BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
LA AGENCIA DE SISTEMAS
www.ba-csirt.gob.ar
BOLETÍN N°03
FECHA DE PUBLICACIÓN
08 12 16

PHISHING: ¿QUÉ ES Y CUÁLES SON SUS POSIBLES CONSECUENCIAS?

Durante los últimos días, múltiples medios de todo el mundo hablaron acerca del masivo "***hackeo***" que se ha estado llevando a cabo por toda Europa y países asiáticos como Tailandia y la isla de Taiwán. El ataque afectó a los cajeros automáticos de diferentes entidades bancarias, haciendo que estos expulsaran billetes descontroladamente.

De acuerdo con la información brindada por la compañía rusa "Group-IB", especialista en la prevención e investigación de fraudes y crímenes cometidos a través de Internet, el método que utilizaron estos hackers para llevar adelante su cometido, es el popular phishing. Hacerlo de ese modo les permitió planificar y ejecutar el ataque de forma remota -es decir, virtualmente, sin necesidad de estar presentes físicamente- y solo acudir a los cajeros en el preciso momento en el que estos entregaran el dinero; lo cual dificulta enormemente a las autoridades que intentan atraparlos y, además, les permite disparar el ataque a varios cajeros en simultáneo.

El "*phishing*" es una práctica de ingeniería social que tiene como objetivo apropiarse de datos personales ajenos para usarlos en beneficio propio.

Ahora bien, ¿qué es exactamente el phishing?

Probablemente lo hayas escuchado o leído en más de una oportunidad: **se trata de un método** sumamente utilizado por los hackers y ciberdelincuentes de todo el mundo **para obtener de modo fraudulento y a través del engaño, información privada, sensible y confidencial de personas, empresas, entidades públicas o privadas, y cualquier otro blanco que pueda resultar atractivo de ser atacado**.

Quienes usan ésta técnica son llamados ***phishers*** y en general llegan a sus víctimas haciéndose pasar por personas y/o empresas o entidades en las que estas confían. Frecuentemente los contactan a través de correos

electrónicos falsos, programas de mensajería instantánea -como WhatsApp, por ejemplo-, mensajes de texto tipo SMS y, en algunas oportunidades, vía comunicación telefónica. Este tipo de técnicas de engaño, son también conocidas como "***ingeniería social***".

El procedimiento más común por medio del cual las personas terminan siendo víctimas de ***phishing*** es el siguiente:

1. Los phishers falsifican el medio que usarán como "carnada" para que parezca confiable: encubren direcciones de correo electrónico para que los receptores crean que provienen de entidades confiables y usan imágenes características de estas, por ejemplo.
2. Luego envían el mensaje a los destinatarios.
3. Al recibirlo, muchos lo toman como auténtico y hacen clic en los enlaces que los hackers adjuntan al mismo, o bien, completan y envían los datos que allí se les solicitan o, en muchos casos, con el solo acto de abrir el mensaje, se descarga automáticamente un malware que se instala en el dispositivo sin que los usuarios lo adviertan.
4. Una vez que ello sucede, los ciberdelincuentes ya tienen la información que buscaban o el acceso a los dispositivos de las víctimas, lo cual les permitirá manejarlos y/o explorar en ellos para extraer lo que deseen.

Por el solo hecho de ser usuarios de Internet, cualquier persona se convierte una potencial vícima de phishing. Siempre debemos estar alertas y ser cuidadosos con nuestra información.

Lo que habitualmente buscan son:

- **Datos de usuarios y claves bancarias.**
- **Datos de tarjetas de crédito y débito.**
- **Información personal y privada.**

La palabra *phishing* deriva del verbo en inglés *fish* que significa "pescar".

Con dicha información pueden, entre otras cosas, robar dinero de cuentas bancarias, cometer nuevas estafas, adoptar la identidad de otras personas para hacer compras y/o llevar adelante otro tipo de delitos, comercializar la información con empresas de publicidad y marketing y, tal como vimos con el ejemplo del mega-hackeo desarrollado en Europa, hasta burlar una red entera de cajeros automáticos y robar grandes cantidades de dinero en pocos minutos.

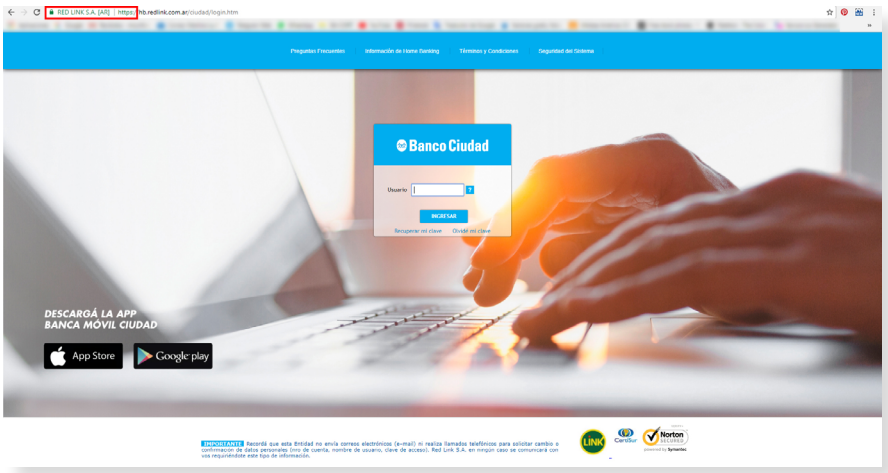
Por eso, considerando las terribles consecuencias que podemos sufrir en caso de ser víctimas de phishing, te sugerimos que tengas en cuenta los siguientes consejos a la hora de abrir correos electrónicos y entrar a sitios web, fundamentalmente si son sitios en los que vas a usar información confidencial, como home-banking o plataformas de compras online.

