Boletín No. 7 – Ciberseguridad
Miércoles 10 de febrero de 2021

AMENAZA DE HACKERS
A INSTITUCIONES FINANCIERAS

La tarde del martes 09 de febrero de 2021, desde la cuenta de Twitter **@corpHotarus** (actualmente suspendida por incumplir las reglas de la red social) se habría publicado, el supuesto robo de información relacionada con el Banco Pichincha, Visa Titanium, Diners Club y Discover. La información comprometida tendría una capacidad de 80 gigabytes, que incluye: datos de clientes y empleados, acceso a sistemas (intranet) y tarjetas de crédito.

En el mensaje se advierte que es una "pequeña demostración" de la información secuestrada y se establece un plazo de 13 días para realizar un pago de 30 millones de dólares en bitcoins, a manera de rescate de la información en su poder; caso contrario **continuarán publicando más información sensible**.

Las instituciones financieras comprometidas a través de sus redes sociales informaron: *"En relación a la noticia que ha circulado en redes sociales sobre un supuesto robo de información, comunicamos que nuestros sistemas no han sido vulnerados y que la información de nuestros clientes se encuentra debidamente resguardada, bajo estrictos estándares internacionales de protección de datos."*, sin embargo, durante la mañana de este miércoles 10 de febrero circuló un enlace para descargar el archivo con dicha información sustraída. Este enlace también fue suspendido por una violación grave de los términos de servicios del sitio de almacenamiento seguro en la nube.

¡IMPORTANTE!

Los ciberdelincuentes continuamente ejecutan ataques a sitios y servicios web con el objetivo de desactivar sus defensas o encontrar vulnerabilidades que les permitan acceder a los valiosos datos que almacenan en sus servidores. Las consecuencias de una filtración de datos son muy graves, pero de alguna manera podemos minimizar el impacto de esta filtración; para esto hay que considerar una serie de **medidas que podemos tomar** si confirmamos que alguna de nuestras cuentas ha sido comprometida, o simplemente si queremos mejorar la seguridad para proteger nuestras cuentas y mantener a salvo nuestra privacidad.

1. Cambiar todas las contraseñas: lo primero y fundamental será cambiar las contraseñas de las cuentas de aquellos servicios que hayan sido comprometidos; y, en el caso de que tengamos otras cuentas en las que hayamos utilizado la misma combinación de correo y contraseña, también deberemos hacerlo.

2. Utilizar una contraseña segura: las contraseñas más débiles son las primeras en ser descubiertas por los ciberdelincuentes. Por ello, para minimizar la posibilidad de que nuestras cuentas sean comprometidas, debemos recurrir a contraseñas robustas y utilizar gestores de contraseñas con los que gestionar distintas contraseñas para cada cuenta.
3. Activar medidas de protección adicionales. Por ejemplo, la verificación en dos pasos (doble factor) siempre que esté disponible en el servicio a utilizar.
4. Comprobar las filtraciones de datos. Finalmente, es recomendable que hagamos una verificación de nuestras cuentas cada cierto tiempo, utilizando para ello herramientas disponibles en la web. De este modo, podremos actuar antes de que nuestra información termine utilizándose para alguna actividad ilícita o sea vendida a terceros.

Es importante que recordemos que, aunque estas filtraciones se deben a vulnerabilidades en los propios sitios y servicios web, **no podemos dejar de lado la seguridad de nuestras cuentas**. El sentido común y la mirada crítica nos ayudarán, por ejemplo, a combatir los ataques basados en ingeniería social que buscan hacerse con nuestros datos y contraseñas.[1]

Nuestros activos financieros, son muchas veces el sustento y patrimonio de nuestras familias y por ello es importante protegerlos. Una medida importante y efectiva es estar muy atentos a posibles contactos o comunicados desde fuentes no autorizadas, personificando a una determinada institución financiara u operadora de tarjetas de crédito, que podrían llegar a través de: Llamadas telefónicas, Correos electrónicos, Conversaciones por chat, Mensajes de texto, u otros.

Estos mensajes podrían contener muchos detalles aparentemente válidos sobre una persona y su entorno familiar, que podrían conducirnos a creer que es un mensaje real de una institución financiera. Por ejemplo, podrían incluir: Direcciones, Teléfonos, Saldos de puntos/millas, Movimientos de uso/activación de servicios, entre otros.

Lo importante es que NO se entregue ningún dato confidencial por teléfono, correo, o ningún otro medio. Se debe desconfiar hasta no tener completa certeza.[2]

Fuente: cuenta de Twitter @Bank_Security,
Oficina de Seguridad del Internauta-OSI,
CSIRT CEDIA

[1] https://www.osi.es/es/actualidad/blog/2020/12/09/cuentas-comprometidas-compruebalo
[2] https://csirt.cedia.edu.ec/2021/02/cuidados-digitales-financieros/