Guía de Seguridad

Fecha de publicación: 15/06/2022

Tema: Guía de Seguridad de prevención de phishing.

Objetivo: Proveer una guía para prevenir incidentes de seguridad ocasionados por ataques de *phishing*.

Índice

¿Qué es el *phishing*?

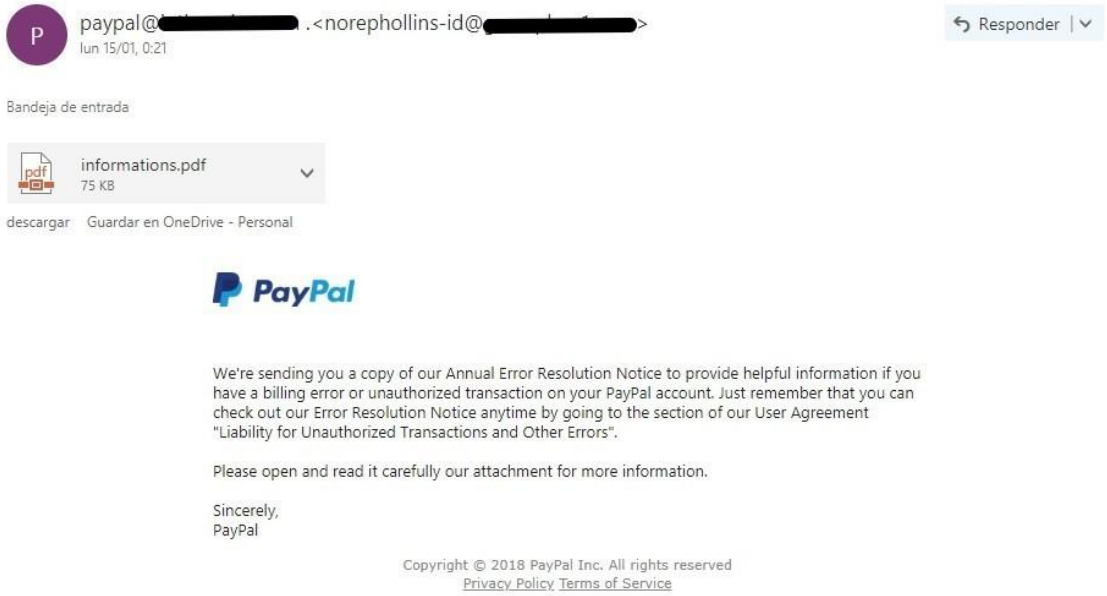
Es un método por el cual un atacante logra captar y robar datos confidenciales de una persona de una manera fraudulenta, mediante el engaño de sitios web bien diseñados, correos electrónicos, mensajes de texto, u otras plataformas muy utilizadas. Un atacante podría robar contraseñas, información de cuentas bancarias y tarjetas de un cliente de un banco u otro tipo de empresa.

¿Cuáles son los tipos de *phishing*?

Los ataques de *phishing* son técnicas de ingeniería social utilizadas para engañar a las personas y pueden tener un amplio rango de objetivos dependiendo del atacante. Podrían basarse estafas por correo electrónico, SMS o llamadas genéricas que tienen como objetivo a cualquier persona que tenga una cuenta bancaria y se clasifican la siguiente manera:

- **Estándar:**

  Este tipo de ataques, como bien dice su nombre “estándar”, no están personalizados para sus objetivos y los correos electrónicos / SMS se envían en masa. El objetivo por lo general son algunos destinatarios muy aleatorios que tienen menos probabilidades de responder al *phishing*.



- ***Smishing*:**

El *smishing* es una técnica que utiliza mensajes texto o servicio de mensajes cortos (SMS). Que consiste en enviar un mensaje a un teléfono móvil mediante SMS y que contiene un enlace para hacer clic o devolver una llamada a un número de teléfono. Por ejemplo, haciendo creer a la víctima que el mensaje procede de una entidad bancaria, que le informa que su cuenta se ha visto comprometida y que necesita responder inmediatamente. El atacante le pide que verifique su número de cuenta, clave de acceso, clave transaccional , etc. Una vez que el atacante recibe la información, obtiene el control de su cuenta bancaria.

