Phishing

¡Te damos la bienvenida al material sobre ataques de Phishing!

El uso del correo electrónico, las redes sociales y los teléfonos celulares forman parte de nuestro día a día. Pero, ¿cuántas veces recibimos SMS de números desconocidos?, ¿cuántos correos recibimos de destinatarios dudosos?

Muchos de estos mensajes y correos son enviados con el firme objetivo de engañar al usuario y obtener sus datos confidenciales.

A lo largo de este material, *te proponemos conocer las modalidades más utilizadas por los ciberdelincuentes para llevar adelante este tipo de ataque y así poder adoptar las medidas de seguridad adecuadas para evitar ser víctimas de estafas.*

Módulos

Módulo 1: Qué es el Phishing

El phishing ***(pescar – morder el anzuelo)*** consiste en el envío de mensajes electrónicos que, poseen la apariencia de provenir de fuentes fiables *(Ej. Entidades Bancarias, Gubernamentales, Servicios)*, intentan obtener datos confidenciales del usuario *(Contraseñas, Datos bancarios, Cédula de identidad, etc.)* y ser utilizados para la realización de algún tipo de fraude.

Para lograr confundir, suelen incluir, por ejemplo, un enlace a **sitios web falsificados** que **se ven iguales a las de empresas confiables**, pero no lo son. De esta manera, el usuario, creyendo estar en un sitio de confianza, introduce la información solicitada que, en realidad, **es capturada por el estafador**.

Módulo 2: Consejos para evitar ataques de Phishing

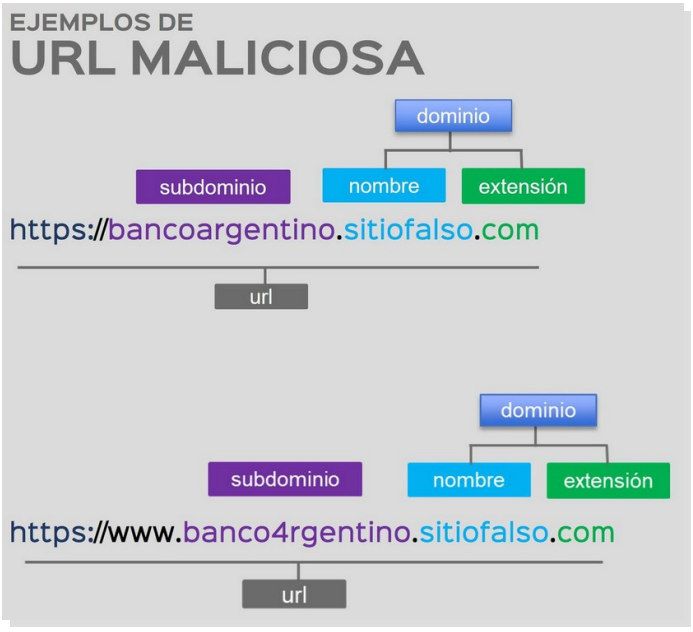
¿Cómo reconocer un sitio seguro?

Cuando navegamos en internet, no siempre lo hacemos en sitios seguros. ¿Cómo reconocer si un sitio es confiable? A continuación presentamos algunos aspectos a tener en cuenta.

1. DOMINIO + URL MAL ESCRITA

- ✔ ***Dominio*** es el nombre con el cual se identifica una página web. Está formado por:
- ✔ ***Nombre*:** valor que se le da al sitio web para simplificarle la navegación al usuario
- ✔ ***Extensión*:** indica el tipo de dominio y el país que lo genera *(ej: .com.ar, .org.es, .com)*

Las URLs mal escritas son direcciones web muy similares a las originales, que a simple vista parecen seguras pero incluyen caracteres distintos o algún error sutil.



¿Qué es una URL ACORTADA?

Son direcciones web con menos caracteres que la URL original y permite acceder al mismo sitio. En estos casos, debemos mirar siempre el sitio al que nos redirigen y evaluar si ese dominio es seguro o no.

