BACSIRT
Vamos Buenos Aires | Centro de Ciberseguridad
LA AGENCIA DE SISTEMAS
www.ba-csirt.gob.ar
BOLETÍN N°12
FECHA DE PUBLICACIÓN
12 04 17

TRANSACCIONES ONLINE: CÓMO OPERAR DE FORMA SEGURA

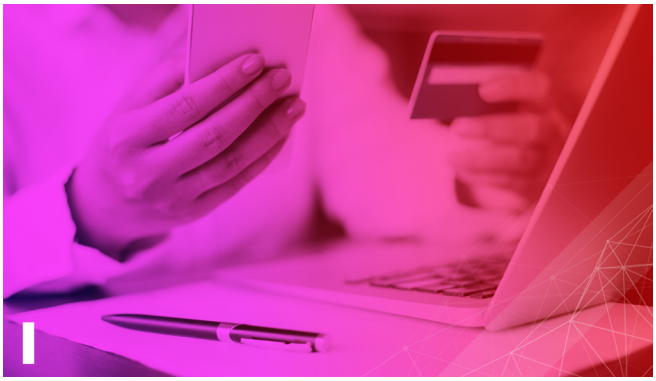
En la época en que vivimos, tenemos la posibilidad de aprovechar cada vez más la tecnología para resolver y solucionar problemas y cuestiones de la vida cotidiana que antes requerían de nuestra presencia o una alta disponibilidad de tiempo. Uno de los ejemplos más emblemáticos al respecto son las operaciones online. Afortunadamente, hoy por hoy casi que no necesitamos realizar enormes filas para efectuar trámites bancarios ni movilizarnos hasta el lugar correspondiente para comprar determinado objeto; en ese sentido, el amplio desarrollo tecnológico con el que contamos nos ha solucionado la vida en muchos aspectos. No obstante, todas estas ventajas podrán ser aprovechadas al máximo siempre y cuando nuestra seguridad a la hora de operar, se encuentre garantizada. Precisamente de eso nos encargaremos en este boletín; te vamos a contar cuáles son los peligros de realizar transacciones online y de qué modo evitarlos, para que a partir de ahora puedas utilizar los beneficios de la tecnología con total tranquilidad.

Los avances tecnológicos hoy en día nos dan la posibilidad de resolver muchos de los trámites y obligaciones que antes requerían sí o sí de nuestra presencia, desde la comidad de nuestros hogares.

Antes que nada: ¿cuáles son los riegos a los que nos exponemos a la hora de realizar operaciones online?

En términos generales, lo que nos puede pasar es **que alguien robe nuestra información y la utilice para efectuar fraude o para robarnos dinero**. Las tácticas más comunes que los ciberdelincuentes utilizan para acceder a nuestros datos son las siguientes:

- **Phishing**: como explicamos en el boletín específico sobre este tema, es el método de engaño más utilizado. Consiste en un fraude que se da por medio del envío de un correo electrónico, el cual



Recordá siempre mantener resguardados los objetos que utilices como segundo factor de autenticación para que no llegan a manos de terceros.

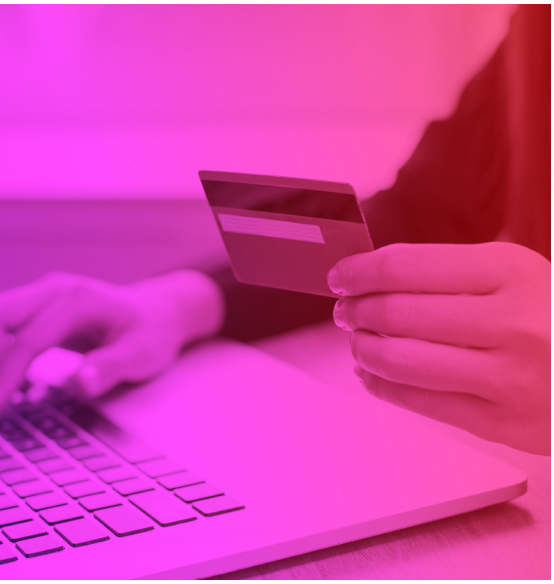
Toda entidad que se tome en serio la seguridad de sus usuarios nunca solicitará información privada y/o sensible a través de medios electrónicos.

