Ciberataques: Cinco consejos para proteger tus cuentas bancarias y dinero

Ante el auge de las nuevas tecnologías y el crecimiento exponencial del trabajo remoto y el incremento de las actividades digitales, todos los usuarios del ciberespacio están expuestos a vulnerabilidades a causa de los ciberataques; debido a que se comparte información personal y profesional y se realizan transacciones online en equipos móviles, laptops, celulares, redes electrónicas y sistemas digitales.

En el 2021 los intentos de ciberataques a entidades financieras se han incrementado en un 52% con respecto al año 2020, siendo las redes sociales y servicios de mensajería los más usados por los ciberdelincuentes para la propagación de *malware* y uso de técnicas de ingeniería social en aras de obtener de manera ilícita datos e información de clientes.

Para que los usuarios puedan realizar sus transacciones con seguridad y evitar ser perjudicado por los ciberataques, los especialistas de Seguridad de la Información del **Banco de Comercio** recomiendan los siguientes pasos a considerar:

1. Evite y protéjase de la suplantación de la identidad o

estafas en las redes sociales

Si un usuario es estafado en las redes sociales, lo primero es mantener la calma. Debe reunir las pruebas que sustenten el hecho, tales como: capturas de pantalla, grabaciones de audio o video, correos electrónicos, etc. Seguido de ello, se debe denunciar la estafa ante la DIVINDAT (unidad especializada en delitos informáticos) de la PNP, proporcionando el mayor detalle posible y aportando las pruebas con las que se cuente.

Es común encontrar en las redes sociales cuentas duplicadas o falsas, ante ello hay tener cuidado cuando se interactúa con las cuentas sospechosas (usualmente no tienen foto y son de reciente creación). En el caso del Facebook del Banco de Comercio, su cuenta oficial tiene el check azul de la red social, la cual certifica que se trata de una cuenta oficial y no de una copia.

2. Evite dar click en enlaces maliciosos

Debemos prestar principal atención a los hábitos de navegación en las páginas web sospechando de aquellos sitios que no cuenten con las medidas mínimas de seguridad, tales como: ausencia de protocolos de comunicación segura (https), inexistencia de certificados de seguridad (candados de seguridad) o que intenten descargar archivos sin su autorización.

El “phishing” es el método más usado por los hackers **(cuando se recibe un correo electrónico falso y/o temporal que**

solicita información personal a través de un link), por eso es importante que los clientes adopten buenas prácticas de seguridad en su vida diaria.

Se recomienda siempre tener actualizados los dispositivos electrónicos y usar un buen antivirus en aquellos lugares desde donde habitualmente se ingresa información personal o se realizan las operaciones financieras.

3. No brindes tus datos personales, ni datos bancarios

Se recomienda a los usuarios que sean muy cautos con su información, desconfiar de terceros desconocidos que intenten contactarlos por medio de mensajes de texto, redes sociales, correos electrónicos, llamadas de voz, etc. para solicitar su información personal y financiera (nombres, N° DNI, cuentas, claves, entre otros).

Un ejemplo de una modalidad de ciberataque es el *Smishing*, consiste en recibir de una entidad bancaria un mensaje de texto indicando que se ha bloqueado la cuenta y se pide al usuario que ingrese a un link para que coloque su información personal. Se recomienda no ingresar al link, bloquear el número y no responde el mensaje.

4. Siempre verifica muy bien las

letras del enlace web y no respondas llamadas sospechosas

Es aconsejable guiarse de los URL con «hhtps» y webs con el candado verde de seguridad. Si las personas ingresan a páginas con enlaces sospechosos o que no tengan el candado de seguridad deben tener cuidado con su información y abandonar dicho portal web.

El Banco de Comercio recomienda que cuando los usuarios busquen su página web, ingresen siempre la dirección completa en su buscador, digitando www.bancomercio.com para que se acceda de forma segura y directa.

Por otro lado, otra de las modalidades de ciberataque, es la denominada, Wangiri, consistente en recibir una llamada y se corta al contestarla, provocando que la víctima quiera devolver la misma y así generar dinero para el estafador, ante ello se aconseja no devolver la llamada ni bloquear el número.

5. Promueve una cultura de ciberseguridad en la organización

Hoy en día la ciber resiliencia en las organizaciones es vital para sostener la continuidad de los negocios, uno de los aspectos clave es sensibilizar a los trabajadores, clientes, socios y accionistas de las empresas a través de charlas, ya que es necesaria su participación activa para detectar riesgos y aplicar día a día un protocolo de respuesta inmediata en cadena ante los ciberataques, se aconseja que los líderes de la compañía generen valor en la co creación con sus equipos de

trabajos para acelerar los procesos de digitalización y fomentar hábitos como utilizar contraseñas complejas en routers y móviles, realizar copias de seguridad de los datos y evitar la conexión a redes Wifi desconocidas.

Finalmente, el Banco de Comercio continua su proceso de transformación digital e incorporando controles de seguridad (code review y ethical hacking) en el diseño y construcción de sus plataformas digitales, así como la inclusión de una solución de autenticación biométrica en todas sus plataformas onboarding, para minimizar el riesgo de fraude financiero.