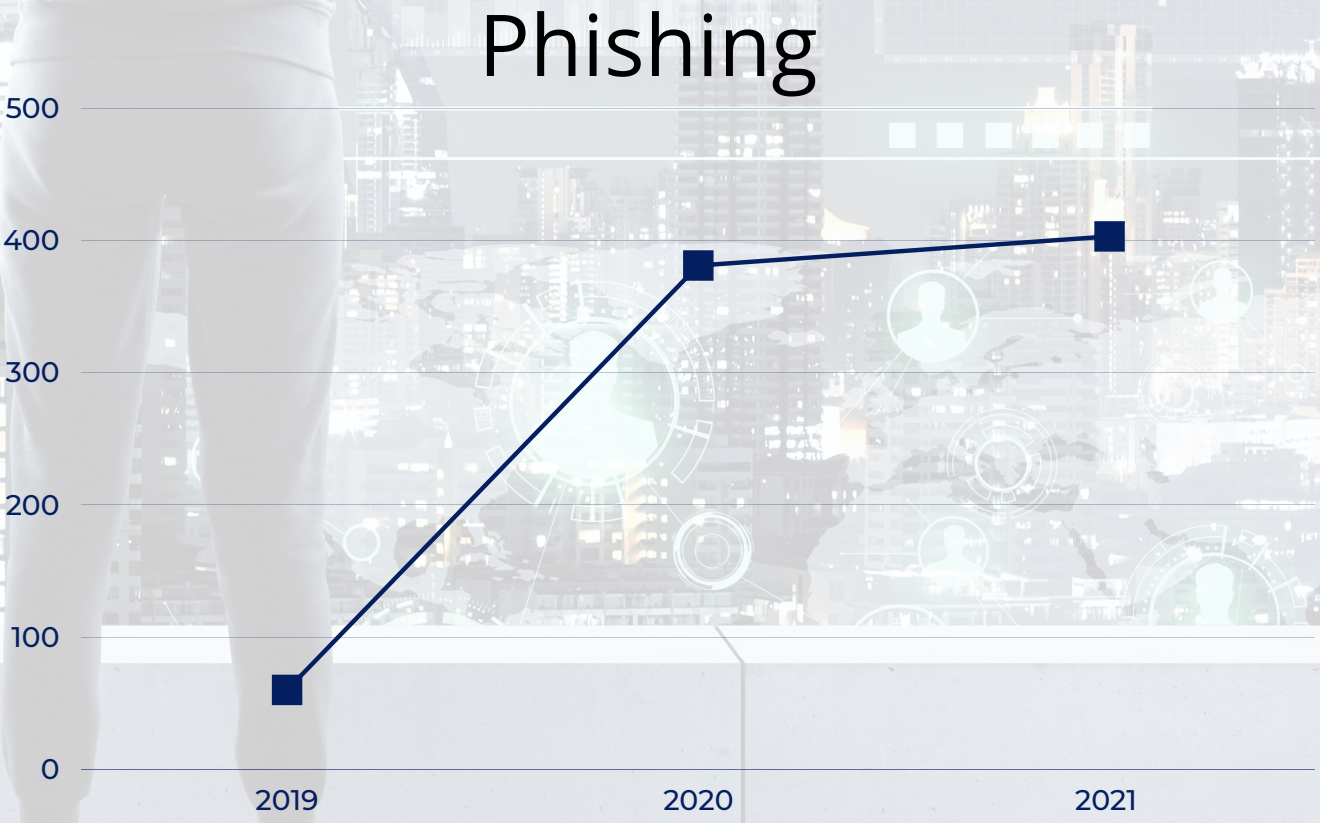
Somos un país que avanza paso a paso en relación a la transformación digital, identificando un amplio progreso en los servicios gubernamentales digitales y en el incremento de facilidades comerciales relacionadas con las compras y pagos en línea. Las denuncias en el Ministerio Público no se han hecho esperar y por primera vez en muchos años se comienza a hablar del tema en diversos programas de televisión y radio, conociendo historias de fraude a través del internet que se efectúa entre la ciudadanía panameña de forma eficaz e inocente. Las asociaciones bancarias manejan la afectación de sus clientes, implementando diversas campañas de concientización en fraude electrónico e incrementando la cultura general en relación a las situaciones de riesgos que se viven día a día en el ámbito digital, como lo es la suplantación de identidad en las redes sociales, fake news, fake shop y técnicas de ingeniera social como Smishing y Vishing.