- ***Vishing*:**

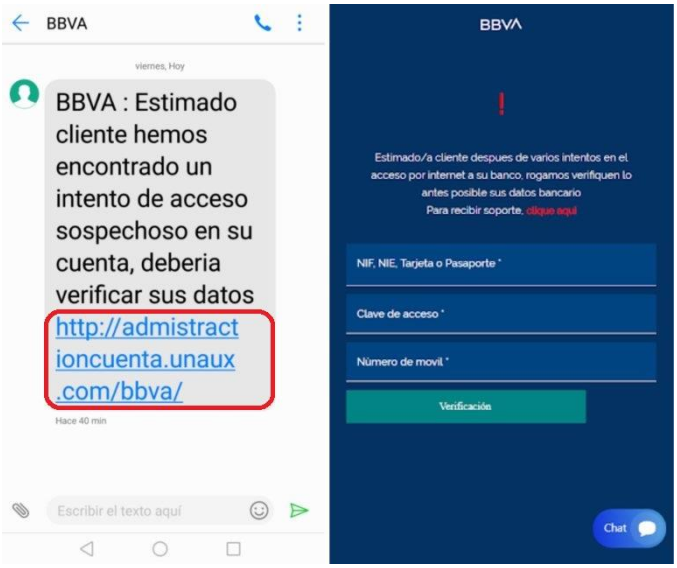
El *vishing* es un ataque que se vale de llamadas telefónicas para obtener información personal y confidencial de la víctima. Consiste en realizar una llamada, utilizando estrategias de ingeniería social para convencer a las víctimas para recaudar información privada y acceder a sus cuentas bancarias.

Al igual que el *smishing*, el *vishing* se basa en convencer a las víctimas de que están haciendo lo correcto al responder a la persona que llama. A menudo, el actor malicioso fingirá estar llamando en representación del gobierno, el departamento de recaudación de impuestos, la policía o el banco de la víctima.

- ***Spear-phishing*:**

Los ataques de *spear phishing* se personalizan para sus objetivos valiéndose de correos electrónicos / SMS / llamadas telefónicas específicas para el objetivo, difíciles de detectar. Están destinados para grandes organizaciones y empleados corporativos.

Los atacantes son en su mayoría distribuidores de código malicioso orientados a los negocios especializados en ingeniería social y actividades fraudulentas.



Nota: La imagen es un ejemplo registrado en España para el banco BBVA

- ***Whale-phishing*:**

Es un término utilizado para describir un ataque de *phishing* que está dirigido específicamente a individuos de gran poder adquisitivo, altos cargos a nivel gobierno o privado.

Caso global de phishing: Netflix

El medio más utilizado para realizar ataques de *phishing* es el correo electrónico, es por ello que se generan en plataformas como:

Netflix:

Netflix es una plataforma de entretenimiento popular, por lo que es objetivo para los ataques de *Phishing*, a través de mensajes de textos y correos electrónicos que redireccionan a un sitio web diseñado para el robo de información relacionada a la cuenta del usuario. Los escenarios más comunes desde mediados del 2020 son:

1. **Mensajes de texto de *phishing***

1.1. "Bloqueados por cuenta" de Netflix

Los atacantes se hacen pasar por Netflix, e intentan engañar a la persona para hacer clic en un enlace de *phishing* que conduce a una página web falsa, donde se solicita ingresar información personal como los datos bancarios, número de tarjetas de crédito y códigos CVC.