Veamos el siguiente ejemplo:

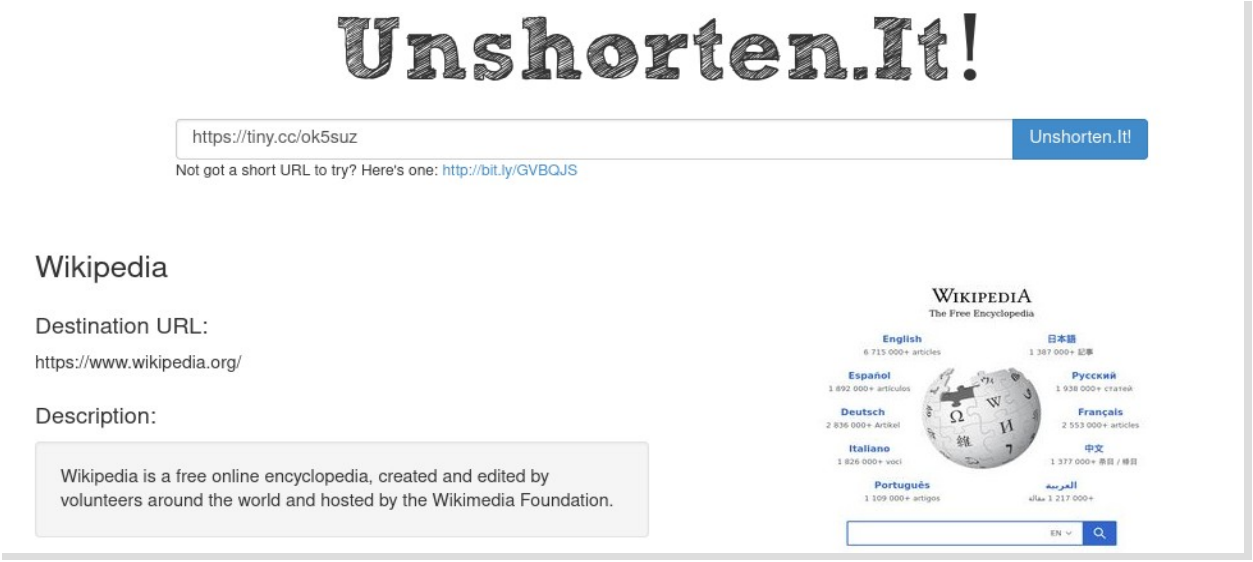
- ➔ **https://tiny.cc/ok5suz**
- ➔ **https://wikipedia.org**

En el caso que un proveedor real nos envíe una URL acortada, debemos verificar con los canales autorizados *(redes sociales)* o chequear que el sitio al que nos redirige es válido. En este ejemplo la URL corta nos redirige a ***Wikipedia***.

Para corroborar si el dominio al que seremos redirigidos es confiable, podemos ingresar la URL corta en la siguiente web:

- ➔ **https://unshorten.it/**

2.



PROTOCOLO DE SEGURIDAD

El HTTPS significa que la información del sitio se transmite de manera “segura”, aunque no siempre es sinónimo de sitio confiable. Los ciberdelincuentes pueden crear sitios falsos con certificados que no son de entidades certificantes legítimas y utilizar igualmente el HTTPS.

Se aconseja siempre volver a verificar la dirección del dominio.

HTTP vs HTTPS

HTTP y HTTPS son dos protocolos de transferencia de datos. La diferencia es que en HTTP se puede acceder a los datos enviados o recibidos, mientras que en HTTPS se utiliza una conexión segura, en la que la información viaja cifrada, impidiendo que terceros puedan visualizarla.

3. CERTIFICADO

El certificado permite confirmar que el sitio es legítimo, lo emite una entidad mundialmente reconocida.