En el transcurso de los años, el Phishing es el incidente con mayor cantidad de reportes en CSIRT Panamá, en el año 2021 el aumento de casos de Phishing equivalente a años anteriores, es aproximadamente a un 20 % de las incidencias.

Phishing en Argentina

Víctor Figueroa
Magíster en Seguridad Informática
Director de Seguridad de la Información,
Ministerio de Gobierno, Neuquén/AR

El Phishing es sin dudas una de las técnicas de la ingeniería social más utilizadas por el cibercrimen durante los últimos años. De acuerdo a la Unidad Fiscal Especializada en Cibercrimen (UFECI), los casos reportados a partir de la pandemia COVID-19 se incrementaron en un 381% del año 2019 al 2020, mientras que del año 2020 al año 2021 el aumento fue del 403%, valores que se encuentran en consonancia con el incremento del cibercrimen a nivel global.



Incremento del Phishing en Argentina. Fuente: UFECI

Global Cyber
soluciones integrales en ciberseguridad

CONTACTO@GLOBALCYBER.CL

Ésta técnica se ha propagado también hacia las plataformas de redes sociales, de mensajería, e incluso a las comunicaciones por voz (vishing), representando ésta última modalidad un 25% de los casos de Phishing en Argentina, de acuerdo al Informe de la UFECI.

En Argentina, el Código Penal sanciona la defraudación causada por cualquier técnica informática, esta es una herramienta fundamental en la lucha contra el Phishing, siempre que las víctimas sepan recurrir a la Justicia.

Por otro lado, en los últimos años se han consolidado cada vez más en el país los Equipos de Respuestas a Incidentes, tanto públicos como privados, desde donde monitorean las actividades del cibercrimen y se toman acciones de contención inmediatas, ejemplos son la emisión de los reportes de Abuso a los Proveedores de Servicios digitales involucrados, la publicación de alertas, o la comunicación directa a las posibles víctimas.

El Phishing, como técnica de ingeniería social, explota las debilidades humanas para obtener información que será utilizada por el cibercrimen con distintos fines; sin dudas, la ciudadanía es el eslabón más débil en este ecosistema digital, y es hacia donde las organizaciones especializadas deben volcar las estrategias de protección.

Phishing en México

Ernesto Ibarra
Jurista Digital
Presidente de la Academia Mexicana de Ciberseguridad y Derecho Digital.

Phishing, uno de los principales vectores de ataque y puerta de entrada para una gran variedad de ciberdelitos.

En México, como en muchos países, los primeros años de Internet la principal vía de phishing fue el correo electrónico, a través de spam, tarjetas con felicitaciones, la noticia de haber ganado un premio y la típica carta del príncipe nigeriano. Posteriormente, se dio gran auge a los engaños vía llamadas telefónicas y del correo electrónico.

Recientemente, he observado mayor número de ataques de phishing vía aplicaciones móviles -Instagram, WhatsApp, Telegram- y que han aprovechado mucho el contexto de pandemia por covid-19; las ofertas apócrifas de empleo, el contexto de trabajo remoto, sitios fraudulentos de trámites y programas de gobierno; y la típica comunicación suplantando alguna institución financiera, vía correo electrónico y, recientemente, vía apps y RRSS.

Resalto el aumento del ransomware -ciberataque que ha afecta tanto a organizaciones públicas como privada-, destacando el ataque a infraestructuras críticas y a cadenas de suministro; así como el aumento en extorsiones bajo amenaza de divulgar información confidencial.

Otra tendencia este 2022, es el apoderamiento de perfiles de redes sociales de influencers y de perfiles de WhatsApp para solicitar dinero a contactos, así como los ataques phishing para obtener información de acceso -contraseñas- a las billeteras de criptoactivos.

