



imperiasti®

Líder es Cumplir

## Cómo evitar el fraude bancario.

Con el avance de la bancarización en todos los estratos sociales y la digitalización del dinero también creció el robo de datos y las estafas virtuales.

Los fraudes y las estafas virtuales siguen aumentando y sofisticándose en la medida que continúa creciendo la digitalización y la bancarización mediante el uso de medios de pagos digitales y de billeteras virtuales. Los ciberdelincuentes aplican nuevas formas de fraudes y estafas y muchas veces resulta difícil prevenirlas. Una de las más comunes es la que está directamente vinculada con Correos electrónicos y/o llamadas telefónicas que tiene como objetivo robar las claves personales de home banking para hacerse del dinero de las cuentas.

Mientras que otro de los métodos delictivos más identificados es el del pedido de descarga e instalación de aplicaciones en celulares y computadoras. Se trata de programas que permiten a los estafadores acceder a la visualización de lo que se está realizando en la pantalla de los dispositivos para robar datos personales.

En sí el método que venimos definiendo conocido como “phishing” o la suplantación de identidad es un mecanismo que se utiliza para conseguir información confidencial de forma fraudulenta y así apropiarse de la identidad digital de las personas. Estar alerta e informado/a, así como custodiar celosamente la información confidencial, da la posibilidad de prevenir cualquier vulneración que ponga en riesgo el bienestar financiero de las personas.

Para evitar el fraude bancario, es importante seguir prácticas seguras y estar atento a posibles señales de actividad fraudulenta. Aquí hay algunas medidas que puedes tomar para protegerte:

### **Mantén seguras tus credenciales bancarias**

Nunca compartas tu información de inicio de sesión, contraseñas, números de cuenta o información personal con nadie, especialmente por correo electrónico, teléfono o mensajes de texto. Los bancos nunca te pedirán esta información por estos medios.

### **Utiliza métodos de autenticación seguros**

Aprovecha las medidas de seguridad ofrecidas por tu banco, como la autenticación de dos factores (2FA), que requiere un código adicional, a menudo enviado a tu teléfono móvil, para acceder a tu cuenta o mediante huella dactilar.

### **Verifica la autenticidad de los sitios web y las comunicaciones**

Asegúrate de que estás utilizando el sitio web oficial de tu banco al acceder a tu cuenta en línea. Verifica la URL y busca el candado de seguridad en la barra de direcciones del navegador para garantizar que la conexión sea segura. Evita hacer clic en enlaces sospechosos o proporcionar información confidencial en sitios web no verificados. Desconfía de los correos electrónicos o mensajes que soliciten información confidencial y verifica su autenticidad contactando directamente con tu banco.

### **Revisa tus cuentas regularmente**

Monitorea tus estados de cuenta bancarios y tarjetas de crédito con regularidad



imperiasti®

Líder es Cumplir

para detectar cualquier actividad sospechosa. Si encuentras transacciones no autorizadas, repórtalas de inmediato a tu banco.

#### **Evita estafas con DEBIN / CREDIN**

A menudo, las estafas se presentan en forma de compras por internet, a través de plataformas como redes sociales o mensajes de texto. El estafador, haciéndose pasar por un comprador, convence a la víctima para que "acepte la transferencia (DEBIN)", cuando en realidad está autorizando un CREDIN hacia la cuenta del estafador. Reconocer que un Debin no equivale a una transferencia; estas últimas no requieren autorización. La complejidad radica en que estas transferencias son irrevocables. Reconocer que un Debin no equivale a una transferencia; estas últimas no requieren autorización.

Confirma la identidad del destinatario antes de realizar pagos. Antes de realizar transferencias de dinero a través de sistemas como DEBIN o CREDIN, verifica la identidad del destinatario y asegúrate de que la transacción sea legítima.

No autorizar un Debin si no se espera recibir un pago.

Mantenerse alerta, ya que el estafador solo necesita el alias o CBU de la cuenta para solicitar el débito, sin necesidad de más información.

Es esencial revisar detenidamente los mensajes de confirmación de las operaciones bancarias y abstenerse de aceptar o realizar movimientos si se tiene alguna duda sobre la legitimidad del procedimiento. Al aceptar un Debin, verificar que la transacción sea la correcta.

Si eres un vendedor, estar especialmente alerta ante posibles compradores fraudulentos que empleen este método de estafa.

Mantenerse vigilante frente a llamadas telefónicas, mensajes de texto o correos electrónicos que soliciten números de cuenta o alias, seguidos por peticiones de autorización de transacciones.

Comunícate directamente con la persona o empresa a través de información de contacto verificada para confirmar los detalles de la transacción.

#### **Protege tus dispositivos**

Mantén actualizado el software de seguridad en tus dispositivos, como antivirus y firewall, y ten cuidado con los enlaces y archivos adjuntos de correos electrónicos y mensajes de texto, ya que podrían contener malware diseñado para robar información.

#### **Protege tus dispositivos móviles**

Evita acceder a tu cuenta bancaria desde dispositivos públicos o redes Wi-Fi no seguras.

Usa medidas de seguridad como el bloqueo de pantalla, la huella dactilar o el reconocimiento facial en tus dispositivos móviles para evitar el acceso no autorizado a tus aplicaciones bancarias.

#### **Ten cuidado con las llamadas no solicitadas**

**Desconfía de las llamadas telefónicas no solicitadas que soliciten información personal o financiera.** Siempre verifica la autenticidad de la llamada contactando directamente con tu banco a través de un número de teléfono oficial.

#### **Educación sobre estafas**



imperiasti®

Líder es Cumplir

Mantente informado sobre las últimas estafas y técnicas utilizadas por los estafadores. Esto te ayudará a reconocer posibles intentos de fraude y tomar medidas para protegerte a ti mismo y a tus finanzas. Comparte esta información con familiares y amigos para ayudarles a protegerse también contra el fraude bancario.

Al ser consciente de estas medidas de seguridad y mantener una actitud vigilante, puedes reducir el riesgo de convertirte en víctima de fraude bancario.

Héctor M. Amodeo

Socio

Gerente Comercial