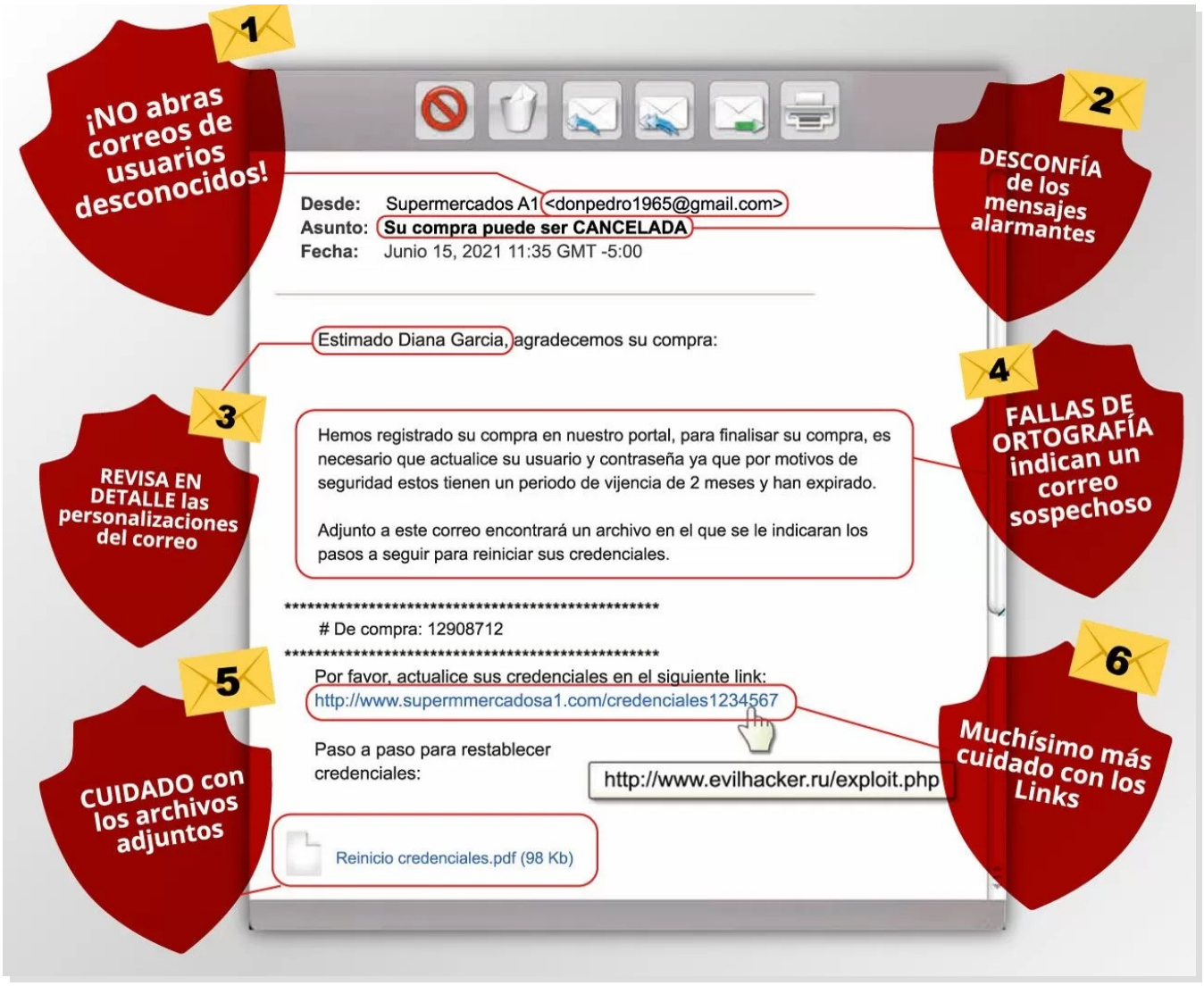
¿Cómo podemos cuidar nuestros datos confidenciales y no exponernos a posibles estafas?

A continuación te brindamos algunos consejos.

- ✔ Comprueba que el sitio web sea https. Verifica que el certificado del sitio sea válido y que la URL sea la correcta; aun así no te fíes. Siempre debes validar los datos solicitados.
- ✔ No abras links o adjuntos, ni respondas mensajes de correos electrónicos de origen sospechoso. Nunca ingreses información en sitios web dudosos.
- ✔ No accedas a la página web de tu banco desde links o accesos rápidos desde tus correos electrónicos, aunque provengan de dicha entidad.
- ✔ Los bancos nunca solicitan claves o información financiera a través de correos electrónicos. Por lo tanto, no los respondas.
- ✔ Cuando realices un pago, no lo hagas desde el link del correo electrónico.
- ✔ Presta atención en caso de que:
  - *Recibas correos electrónicos de remitentes desconocidos o que no estén relacionados con el trabajo;*
  - *Encuentres errores de ortografía y/o mezcla de idiomas;*
  - *Recibas un llamado o SMS solicitando tus datos personales, o indicando que fuiste el ganador de un premio. Recordá entregar tus datos personales únicamente si estás seguro de quién es el receptor.*
- ✔ Desconfía en caso de que el interlocutor tenga mucha urgencia por saber tus datos o si te advierte que hay peligro con tu dinero.