En el combe contra phishing, destaca la Campaña **“#MéxicoContraElCiberfraude”** coordinada por la División Científica de la Guardia Nacional, desde la que se comparte información útil y consejos.

Finalmente, invito a que conozcan el **Portal de Fraudes Financieros**, de la Comisión Nacional de Defensa de los Usuarios de Servicios Financieros: CONDUSEF; en el cual permite a los usuarios que han sido víctimas contar su experiencia. La misma CONDUSEF publica periódicamente reportes sobre fraudes y consejos para evitar ser víctima de fraudes, incluyendo consejos para prevenir el phishing.

Revisa el portal aquí:
https://phpapps.condusef.gob.mx/fraudes_financieros/index.php

CONTACTO@GLOBALCYBER.CL

Phishing en Paraguay

Gabriela Ratti
Directora General de Ciberseguridad y Protección de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones de Paraguay

En Paraguay, una de las técnicas de ingeniería social mas frecuentes y efectivas para los criminales es, por lejos, la ingeniería social.
Los ganchos mas frecuentes son las promesas de algún plan social o beneficio del Gobierno, las falsas ofertas o verificaciones técnicas de compañía telefónicas. En el 2021 se sumó el COVID como uno de los temas frecuentes: falsos ofrecimientos de agendamiento para la vacunación, planes de compensación gubernamental, etc.
La gran mayoría de estos ataques de ingeniería social se realizan a través de llamadas, aprovechándose sobre todo de bases de datos públicas o filtradas de datos personales para hacer más creíbles los engaños.

Por lo general, el objetivo es conseguir el PIN de la billetera electrónica para luego realizar transferencias o el código de verificación de Whatsapp, logrando así el secuestro de la cuenta. Esos casos son especialmente efectivos ya que permiten un esquema piramidal de estafa, engañando y solicitando dinero a los contactos de la victima, haciéndose pasar por ella con su cuenta de Whatsapp "secuestrada".

Prácticamente la totalidad de estos casos son realizados por bandas criminales comandadas desde las cárceles del país.
En el 2021 también se vio un notorio aumento del phishing bancarios, a través de correos y paginas falsas muy bien enmascaradas, que lucen casi idénticas a las oficiales.

Phishing en Costa Rica

Roberto Lemaître Picado
Abogado-Ingeniero Informático
Máster en Computación
Especialista en Delitos Informáticos
Profesor Universitario

El 2021 estuvo marcado por enormes retos en ciberseguridad, tanto para los equipos técnicos como para los ciudadanos en general, en donde:
El 36% de las infracciones han estado relacionadas con ataques de phishing, un aumento del 11%, que en parte podría atribuirse a la pandemia de COVID-19. Como era de esperar, se ha observado que los ciberdelincuentes ajustan sus campañas de phishing en función de lo que es noticia en cada momento.

Los ataques de ingeniería social constituyen la amenaza más grave para la Administración Pública, representando el 69% de todas las filtraciones analizadas por Verizon en 2021. (Informe de Verizon sobre investigaciones de fugas de datos en 2021)

Es por esta razón, que resulta fundamental, para enfrentar la pandemia de ingeniería social y phishing, trabajar en cultura digital con todos los ciudadanos para lograr el disminuir el impacto que producen este tipo de acciones. Esto incluye el contar con las herramientas tecnológicas en nuestros dispositivos que prevenga estas acciones, y otras que van de la mano con estos procesos como el ransomware, pero sobre todo el educar para no caer. Siempre sea escéptico, es mejor ser muy precavido ante cualquier correo electrónico sospechoso, de igual forma antes de hacer clic en cualquier enlace o de descargar cualquier archivo adjunto. Además, siempre confirme antes de actuar, es mejor que llame usted mismo a la empresa con los datos de contacto que aparecen en su sitio web legítimo para confirmar cualquier cosa que se le haya dicho en el correo electrónico o la llamada, esto va de la mano en no responder directamente a los correos electrónicos sospechosos. Recuerde actualizar las contraseñas y utilizar doble factor de autenticación.

