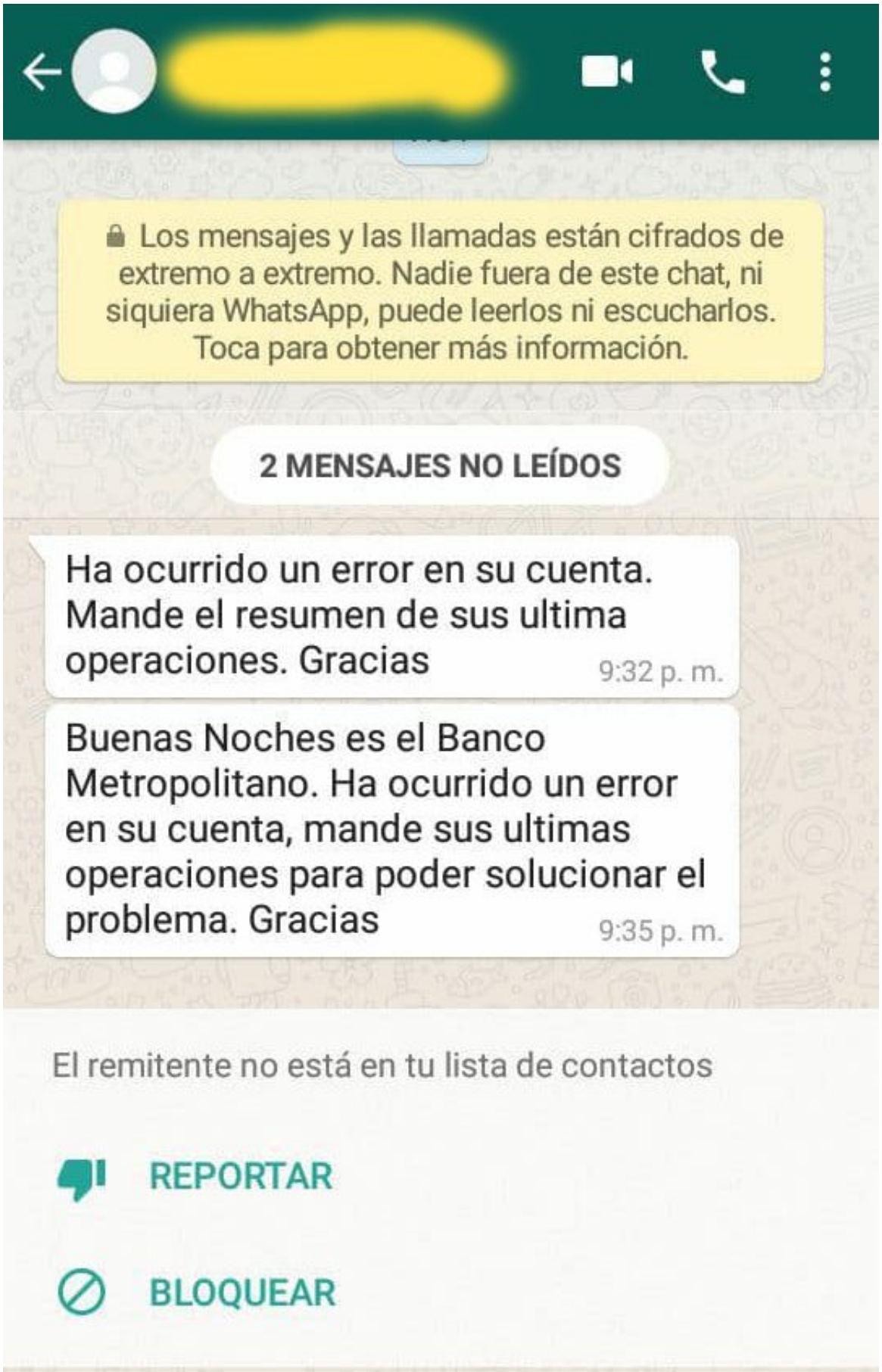
Alertan sobre posible estafa para hacerse con tu tarjeta electrónica.
Última actualización: Jueves, 26 Noviembre 2020 16:25
Visto: 1020

El comercio electrónico en Cuba, es un hecho. Miles de cubanos se han beneficiado de las bondades de la informatización. Incluso en momentos de pandemia, se simplificaron procesos que hace algunos años se veían empantanados en largos procedimientos burocráticos, o como conoce el cubano, en largas colas. Nacieron y se fortalecieron opciones para el transporte y la gastronomía. Se facilitó el pago de servicios de electricidad, gas, telefonía, agua, internet, entre otros. Y en casi todos estos servicios, dos plataformas estuvieron involucradas: Transfermóvil y Enzona.

