PHISHING Y ESTAFAS: ANATOMÍA DE UN ENGAÑO

Los atacantes imitan a tu banco, redes sociales o proveedor para robarte datos y dinero. Aprendé a reconocer el engaño antes de hacer clic.

>> SEÑALES DE ALERTA

01 Urgencia artificial

"Actúe ya o su cuenta será bloqueada". Buscan que actúes sin pensar.

02 Premios y dinero fácil

"Ganaste un premio, ingresá tus datos para cobrarlo". Explotan la ambición.

03 Dirección casi idéntica

www.faceb00k.com en vez de facebook.com: ceros que parecen letras "o".

04 Enlaces acortados

bit.ly/Ub1XC1 oculta el destino real. El navegador puede terminar en otro sitio.

05 Adjuntos inesperados

Archivos que al abrirse instalan malware y roban tus datos.

06 Diseño "oficial"

Usan logos, textos y estética reales de la empresa. Que se vea bien no prueba nada.

>> VARIANTES DEL MISMO ENGAÑO

PHISHING — e-mail

SMISHING — SMS / WhatsApp

QUISHING — códigos QR falsos en parquímetros, restaurantes y mensajes

>> PROTOCOLO ANTE CUALQUIER MENSAJE SOSPECHOSO

1. **Dudá siempre**
   Desconfiá de todo mensaje que recibas, conocido o no. Pensá dos veces antes de hacer clic.

2. **No hagas clic ni abras adjuntos de desconocidos**
   Lo ideal es ignorarlos directamente.

3. **Nunca entregues tus datos por mensaje**
   Los servicios legítimos no piden usuario y contraseña de esta forma.

4. **Verificá por el canal oficial**
   Ante la duda, llamá por teléfono a la empresa para confirmar si el mensaje es real.

5. **Inspeccioná la dirección exacta**
   Antes de ingresar datos, confirmá que la URL coincida exactamente con la del sitio verdadero.

REGLA DE ORO

Siempre dudá y luego verificá antes de confiar.