Recuerde la mejor defensa es ser muy desconfiado

CONTACTO@GLOBALCYBER.CL

Phishing en Ecuador

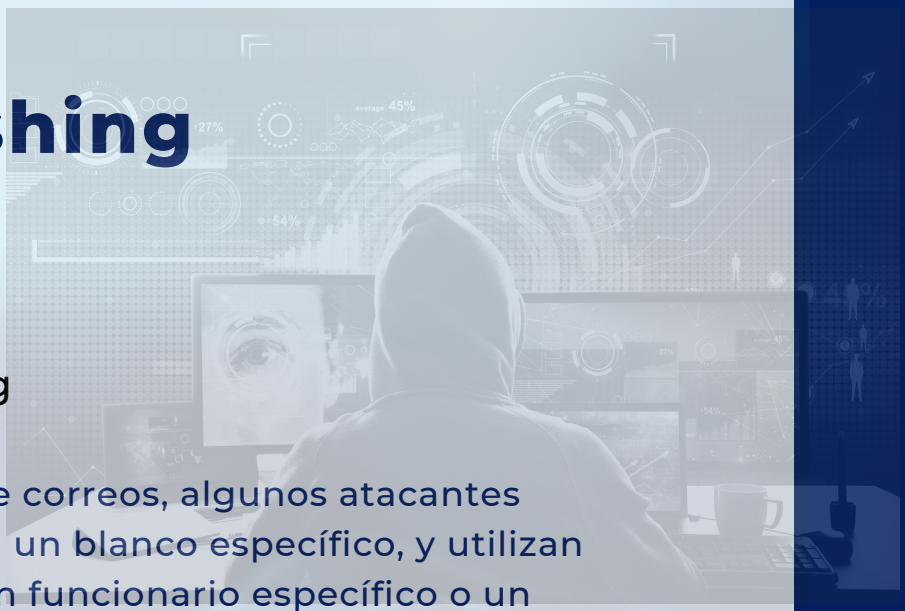
Gabriel Llumiquinga
Presidente de la Asociación
Ecuatoriana de Ciberseguridad (AECI).
Gerente Regional GRC en Audetic.

Ecuador, al igual que otros países a nivel mundial, experimentó un incremento considerable de delitos informáticos debido a la pandemia ocasionada por la Covid 19. Fabián Chávez, Fiscal de la Unidad de Fuero de Corte Nacional de la Fiscalía General Del Estado, en su artículo “Ciberdelitos: una primera aproximación y proyecto institucional”, presentó un cuadro estadístico de los delitos informáticos más comunes, en el cual se menciona que la “estafa” y la “apropiación fraudulenta por medios electrónicos” son los delitos más denunciados en el Ecuador; solo en el 2021 se presentaron 16.272 y 3962 casos, respectivamente. Seguramente estas cifras son mayores, pues, no todos los ciudadanos realizamos las denuncias que corresponden cuando somos víctimas de este tipo de delitos.

Si comparamos las estadísticas presentadas por Fabián en su artículo, con la cantidad de correos electrónicos fraudulentos que recibimos a diario en nuestras cuentas personales y empresariales de correo electrónico, me atrevería a afirmar que los métodos más utilizados por los delincuentes informáticos para los dos delitos antes mencionados son el “phishing” y “spear phishing”, técnicas que no son tan nuevas, pero que aún son efectivas y tienen una alta probabilidad de ocurrencia en los ciudadanos. Lamentablemente, en Ecuador no existe una cifra oficial de casos de “Phishing” o “Spear Phishing” suscitados a nivel nacional.

Esta no es una problemática aislada y afecta considerablemente a los ecuatorianos, independiente de su situación socio – económica, lamentablemente, las personas que no tienen la oportunidad de contar con una educación digital robusta son los más vulnerables. Para ello es importante poner en marcha y garantizar como una política de Estado el “Derecho a la Educación Digital”, el cual ya se establece en el artículo 23 de la Ley Orgánica de Protección de Datos del Ecuador, vigente desde el 26 de mayo del 2021. Estoy convencido de que esta situación debe ser combatida desde una perspectiva de educación y concienciación a través de la implementación de políticas públicas eficaces y robustas, que sean construidas con una perspectiva a largo plazo. Es responsabilidad de todos los actores de la sociedad ecuatoriana el colaborar en la construcción de una sociedad más segura desde el punto de vista digital.

