

TÉCNICAS UTILIZADAS PARA “ATACAR” A LOS USUARIOS DE INTERNET

Como resultado de Las medidas de seguridad, los ladrones de identidad han comenzado a modificar su estrategia y están utilizando nuevas técnicas para atacar directamente contra los usuarios de Internet.

“Phishing” o “Pharming”

Una de las técnicas que más se está proliferando es la que se conoce como “phishing” o “pharming”. Esta técnica utiliza el método de correo electrónico (e-mail) para obtener información de identidad de los consumidores y sus credenciales, tales como: números de cuenta, nombre de usuario y “passwords”, o claves secretas, entre otros.

Este esquema utiliza un correo electrónico a través del cual se le solicita al usuario que visite la página cibernética de una entidad legítima, o le pide que acceda una dirección cibernética que parece legítima utilizando un enlace (“link”) que está dirigido a una página ilegítima. Cuando el usuario la accede, toda la información que divulgue o provea en esta página ilegítima, incluyendo sus nombres de usuarios y claves secretas, o “passwords”, es guardada por el/los ladrón/es de identidad para luego ser usada de forma ilegal. En algunos casos, le indican al usuario que ha ocurrido un problema de seguridad y que tienen que validar la información del consumidor solicitando datos personales tales como: nombre, dirección, número de Seguro Social y números de cuentas bancarios, entre otros.

“Key logging”

Este esquema utiliza un programa de computadora que envía a otra computadora personal en el Internet toda la secuencia de teclas usadas en el teclado de la computadora. Este programa se adquiere usualmente en forma de virus de computadora adjuntado a un e-mail o bajado del Internet a través de otros programas, sin que el cliente se percate. Estos se conocen como “Spyware” o “Adware”.

CÓMO PUEDE PROTEGER SU IDENTIDAD AL USAR EL INTERNET

Scotiabank recomienda que siempre sea cauteloso cuando reciba correos electrónicos y en especial con aquellos que solicitan obtener sus datos personales. Scotiabank NUNCA enviará un correo electrónico solicitando su información personal.

Observe siempre las siguientes medidas de seguridad para prevenir o evitar el robo de identidad en la red del Internet:

1. Nunca responda a correos electrónicos en los que se le solicita información personal.
2. Asegúrese siempre que la dirección de Internet de la página cibernética que está accediendo sea la correcta.
3. Asegúrese que exista una “s” luego de las letras “http” en la dirección. Esta “s” indica que la conexión es segura.
4. Verifique que exista un símbolo en forma de candado en la parte inferior derecha de su monitor: Este símbolo indica que la página que está viendo está protegida por certificados de autenticidad. Este símbolo existe en todas las páginas del servicio de Banca por Internet de Scotiabank, excepto en la página principal, scotiabank.com.do De no ser así, no utilice la página para hacer transacciones bancarias o ingresar sus datos personales.

PREGUNTAS MAS COMUNES SOBRE LA SEGURIDAD DE LA INFORMACION EN EL INTERNET

¿Está segura mi información confidencial?

Cada vez que le pedimos información confidencial a través de Internet, incluyendo datos de sus cuentas personales, requerimos una sesión segura utilizando la tecnología “Secure Socket Layer” (SSL). Esta tecnología de encriptación utiliza llaves públicas para “encriptar” la comunicación entre su navegador SSL y nuestra página de Internet. De este modo prevenimos la interceptación de datos.

¿Cuáles navegadores apoyan SSL?

Recomendamos el uso de navegadores tales como Microsoft Internet Explorer versión 5.5 o más, Netscape versión 7.x o más, Mozilla versión 1.x o más, Safari versión 1.x o más, y Opera versión 6.x o más, los cuales apoyan la encriptación SSL. Si usa otro navegador, verifique la documentación para asegurarse de que sí tenga la capacidad de SSL. No utilice ninguna versión Beta de un navegador para comunicaciones seguras.

¿Cómo puedo verificar que estoy en una sesión segura?

Si usa un navegador Netscape, verá un símbolo en forma de candado cerrado en color amarillo en la parte inferior de su monitor. Si usa Microsoft Internet Explorer, verá un candado amarillo al pie de la ventana del navegador similar a este símbolo . Si usa Macintosh verá una línea azul debajo del menú y un candado amarillo al pie de la ventana del navegador indicando que la sesión está encriptada. Además, con cualquier navegador, puede verificar si está en una sesión segura si la dirección comienza con "https://".

¿Qué navegador se requiere para usar Banca por Internet?

Recomendamos que use un navegador con SSL que apoye encriptación de 128-bit, el cual le provee una comunicación más segura sin costo adicional. A continuación los navegadores recomendados para utilizar Banca por Internet de Scotiabank:

Internet Explorer versión 5.5 SP1 o más para Windows 2000 y XP, Internet Explorer versión 5.x o más para Mac OS 9 y X,

Netscape versión 6.1 o más para Windows 2000 y XP y Mac OS 9 y X.

Scotiabank está comprometido en continuar con sus esfuerzos de proteger la seguridad y privacidad de nuestros clientes. Si tiene preguntas sobre esta información, llámenos al TeleScotia al teléfono: **(809) 567-7268 o 1 (809) 200-7268**, desde el interior sin cargos.

Nuestros representantes están disponibles 24 horas al día, 365 días al año.