



PHISHING BANCARIO

Por: 3+ Security Colombia

Es un tipo de estafa que consiste en enviar correos electrónicos fraudulentos que engañan a los destinatarios para que compartan su información personal, financiera o de seguridad.



78%

de las personas son conscientes de los riesgos de los enlaces desconocidos **y sin embargo les dan click**

Le suenan estas frases?

Acceda al siguiente enlace para conocer sus deudas

Presione click aquí para descargar su estado de cuenta

Multa por el incumplimiento de sus obligaciones con la Dian

Evítese sanciones, revise por favor el documento anexo

4 DE CADA 10

Pymes en Europa han recibido al menos un intento de Phishing en el último año

CÓMO LO HACEN?

Estos correos pueden parecer idénticos al tipo de correspondencia que envían los bancos reales

- Le piden que descargue un archivo adjunto o de click en un enlace.
- Usan un lenguaje que transmite sentido de urgencia.
- Los ciberdelincuentes asumen que las personas están ocupadas o distraídas y a simple vista estos correos pueden parecer reales o legítimos.
- Se debe tener más cuidado en el celular, pues en estos dispositivos es más difícil detectar que es un intento de Phishing, que en un computador.

CUÁNTO PUEDE GANAR UN ATACANTE?



1 MILLÓN de correos enviados



5,000 Lo abren



1,000 Envían datos



10 USD a cada uno

USD 10.000

CLAVES PARA EVITARLO

- Mantener actualizadas las aplicaciones como el antivirus, también el navegador y el sistema operativo.
- Preste atención especial si llega un correo de su banco (u otro banco) solicitando información personal.
- Revise el correo con cuidado: compare la dirección con la de los mensajes habituales de su banco, revise si hay errores de ortografía o gramática.
- No responda a un correo sospechoso. Si va a reportarlo a su banco escriba a la dirección de correo habitual, NO a la del correo sospechoso.
- NUNCA haga click en el enlace ni descargue archivos adjuntos. Tome nota de la dirección, pantallazo del correo y repórtelo a su banco a través de otro canal: chat virtual o redes sociales.
- En caso de duda, Asuma que se trata de un fraude y comuníquese con su banco