Tipos de phishing



Spear phishing

En vez de enviar miles de correos, algunos atacantes deciden concentrarse en un blanco específico, y utilizan ingeniería social sobre un funcionario específico o un grupo de ellos de empleados de una organización para el robo de información sensible.
Los mensajes de spear phishing parecen provenir de una fuente confiable. El correo también parece legítimo, alguien de la misma organización, y por lo general que ostenta una posición de autoridad. Pero el mensaje es enviado por un atacante.
La tasa de respuesta de un spear phishing es mayor en comparación con un ataque de phishing, porque parece provenir de una fuente confiable de la organización.
económica

Whaling

Es un tipo de phishing cuyos objetivos son ejecutivos de alto perfil en una organización, como el CEO, algún político o una celebridad. La idea es acceder a ellos y a su información confidencial altamente valiosa. En este caso, los atacante engañan a la víctima para que revele información corporativa y personal valiosa (como detalles bancarios, información de empleados, información cotidiana, tarjetas de crédito, etc), generalmente a través de correo o website de spoofing (suplantación de identidad). El whaling exige la realización de un plan cuidadosamente diseñado para la persona de liderazgo seleccionada como víctima.

Pharming

Es una técnica en la cual el atacante ejecuta programas maliciosos en el computador de la víctima o servidor. Cuando la víctima ingrese una dirección URL o nombre de dominio web, su tráfico se redirige inmediatamente a un tráfico controlado por el atacante. En este caso, los atacantes roban información confidencial, como credenciales bancarias y de cuentas, por ejemplo.

El Sistema de Nombres de Dominio, o DNS por sus siglas en inglés, es un sistema de nombres utilizado por Internet para convertir cadenas de direcciones de IP como google.com en una IP numérica para llevar al usuario al sitio web de Google.com. Cuando un atacante emplea la técnica del envenenamiento de caché DNS, ataca un servidor DNS y cambian la IP de un determinado sitio web a su propia IP

Spimming

SPIM, o el Spam en mensajes instantáneos, es una técnica que explota ese tipo de plataformas para usar los mensajes instantáneos como herramienta para distribuir spam. El Spimmer, por lo general, es realizado por bots (una aplicación que ejecuta tareas de manera automática sobre la red) para recolectar y reenviar mensajes de spam. Al igual que el Spam, estos mensajes pueden contener publicidad y malware (programas maliciosos) adjuntos o enlazados al correo. Si una personas hace click en el adjunto, será redirigido a sitios maliciosos dónde se expone a la pérdida de información financiera o credenciales personales, entre otros.

.

CONTACTO@GLOBALCYBER.CL

ANEXOS

ÍNDICE DE ANEXOS

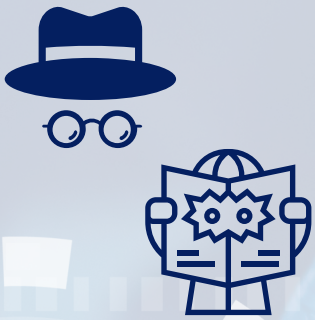
Global Cyber
soluciones integrales en ciberseguridad

Tipos y técnicas de ingeniería social basadas en interacción entre personas

Estas técnicas involucran la interacción entre la víctima y el atacante. Con el pretexto de ser un persona legítima, el atacante interactúa con la persona seleccionada como blanco para recolectar información sensible de la organización a la que pertenece, como estrategias, información de sus redes, etc. Las técnicas que pueden utilizar son:

	Suplantación de identidad	En esta técnica, el atacante pretende ser un usuario legítimo o alguien que cuenta con autorización dentro de un sistema
	Tailgating (seguir por detrás)	Implica ganar acceso a un área restringida siguiendo a una persona con autorización para ello
	Vishing	consiste en la suplantación a través de tecnología de voz , en la que se trata de engañar al individuo para revelar información crítica
	Baiting	consiste en dejar un dispositivo de almacenamiento infectado – como un pendrive- en un lugar estratégico, para que una persona lo encuentre y lo utilice en su equipo.