- ✔ Siempre que sea posible recuerda activar la “autenticación de doble factor ”. Este es el método más efectivo para poner barreras a los ataques de phishing.

¿Cómo reconocer correos de phishing?



Módulo 3: Qué hacer si eres víctima de Phishing

Si abriste un link fraudulento, descargaste un archivo malicioso o ingresaste tus datos personales y te das cuenta que fuiste víctima de phishing, estas son las acciones que debes tomar.

Si tu proveedor de correo electrónico ofrece un registro de actividad, compruébalo para ver si se han realizado acciones repetidas, para marcar los mensajes como <<no leídos>>. Revisa la carpeta de mensajes enviados para determinar si hay algún mensaje que te llama la atención, así como también <<papelera>> para descubrir notificaciones de <<delivery failure>>.

Es prioritario cambiar o recuperar la contraseña desde sitios oficiales. Ingresa manualmente a cada sitio (no desde enlaces) y asegúrate de no tener activada la opción “guardar contraseña” en los navegadores de internet o smartphones.

Comunícate con el sector de Tecnología de la organización usando los canales oficiales.

Limpia el caché de tu navegador y no dejes ninguna cuenta abierta en la red.

Verifica la presencia de notificaciones en tu correo electrónico del tipo <<Nuevo aviso de inicio de sesión>>, en la <<Papelera>>, o en la bandeja de entrada.

Elimina los datos de cuentas que sean del tipo bancario, billeteras virtuales, e-commerce y tarjetas de crédito guardadas en el navegador.

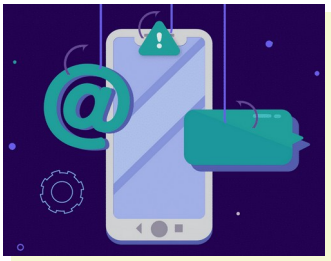
Módulo 4: Resumen

Con objetivo de fortalecer y realizar un breve repaso de lo visto hasta acá les dejamos el siguiente vídeo.

Enlace: Video resumen Phishing.

Glosario

Phishing tradicional



Los phishers *envían correos electrónicos con enlaces a páginas de registro falsas*. Cuando la víctima introduce sus datos en el formulario, estos se almacenan inmediatamente en un servidor remoto al que los phishers tienen acceso y así logran capturar sus datos. Por ejemplo, usan esta técnica para enviar un conjunto de correos electrónicos con el asunto “urgente”, solicitando a la potencial víctima que actualice su contraseña de homebanking o reclame algún premio.

Pharming

Consiste en aprovechar una vulnerabilidad de software de la computadora, donde *el usuario es redirigido hacia un sitio web fraudulento*, al momento de ingresar a la web original.

Smishing

Este tipo de phishing está relacionado con el uso de teléfonos celulares, ya sea por SMS, WhatsApp, Messenger, Telegram, entre otros.

Normalmente *los ciberdelincuentes se hacen pasar por entidades conocidas y envían un mensaje de texto alertando a la víctima* que, por ejemplo, ha ganado un premio, que su pago de servicios se registró 2 veces, que tiene una tarjeta pendiente a retirar, u otros tipos de engaños para atraer la atención de la víctima. La víctima debe responder con algún tipo de código o número especial para validar su falso premio.

Los **smishers** *utilizan la Ingeniería Social* para lograr que las víctimas procedan haciendo una de las siguientes acciones:

- ✔ Hacer clic en un hipervínculo.
- ✔ Responder a un mensaje de texto.
- ✔ Llamar a un número de teléfono.

Vishing

Existen centros de atención telefónica que *realizan llamadas con el objetivo de realizar un fraude*. Este ataque muchas veces suele estar relacionado con otro tipo de phishing, de forma que se complementan para lograr una mayor credibilidad y de esta manera engañar a la víctima de una forma sencilla y eficaz.

Spear Phishing

Se trata de una *técnica más sofisticada* que el phishing tradicional. *El objetivo es engañar a una persona específica de una compañía en concreto*. Para ello, los ciberdelincuentes recopilan previamente

información sobre la víctima, por ejemplo: nombres, direcciones de correos electrónicos y otras informaciones de redes sociales como Linkedin o registros de correos electrónicos pirateados (investigación de ingeniería social). Así logran ser muy meticulosos en el ataque.

El spear phishing es una herramienta típica usada en ataques a empresas, bancos o personas influyentes.