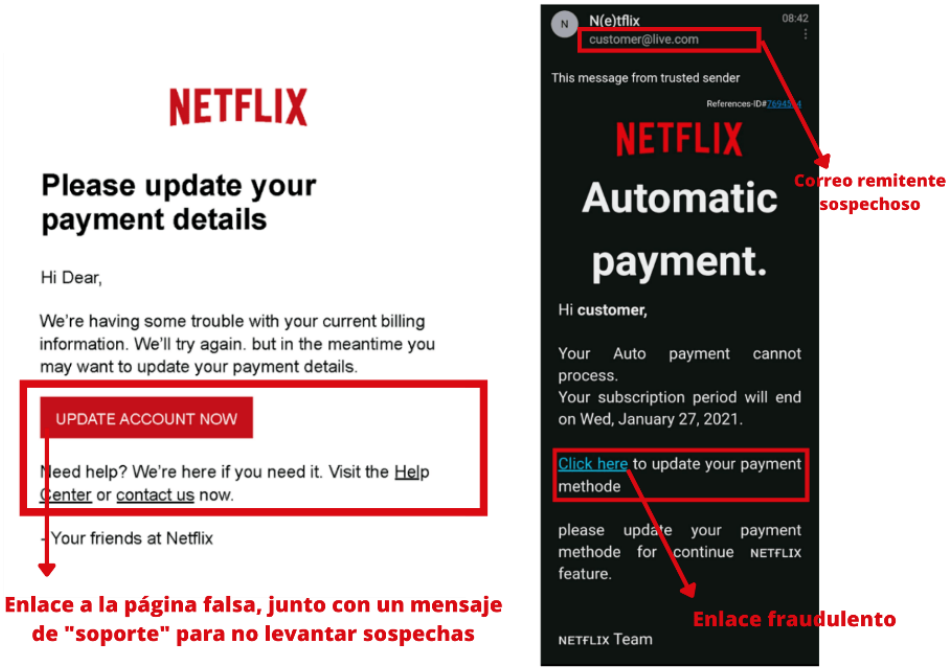
1.2. Suscripción gratuita de 1 año en Netflix

Este escenario empezó durante el inicio de pandemia Netflix, haciendo creer que es un premio para ayudar a quedarse en casa. Los estafadores afirman falsamente que están regalando suscripciones gratuitas debido a la pandemia, lo que le pide que haga clic en el enlace de *phishing* incluido en el mensaje.

2. Correo electrónico fraudulento

2.1. **“Actualiza tus datos de pago”:**

Al igual que los anteriores casos, los atacantes se hacen pasar por Netflix pidiendo que actualices tu método de pago ya que existe un problema con él, pero mediante un correo electrónico falso.



Nota: Netflix deja sus recomendaciones en el siguiente enlace.

Casos locales de *phishing*

Al inicio del mes de junio de 2022, se ha evidenciado un aumento significativo de casos de *phishing* a gran escala, que buscaban engañar a los clientes de entidades financieras a nivel nacional.

¿Cuáles son las recomendaciones para evitar ser víctima de *phishing*?

- Evitar acceder a sitios web a través de enlaces acortados.
- Mantenerse actualizado e informado acerca de las tendencias del *phishing*.