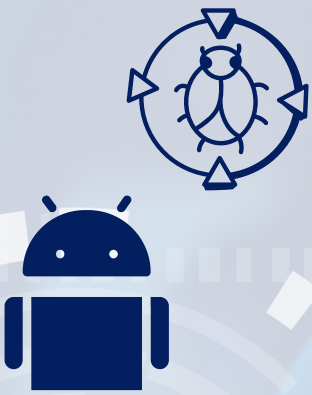
CONTACTO@GLOBALCYBER.CL

	Shoulder surfing	Reunir información mientras se está detrás de una víctima, cuando esta interactúa con otra persona mientras tratan un tema respecto a información sensible de una organización
	Dumpster Diving (indagar por información en la basura)	consiste en la suplantación a través de tecnología de voz , en la que se trata de engañar al individuo para revelar información crítica
	Eavesdropping	Se trata de obtener información escuchando conversaciones de terceras personas o leyendo información en forma desapercibida

CONTACTO@GLOBALCYBER.CL

Técnicas de ingeniería social basada en dispositivos móviles

Los atacantes utilizan aplicaciones móviles para perpetrar un ataque basado en estos dispositivos, imitándolas, para crear aplicaciones móviles maliciosas. Los usuarios desprevenidos descargarán estas aplicaciones y se infectarán con los programas maliciosos (malware).

	App Maliciosa	En esta técnica, el atacante Crear réplicas de aplicaciones populares con código malicioso para disponibilizarlas en tiendas en línea para ser descargadas en gran escala. El objetivo es que, cuando un usuario se registra en la aplicación falsa, enviará sus credenciales a un servidor controlado por un atacante
	App Falsas	Similar al método anterior, con la diferencia que este tipo de aplicaciones puede ser descargado por una ventana emergente (pop-up) cuando el usuario esté navegando en una website de internet.
	Smishing (phishing de SMS)	Se trata del envío de mensajes de texto o SMS 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.

CONTACTO@GLOBALCYBER.CL

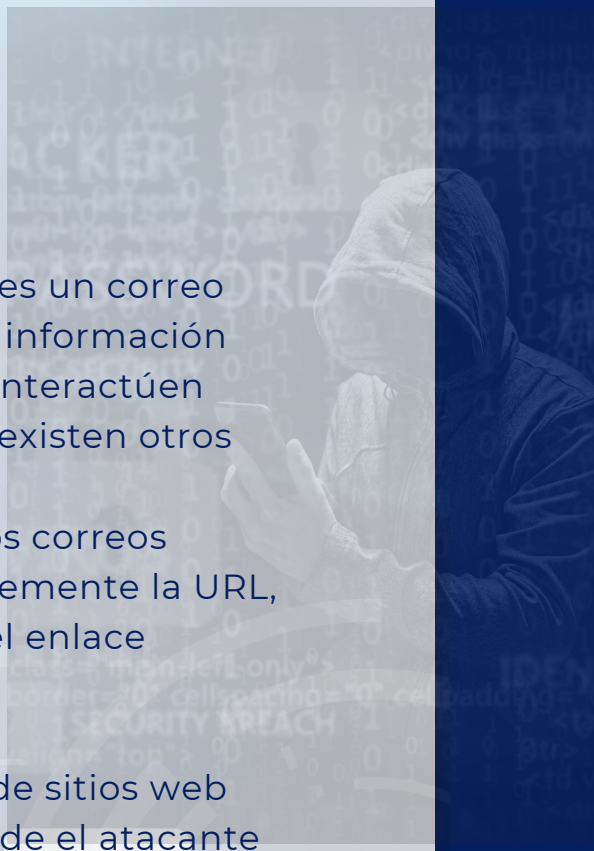
Técnicas de ingeniería social basada en computadores

Este tipo de ataques se basa en computadoras, sistemas de internet y servicios de correos para ejecutar sus ataques, utilizando algunas de las siguientes técnicas