La información más buscada a través de ésta técnica son claves de acceso a cuentas bancarias y datos de tarjetas de crédito.

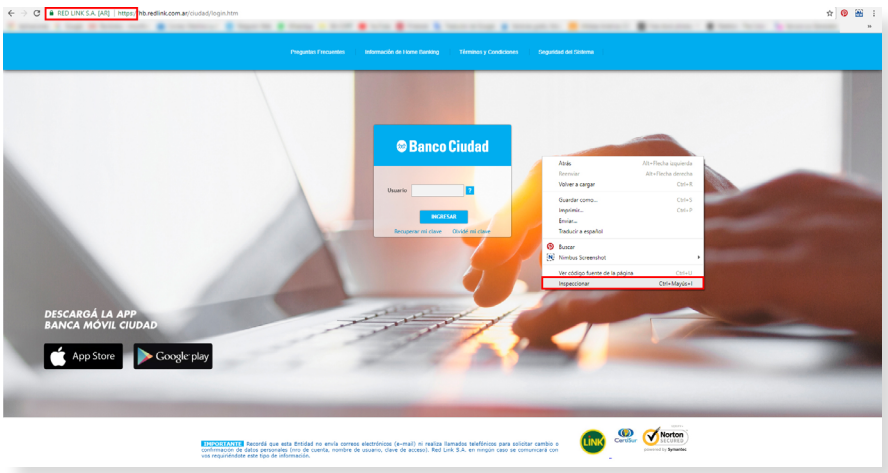
AUTENTICIDAD DE SITIOS WEB

- Verificá que, en la barra de direcciones del navegador, aparezca el símbolo de un candado a la izquierda de la URL de la página; lo cual indica que ese sitio tiene un certificado de seguridad;
- Revisá dicho certificado (más abajo te mostramos en imágenes cómo debés hacer), para verificar lo siguiente:
  1. que el destinatario del mismo sea la entidad/compañía a cuya web estás ingresando;
  2. que el certificado esté vigente y tenga validez por no más de dos años.
- Por último, asegúrate de que aparezca la sigla “https” (en lugar de simplemente “http”) también al comienzo de la dirección. Ello indica que ese sitio tiene cifrado, lo cual garantiza que toda la información que los usuarios escriban sobre él, no pueda ser interceptada, copiada ni hurtada.

Aquí te lo mostramos en imágenes para que quede más claro:

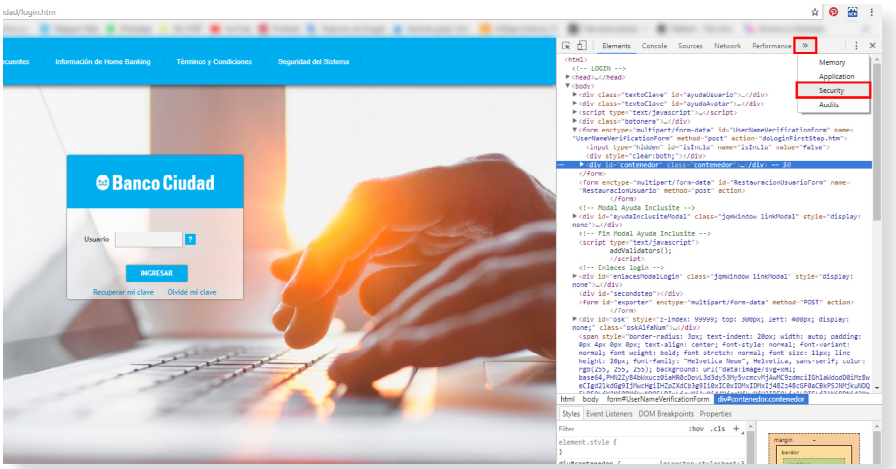


Paso 1: verificar que el sitio sea HTTPS y que aparezca el dibujo del candado.