Pero en la era de las compras y servicios online, también hay sombras. Cada día se dan a conocer nuevos métodos para proteger nuestros datos, en la misma medida en que salen a relucir nuevas formas de estafa. Y Cuba no está exenta de eso. Antiguas formas de suplantación de identidad, lo que conocemos como phishing, virus informáticos para robar información, test y mucho más, suceden también en nuestra isla. Pero algo mucho más simple nos pasa factura, la falta de conocimiento de las tecnologías de la información.

Desde hace unos días circula por grupos de redes sociales, una alerta sobre cómo un estafador puede hacerse con el control de tu tarjeta de banco mediante el uso coordinado de las aplicaciones de Transfermóvil y Enzona.

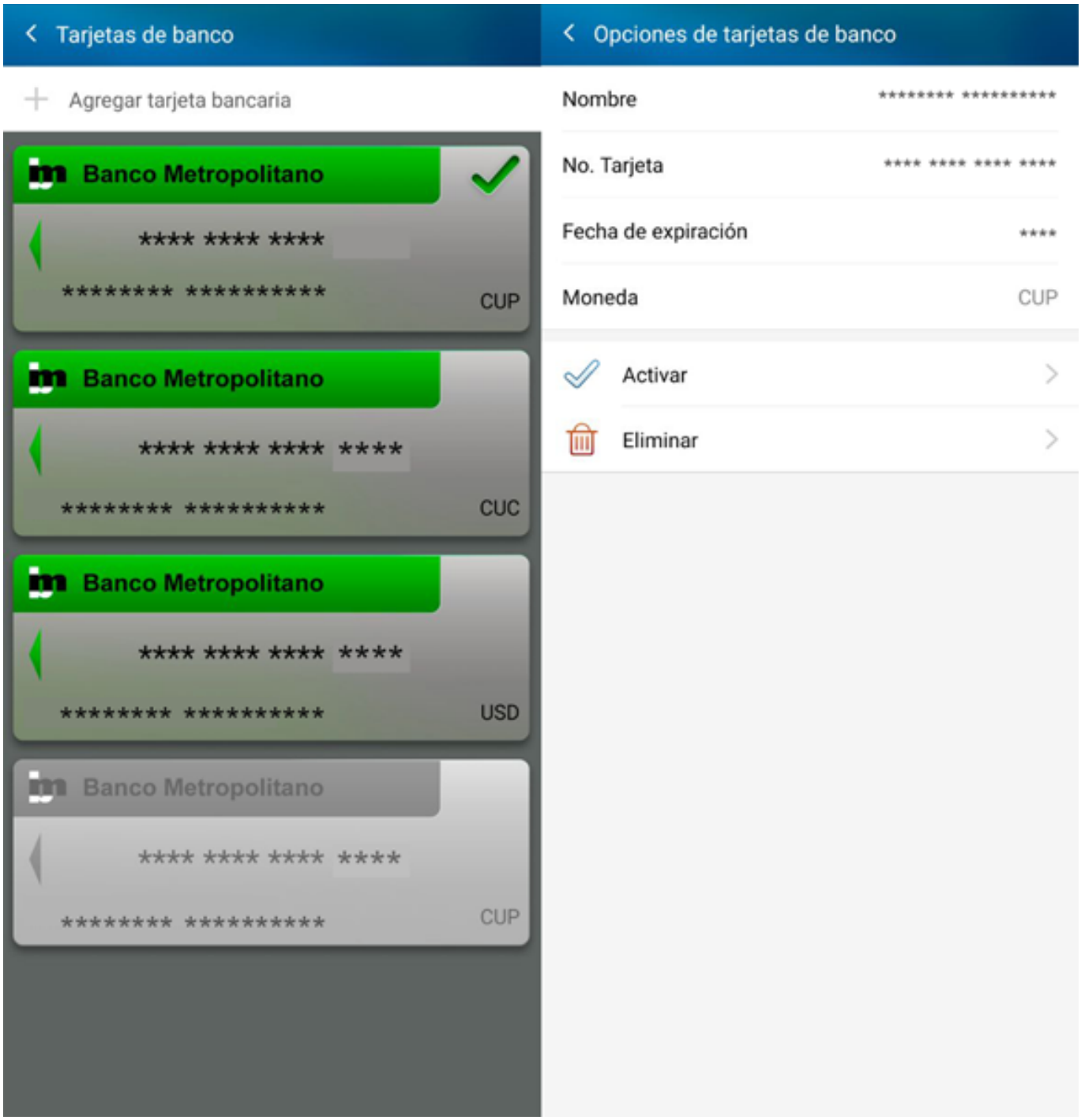
La aparición de capturas de pantalla con chats privados donde individuos se hacen pasar por instituciones cubanas exigiendo datos personales de los usuarios, incendió aún más las redes sociales, en especial Twitter, Youtube y Telegram.


