CUIDADO CON LO QUE CLICKEAS

La nueva modalidad de fraude

Con la digitalización de los servicios financieros y el uso creciente de plataformas bancarias, los fraudes se han vuelto más sofisticados y difíciles de identificar. La rapidez con la que las o los ciberdelincuentes crean nuevas estrategias resalta la importancia de mantenernos alerta y proteger nuestra información personal y financiera para prevenir vulneraciones a nuestra privacidad.

En este artículo, queremos hablarte sobre un nuevo tipo de ataque cibernético, conocido como: *Man-in-the-Middle*, el cual representa una amenaza significativa para tus datos personales y financieros. Te explicaremos en qué consiste, cómo opera y cuáles son las señales de alerta que pueden ayudarte a identificarlo.

¿En qué consiste?

Este tipo de ataque cibernético ocurre cuando un *hacker* interviene en las comunicaciones entre dos partes, con el objetivo de interceptar, alterar o robar la información que se transmite entre ambos, sin que ninguna de las partes lo note. Por ejemplo, si accedes a tu cuenta bancaria desde una red pública de internet, un atacante podría interceptar los datos que envías y recibes, obteniendo así tus credenciales de acceso y otra información personal.

Este fraude pone en riesgo tus finanzas al permitir que las o los ciberdelincuentes accedan a información confidencial, realicen transacciones no autorizadas y vendan tus datos. Además, pueden manipular comunicaciones para hacerte creer que interactúas con una entidad legítima.

¿Cómo lo llevan a cabo?

La persona atacante primero accede a tu conexión, y algunas formas de hacerlo es a través de una red Wi-Fi pública no segura, la descarga de archivos de páginas desconocidas o mediante trampas como correos falsos (*phishing*) y sitios web engañosos.

Una vez infiltradas, las personas atacantes redirigen los datos que envías y recibes a través de su propio dispositivo sin que lo notes. Por ejemplo, si usas una red pública para realizar compras en línea e ingresas los datos de tu tarjeta, y el sitio no tiene la seguridad adecuada, pueden capturar esa información para hacer compras o retirar dinero.

Otro método es tomar el control de las cuentas de correo electrónico de empresas u organizaciones, especialmente de instituciones financieras. Con acceso a estas cuentas, interceptan mensajes y recopilan datos personales y transacciones de las y los clientes, lo que les permite cometer fraudes que afectan tanto a las empresas como a sus personas usuarias.

Al cierre de 2023 las quejas por fraudes cibernéticos crecieron un 20.1% en comparación con 2022, representando el 71% del total de fraudes, frente al 59% registrado en 2018.

CONDUSEF

Formas de prevenirlo

Aunque nadie está exento de ser víctima de fraudes o ataques cibernéticos, existen medidas que puedes tomar para reducir significativamente los riesgos. Aquí te compartimos algunas recomendaciones clave:

Evita conectarte a redes Wi-Fi públicas. Estas redes son especialmente vulnerables quien busca atacar puede acceder a ellas sin autorización o incluso crear redes falsas con nombres similares para engañar a las y los usuarios. Si es imprescindible utilizarlas, evita compartir información sensible, realizar transacciones bancarias o descargar archivos.

Instala y actualiza un antivirus. Aunque puede parecer básico, un buen antivirus es esencial para mantener tus dispositivos protegidos. Asegúrate de configurarlo correctamente y mantenerlo actualizado para bloquear amenazas.

Revisa que los sitios tengan "https://". Las páginas web con este protocolo de seguridad cuentan con un certificado que encripta la información, protegiéndola de ser interceptada por terceros.

Descarga aplicaciones solo de fuentes confiables. Muchas amenazas se ocultan en aplicaciones o archivos que parecen legítimos. Asegúrate de usar tiendas oficiales como *Google Play* o *App Store*, y antes de descargar algo, reflexiona si realmente lo necesitas.

Adoptar hábitos de seguridad, como proteger tus dispositivos, evitar redes inseguras y verificar la autenticidad de las páginas web y aplicaciones que utilizas, no solo reduce el riesgo de ser víctima de fraude, sino que también te permite disfrutar de los beneficios de la tecnología con mayor tranquilidad. La seguridad comienza con pequeñas acciones, y cada medida que tomes marcará la diferencia en la protección de tu información.

Según datos de la firma de ciberseguridad Fortinet, durante la primera mitad de 2024, México enfrentó 31 mil millones de intentos de ciberataques, lo que equivale al 55% del total registrado en América Latina.