	Pop Up	Un pop-up es una ventana emergente no solicitada por el usuario. Estos cuadros contienen mensajes –generalmente con información de advertencia- que comprometen a los usuarios a utilizar enlaces que los redirigen a sitios web fraudulentos, en los que preguntan por información personal o los invitan bajar archivos con contenido malicioso
	Spam	las cadenas de correos son irrelevantes, inesperadas y no solicitadas, cuyos contenidos buscan recolectar información sensibles del usuario. Los atacantes suelen adjuntar en mensajes de spam virus y troyanos.
	Phishing	Es una técnica en la cual el atacante envía un correo a un usuario, provisto de un falso enlace que pretende ser legítimo, con la intención de a través del direccionamiento de la persona a un sitio fraudulento, pueda obtener información personal y de la cuenta del usuario

CONTACTO@GLOBALCYBER.CL

Métodos Utilizados para el phishing



El método más común utilizado para el phishing es un correo electrónico en el que el atacante intenta obtener información confidencial al hacer que los usuarios accedan e interactúen con sitios web maliciosos. Sin embargo, también existen otros métodos como:

- Un atacante puede manipular los enlaces en los correos electrónicos enviados. Hacen esto cambiando levemente la URL, por lo que el usuario no puede diferenciar entre el enlace malicioso y el sitio web real.

- Algunos hackers también usan la falsificación de sitios web como medio de phishing. Este es un proceso donde el atacante usa comandos de JavaScript para desarrollar un sitio web falso que parece genuino.

- Los atacantes también usan una técnica conocida como redirección encubierta. En este proceso, infectan sitios web genuinos para lanzar ventanas emergentes. Un usuario hace clic en enlaces en la ventana emergente que lo redireccionan convenientemente hacia el sitio web del atacante.

- Los atacantes pueden liberar malware y ransomware en el sistema o la red de un usuario mediante adjuntos .exe, PDF y de Microsoft Office infectados.

- Los atacantes también pueden ejecutar ataques de phishing a través de otros medios, como mensajes de texto, llamadas telefónicas y redes sociales.

.