tiene el aspecto de ser un e-mail auténtico de la entidad que pretende suplantar; en general estos mensajes imitan la estética y enmascaran la dirección de correo con un nombre que parece pertenecer a la misma. Estos correos suelen solicitar a los usuarios que ingresen a un enlace, incluido en el cuerpo del texto, para modificar su clave, recuperar su nombre de usuario o algún otro pedido similar. Dicho enlace, el cual también está enmascarado o es muy parecido a la URL verdadera de la entidad en cuestión, direcciona al usuario a un sitio web que es administrado por el ciberatacante, quien interceptará y guardará toda la información que allí se escriba.

- **Keylogger**: consiste en una herramienta que se utiliza para registrar las pulsaciones de teclado cuando alguien escribe y, de ese modo, le permite a los ciberdelincuentes obtener los nombres de usuario y claves de acceso de las víctimas.
- **Vishing**: este método es similar al phishing pero se lleva a cabo por medio de una llamada telefónica. Los usuarios reciben una llamada automática que proviene, supuestamente, de una entidad de confianza para verificar información, por lo que se les pide que marquen o digan sus datos y de ese modo, el delincuente se apodera los mismos.
- **Smishing**: como en el caso anterior, se trata de una variante del phishing que se efectúa a través de mensajes SMS.

Como vemos, **lo que se repite en todos los casos es el uso del engaño o bien, de la utilización de herramientas de forma ilícita; prácticas que pertenecen a lo que se conoce como ingeniería social**. Es por ello que lo más importante para no convertirse en una víctima es estar muy atento y ante la duda ser desconfiado, a la vez que te recomendamos enérgicamente implementar los siguientes consejos de seguridad al momento de realizar alguna transacción en línea:

- Tener instalados y actualizados programas antivirus en todos los dispositivos con los cuales se realizarán operaciones que incluyan información privada y sensible.
- Verificar que el navegador que se esté utilizando para operar se encuentre correctamente actualizado y que la opción “autocompletar formularios” esté deshabilitada.
- Preferentemente, y sobre todo si el dispositivo se comparte entre varias personas, no permitir que el navegador guarde las contraseñas.
- No abrir, reenviar ni responder correos electrónicos, mensajes de texto, mensajes de Whatsapp, Telegram o aplicaciones similares que provengan de remitentes desconocidos o resulten sospechosos.
- Nunca hacer clic sobre enlaces contenidos en correos electrónicos o mensajes de texto, en todo caso, escribir manualmente en el navegador la URL a la cual se quiere acceder.
- No confiar en comunicaciones “oficiales” de entidades financieras o similares que soliciten datos personales por medios electrónicos;



Tené en cuenta utilizar redes confiables siempre que vayas a realizar alguna transacción en línea.

una compañía que tome en serio la seguridad y privacidad de sus clientes nunca realizará tales pedidos. De todos modos, y ante la duda, recomendamos comunicarse con la entidad en cuestión para verificar la autenticidad del pedido.

- Cada vez que se acceda a un sitio en el cual se cargarán datos sensibles (claves de acceso a cuentas, números de tarjeta, etc.)
  1. Verificar, por un lado, que en la barra de direcciones del navegador aparezca el símbolo de un candado a la izquierda de la URL. Ello significa que el sitio tiene certificado de seguridad, es decir, que el propietario del mismo es quien dice ser.
  2. Y, por otro, que aparezca la sigla "https" (en lugar de simplemente "http") también al comienzo de la dirección. Ello indica que el sitio tiene cifrado, lo cual garantiza que toda la información que los usuarios escriban sobre él, no podrá ser interceptada, copiada ni hurtada.
- Para acceder a alguna cuenta desde una PC pública o compartida, al momento de ingresar datos como usuarios, claves, números de tarjetas o información similar, utilizar el teclado virtual.
- Guardar cuidadosamente todos aquellos elementos que se usen como segundo factor de autenticación para completar operaciones, como tarjetas de coordenadas y token.

Por último, si tenés la sospecha de que alguna otra persona haya obtenido tus claves, te recomendamos cambiarlas inmediatamente, poner a funcionar el antivirus en el dispositivo que hayas estado utilizando y comunicarte cuanto antes 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. ▪