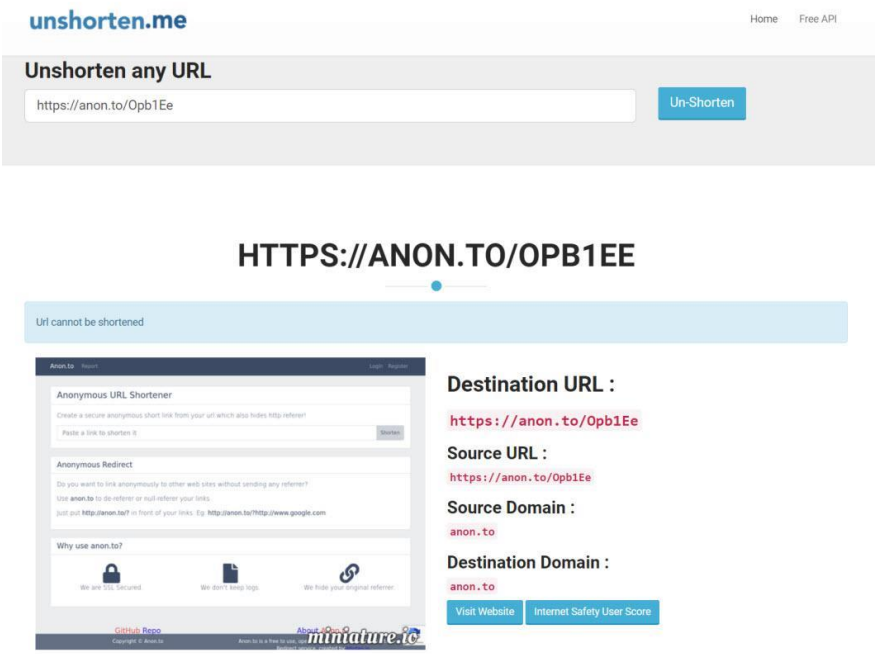
- Tener en cuenta que las entidades bancarias y financieras no solicitan datos confidenciales a través de correo electrónico o SMS, de esta manera se minimiza la posibilidad de ser víctima de esta acción delictiva.
- Desconfiar de los correos que dicen ser emitidos por entidades que brindan servicios y solicitan cambios de datos sensibles (contraseñas, números de tarjeta, códigos de seguridad, etc.) ya que suelen ser engaños.
- No hacer clic sobre enlaces que aparecen en el cuerpo de los correos electrónicos, ya que pueden redireccionar hacia sitios web clonados o hacia la descarga de *malware*.
- Observar con atención la dirección del remitente del correo.
- Tener cuidado con el correo que llega a la bandeja de correo no deseado o spam. Si bien, en ocasiones el correo legítimo puede terminar en la bandeja de correo no deseado o spam, en muchos casos el correo que se encuentra allí es fraudulento. Si no estamos absolutamente seguros de que es un correo legítimo, no debemos abrirlo.
- Si se tiene dudas sobre la legitimidad de un correo, comunicarse telefónicamente con la persona u organización que dice ser el remitente para descartar la posibilidad de ser víctimas de un engaño.
- Evitar enviar contraseñas, números de tarjetas de crédito u otro tipo de información sensible a través del correo electrónico.
- Habituarse a examinar periódicamente la actividad en las cuentas (bancarias, correo electrónico, redes sociales, etc.), a fin de detectar a tiempo actividad extraña relacionada con la manipulación de la cuenta o transacciones no autorizadas.

Recomendaciones adicionales para la detección

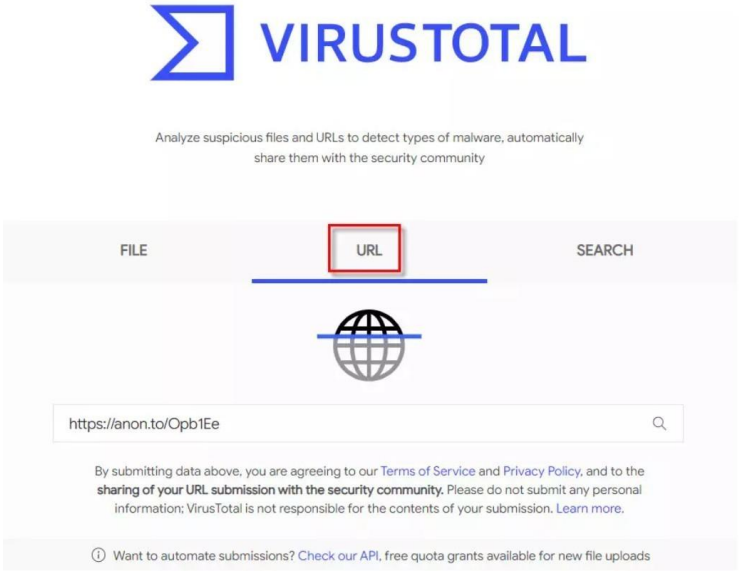
Si bien, estos ataques se destacan por presentar sitios web falsos, se puede contrarrestar verificando que los enlaces estén alojados en dominios legítimos y pertenezcan a la organización que dice enviar. En lo posible, siempre utilizar páginas web oficiales y/o aplicaciones legítimas para el envío de datos personales, información bancaria o para realizar compras y/o algún tipo de transacción. Algunos pasos prácticos a seguir para tener en cuenta los detalles recién mencionados:

1. **Utilizar** herramientas para la detección de enlaces acortados fraudulentas:

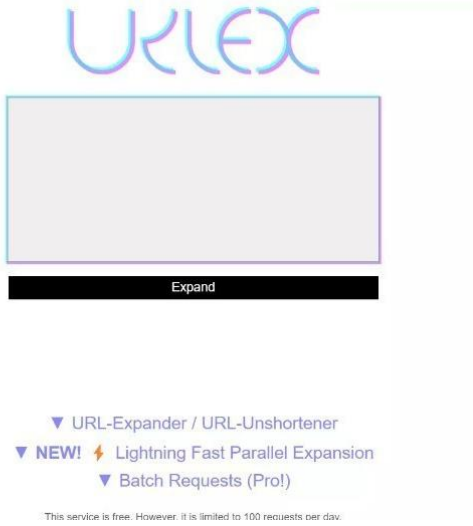
- **Unshorten.me**: Es un sitio web bastante sencillo, que nos muestra que hay detrás de cada enlace acortado, indicando el enlace original y una vista previa.



- **VirusTotal:** es un servicio bastante útil para trabajar con enlaces acortados, se debe seleccionar la pestaña URL para comprobar si es un enlace seguro, al final del análisis se obtendrá un resultado distintos motores mostrarán si han visto algo malo en el enlace.



- **URL Expander:** de igual manera a las anteriores herramientas mencionadas, en esta se podría colocar varios enlaces simultáneamente.



Nota: Puede visualizar la lista completa de todas las herramientas que pueden ser utilizadas para la comprobación de URL.

2. Bloquear la publicidad mediante extensiones de navegadores:

- *Ads Link Skiper*, disponible para Chrome.
- *Adfly Skipper*, disponible para Firefox.
- *Universal Bypass*, disponible para Mozilla Firefox y Microsoft Edge.

Referencias:

- https://cert.gov.py/application/files/9914/5770/8395/Guia_Seguridad_Usuarios.pdf
- https://www.cert.gov.py/noticias/como-protegerte-del-phishing-en-internet
- https://cert.gov.py/application/files/8616/5472/4028/BOL-CERT-PY-2022-25_Phishing_a_traves_de_tunelizacion_inversa_y_acortadores.pdf
- https://ejemplos.net/ejemplos-de-phishing/#:~:text=%2010%20Ejemplos%20de%20Phishing%20%201%20Los,as%C3%AD%20acceder%20a%20la%20informaci%C3%B3n%20bancaria.%20More%20
- https://www.conceptosjuridicos.com/phishing-bancario/#:~:text=Phishing%20bancario%20El%20phishing%20bancario%20es%20un%20m%C3%A9todo,de%20un%20banco%20u%20otro%20tipo%20de%20empresa.
- https://selfoy.com/how-do-spear-phishing-attacks-differ-from-standard-phishing-attacks/#:~:text=Standard%20Phishing%20is%20a%20general%20phrase%20that%20refers,social%20media%2C%20phone%20calls%2C%20and%20even%20text%20messages.
- https://www.antivirus.com/2021/08/05/netflix-phishing-scams-of-2021-how-to-avoid-them/