CONTACTO@GLOBALCYBER.CL

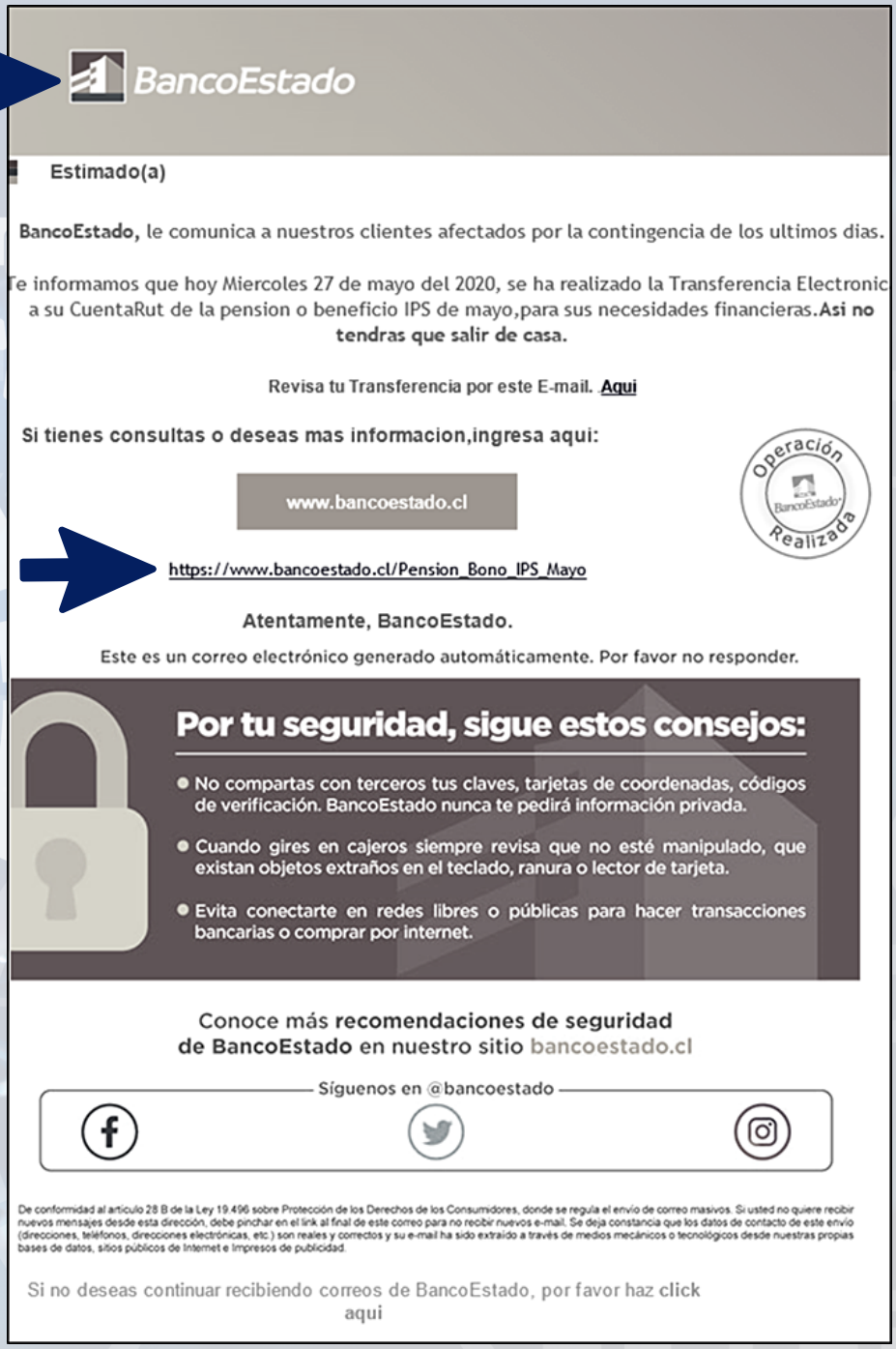
Ejemplo de un mensaje de phishing

Utiliza símbolos idénticos a los legítimos

Mensaje sobre contingencia

Contiene enlaces a sitios fraudulentos

Apela a factores de seguridad para reforzar idea de legitimidad



BancoEstado

Estimado(a)

BancoEstado, le comunica a nuestros clientes afectados por la contingencia de los ultimos dias.

Te informamos que hoy Miercoles 27 de mayo del 2020, se ha realizado la Transferencia Electronic a su CuentaRut de la pension o beneficio IPS de mayo,para sus necesidades financieras.**Asi no tendras que salir de casa.**

Revisa tu Transferencia por este E-mail. **Aqui**

Si tienes consultas o deseas mas informacion,ingresa aqui:

Operación Realizada

www.bancoestado.cl

https://www.bancoestado.cl/Pension_Bono_IPS_Mayo

Atentamente, BancoEstado.

Este es un correo electrónico generado automáticamente. Por favor no responder.

Por tu seguridad, sigue estos consejos:

- No compartas con terceros tus claves, tarjetas de coordenadas, códigos de verificación. BancoEstado nunca te pedirá información privada.
- Cuando gires en cajeros siempre revisa que no esté manipulado, que existan objetos extraños en el teclado, ranura o lector de tarjeta.
- Evita conectarte en redes libres o públicas para hacer transacciones bancarias o comprar por internet.

Conoce más **recomendaciones de seguridad de BancoEstado** en nuestro sitio bancoestado.cl

Síguenos en @bancoestado

De conformidad al artículo 28 B de la Ley 19.496 sobre Protección de los Derechos de los Consumidores, donde se regula el envío de correo masivos. Si usted no quiere recibir nuevos mensajes desde esta dirección, debe pinchar en el link al final de este correo para no recibir nuevos e-mail. Se deja constancia que los datos de contacto de este envío (direcciones, teléfonos, direcciones electrónicas, etc.) son reales y correctos y su e-mail ha sido extraído a través de medios mecánicos o tecnológicos desde nuestras propias bases de datos, sitios públicos de Internet e Impresos de publicidad.

Si no deseas continuar recibiendo correos de BancoEstado, por favor haz click aqui

CONTACTO@GLOBALCYBER.CL

Ejemplo de un sitio de phishing

Dirección web falsa

CONTACTO@GLOBALCYBER.CL

UNIDOS POR LA CIBERSEGURIDAD

FEBRERO 2022

Global Cyber

soluciones integrales en ciberseguridad