'PHISHING' BANCARIO POR CORREO ELECTRÓNICO

'Phishing' se refiere a correos electrónicos fraudulentos que engañan a los destinatarios para que compartan su información personal, financiera o de seguridad.

¿CÓMO LO HACEN?

Estos correos electrónicos:

Pueden parecer idénticos al tipo de correspondencia que envían los bancos reales.

Copian los logotipos, el diseño y el tono de los correos electrónicos reales.

Te piden que descargues un documento adjunto o hagas clic en un enlace.

Usan un lenguaje que transmite un sentido de urgencia.

Los ciberdelincuentes asumen que las personas están ocupadas; a simple vista, estos correos electrónicos falsos parecen ser legítimos.

Ten cuidado cuando uses un dispositivo móvil. Puede ser más difícil detectar un intento de 'phishing' desde tu tableta o móvil.

¿QUÉ PUEDES HACER?

- **Mantén tus aplicaciones actualizadas,** incluyendo navegador, antivirus y sistema operativo.
- Presta especial atención si un correo electrónico de tu 'banco' te solicita información confidencial (p. ej. la contraseña de tu cuenta bancaria).
- **Revisa el correo con cuidado:** compara la dirección con los mensajes auténticos de tu banco. Comprueba si existen errores de ortografía o de gramática.
- **No respondas a un correo electrónico sospechoso,** reenvíalo a tu banco escribiendo tú la dirección real.
- **No hagas clic en el enlace o descargues el archivo adjunto, escribe la dirección real de tu banco en el navegador.**
- En caso de duda, **comprueba la información** entrando en la página web de tu banco o por teléfono.

#Ciberestafa

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · ASOCIACIÓN ESPAÑOLA DE BANCA · DSN