Los mensajes y las llamadas están cifrados de extremo a extremo. Nadie fuera de este chat, ni siquiera WhatsApp, puede leerlos ni escucharlos. Toca para obtener más información.
2 MENSAJES NO LEÍDOS
Ha ocurrido un error en su cuenta. Mande el resumen de sus ultima operaciones. Gracias
9:32 p. m.
Buenas Noches es el Banco Metropolitano. Ha ocurrido un error en su cuenta, mande sus ultimas operaciones para poder solucionar el problema. Gracias
9:35 p. m.
El remitente no está en tu lista de contactos
REPORTAR
BLOQUEAR

La estafa ocurre de la siguiente forma:

El estafador se pone en contacto con la víctima y le pide el número de tarjeta para enviarle una transferencia. Al recibir el número, agrega esa tarjeta a su cuenta de Enzona y solicita el código de verificación que exige la aplicación para completar el proceso.

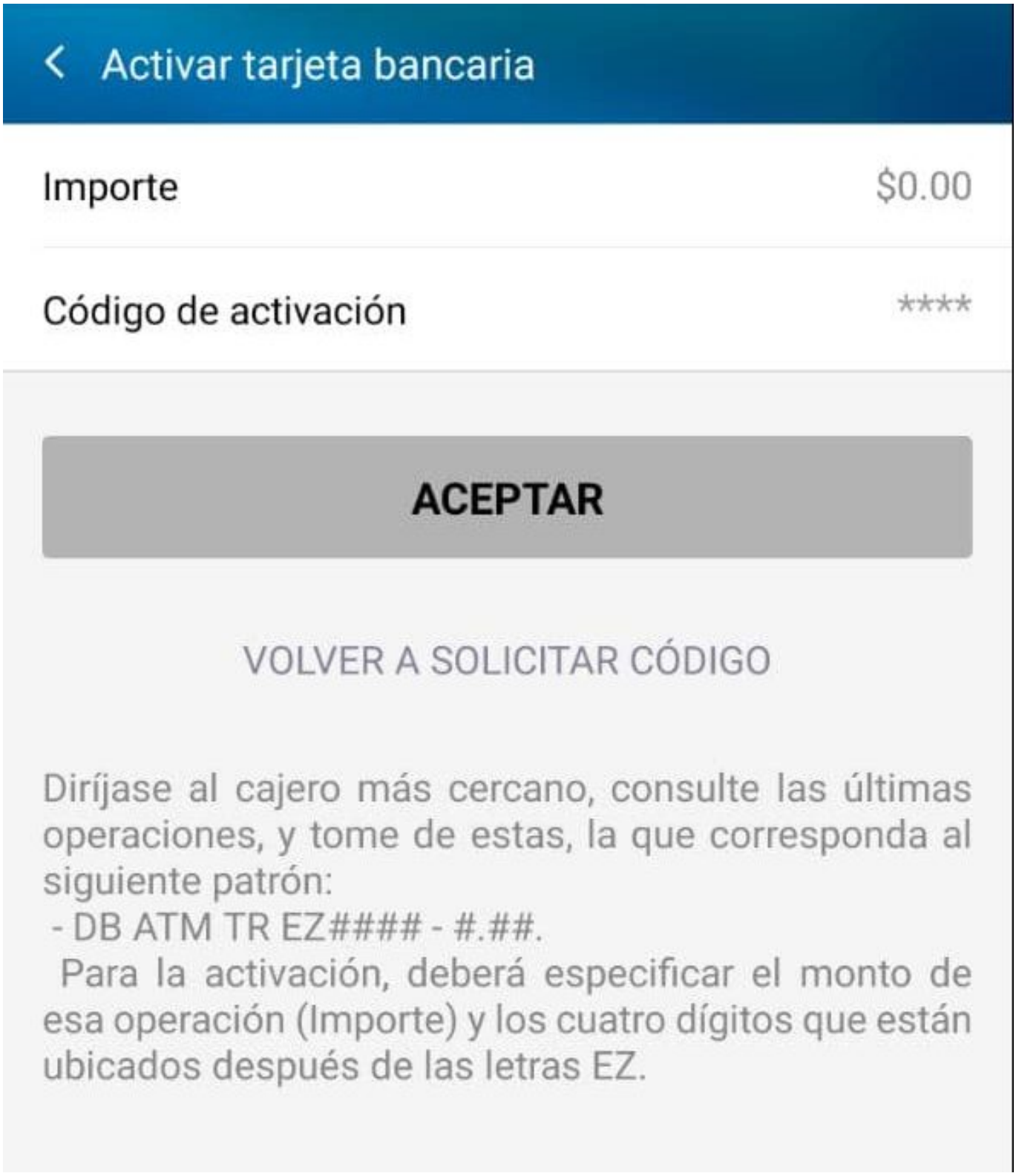
El código que pide Enzona, se toma de las últimas operaciones que el usuario debe consultar en el cajero o a través de Transfermóvil. La numeración es el resultado “del monto de la operación (importe) y los cuatro dígitos que están ubicados después de las letras EZ”, dice la información proporcionada para activar la cuenta.