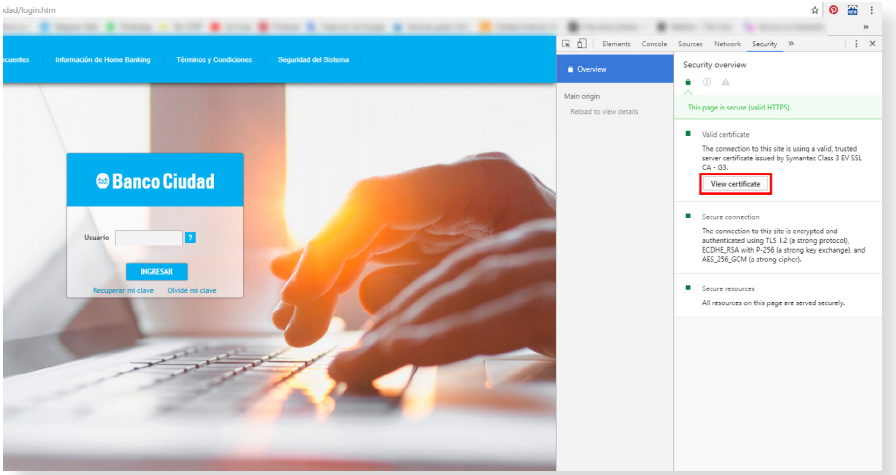


Paso 2: hacer click derecho sobre cualquier punto de la pantalla. Se desplegará un menú, allí seleccionar la opción “Inspeccionar”.

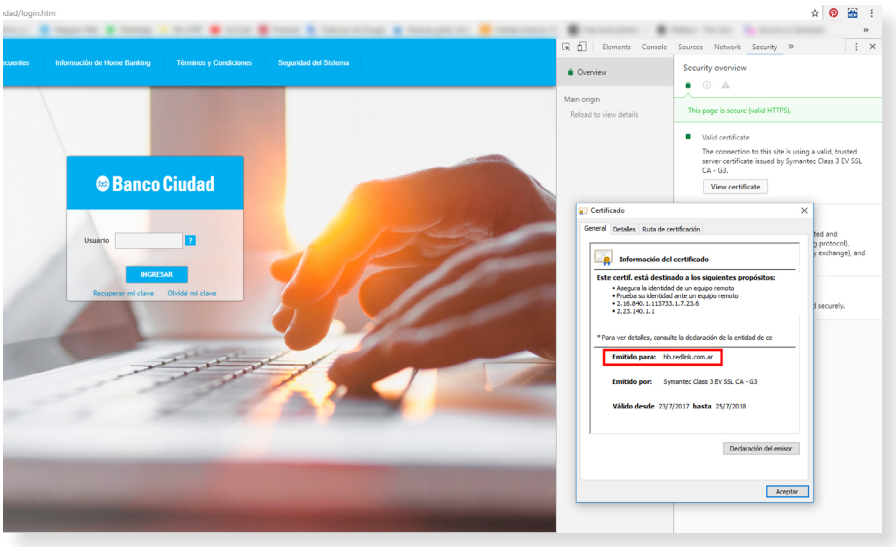
Paso 3: acto seguido aparecerá el "Inspector de elementos" (según el navegador puede cambiar su posición dentro de la pantalla). Dentro del mismo, si es necesario, desplegar el menú y seleccionar la opción "Security".



Paso 4: en la sección de "Security overview", hacer click sobre el botón "View certificate".



Paso 5: como consecuencia, aparecerá una ventana con los datos del certificado. En ella chequear que el mismo haya sido emitido para la entidad a la cual pertenece el sitio.



Como precaución, si vas usar un dispositivo compartido, utilizá el teclado virtual para ingresar tus datos personales.

- Además, te aconsejamos que, al momento de ingresar datos como usuarios, claves, números de tarjetas e información similar, lo hagas a través del teclado virtual que te aparece como opción en los sitios web preparados para que los visitantes carguen datos de ese estilo; en especial si estás utilizando una computadora pública o de uso compartido.

AUTENTICIDAD DE CORREOS ELECTRÓNICOS.

- Nunca confíes ni abras correos electrónicos de remitentes desconocidos, que vayan dirigidos a muchos destinatarios y/o cuyos asuntos te parezcan sospechosos, con mensajes de alerta e incitación a llevar adelante algún tipo de acción o inusuales respecto de lo que comúnmente recibís.
- **Tené siempre presente que las entidades bancarias, las compañías de tarjetas de crédito/débito y/o financieras, nunca te solicitarán que envíes información confidencial por correo electrónico, ni que los ingreses en algún sitio web**; por lo cual, jamás hagas caso a ese tipo de requerimientos y ante la duda, comunícate con la entidad en cuestión para verificar la autenticidad del pedido.
- **Nunca hagas clic en botones o enlaces que aparezcan en correos electrónicos sospechosos**, aunque a simple vista parezca que se trata de sitios web confiables. En tal caso, si quisieras ver qué hay en ese sitio, abrí el navegador e ingresá manualmente la URL en la barra de direcciones.
- Jamás respondas un correo que te resulta sospechoso, directamente eliminalo.
- Y por último, si sospechás haber sido víctima de phishing, cambiá inmediatamente todas tus contraseñas, poné a funcionar el antivirus en el dispositivo que hayas estado utilizando y comunícate con tu banco y/o compañía de tarjetas de crédito para informales acerca de lo sucedido de modo que puedan indicarte los pasos a seguir. ▪