Como al estafador le falta ese paso, le dice al usuario que ya realizó el pago. El usuario nota que no ha recibido nada y se lo comunica. Es entonces que el individuo, en el papel de víctima, le pide que envíe una captura de las diez últimas operaciones para comprobar que la otra persona dice la verdad.

Como el atacante ya lo había solicitado desde su cuenta, en la solicitud de las últimas operaciones estará el código que necesita el estafador para completar el proceso. El usuario le envía la captura, y

el atacante completa el último paso para hacerse con la tarjeta y así agregarla a su cuenta.



Esta estafa tiene las piernas cortas. Enzona exige un número de teléfono, solo admite IP nacionales (en caso de aquellos que quieran

perderse tras una VPN), pero más importante, el atacante debe transferir el dinero a otra tarjeta si quiere disfrutarlo. Por lo que es fácil atrapar al estafador. Sin embargo, según nos confirmó el equipo de Enzona, se han dado casos de diversas estafas.

En manos de alguien que no es nativo digital, puede adjudicarse la culpa a un error de la pasarela de pago o el banco. Sin embargo, amén de que puedan implementarse más funcionalidades para evitar este tipo de estafas, la cultura informática es la primera línea de defensa de toda aplicación o página web que contenga datos personales.

Enzona recomienda NO ENVIAR el número de cuenta o las últimas operaciones a otra persona. Asimismo, el usuario no debe proporcionar por ninguna vía datos esenciales de su cuenta, como el PIN, la contraseña, el correo o su número de teléfono. Los usuarios deben utilizar sus datos únicamente para acceder a la plataforma www.enzona.net (compruebe siempre que el dominio coincida con el sitio oficial).

> **ENZONA@ENZONA_BX**

Para evitar ser engañado, por servicios que solicitan datos de sus tarjetas, cuentas y contraseñas, le aconsejamos… https://t.co/LaWBKUKivD

¿Cómo proteger tu cuenta?

1. Usa contraseñas seguras y doble factor

Usa contraseñas únicas para cada sitio web. Enzona tiene además autenticación de doble factor y por huella.

2. Cuidado con lo que compartes en redes sociales

No compartas información personal en redes sociales. No uses tu nombre completo y evita contestar tests donde la respuesta involucra dar información sensible, como tu fecha de nacimiento o número de teléfono, etc. También procura ocultar tu email y teléfono personal de tu perfil.

3. No ingreses tus datos en redes públicas

Cuando te encuentres en una wifi pública, nunca debes introducir información personal, ni contraseñas. Cualquier persona tiene acceso a esa red, por tanto, es posible llegar a tus datos personales.

4. Cuidado con el phishing

El phishing es un tipo de fraude en el que se busca obtener contraseñas o información financiera.

Prevenirlo es muy simple: No abras enlaces ni descargues archivos enviados por desconocidos. Estos podrían ser virus o programas espías que buscan robar tu información.

Otra modalidad del phishing consiste en suplantar a alguna institución de confianza. Si recibes un correo de un banco o compañía diciendo que tienes una cuenta con ellos y que debes confirmar tus datos, tampoco hagas clic en enlaces o descargues nada. Ante cualquier duda contacta con tu banco.

CUBADEBATE