CIBERCONSEJOS

¿QUÉ ES EL PHISHING Y CÓMO PROTEGERTE?

¿Qué es el Phishing?

El phishing es una técnica de fraude digital usada por ciberdelincuentes para engañarte y robar tus datos personales, financieros o de acceso. Se hacen pasar por bancos, redes sociales o empresas conocidas, usando medios como:

- Correos electrónicos falsos
- Mensajes engañosos
- Sitios web falsos
- Llamadas o aplicaciones fraudulentas

¿QUÉ BUSCAN OBTENER?

INFORMACIÓN SENSIBLE

- **Datos personales** (nombre, CI, dirección, fecha de nacimiento).
- **Información financiera** (números de tarjetas, cuentas).

TÉCNICAS MÁS COMUNES

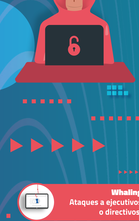
- **Correos urgentes** de "tu banco" pidiendo datos.
- **Mensajes de "premios falsos"** que requieren tu información.
- **Falsas alertas de seguridad** de redes sociales y servicios digitales para "verificar tu cuenta".
- **Ofertas laborales falsas** que piden tus datos personales.
- **Falsos técnicos** que piden acceso remoto a tu equipo.
- **Mensajes SMS engañosos** con enlaces peligrosos.

¿CÓMO DETECTAR UN INTENTO DE PHISHING?

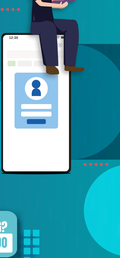
PRESTA ATENCIÓN A:

- Errores ortográficos o gramática extraña.
- Correos que generan urgencia o miedo.
- Enlaces sospechosos.
- Solicitudes de información personal por correo o mensaje.

TIPOS DE PHISHING



- **Phishing tradicional** — Correos falsos que imitan a bancos o servicios.
- **Spear phishing** — Ataques personalizados con tus datos.
- **Pharming** — Páginas web falsas con URL engañosa.
- **Vishing** — Llamadas telefónicas con engaños.
- **Smishing** — Mensajes de texto con enlaces falsos.
- **Whaling** — Ataques a ejecutivos o directivos.
- **Clone phishing** — Correos legítimos clonados con enlaces maliciosos.
- **QRishing** — Códigos QR falsos que redirigen a páginas fraudulentas.
- **Phishing por apps** — Aplicaciones móviles falsas.



¿CAISTE EN UN ATAQUE DE PHISHING? ACTÚA RÁPIDO

1. **Cambia tus contraseñas inmediatamente.**
   - Usa contraseñas fuertes y únicas.
   - Activa la autenticación de dos factores (2FA).
2. **Informa a tu banco o plataforma digital suplantada**
   - Bloquea cuentas o tarjetas si es necesario.
   - Revisa tus movimientos financieros.
3. **Reporta el incidente a las autoridades**
   - Guarda evidencia (correo, mensajes, enlaces).

TU MEJOR DEFENSA ES LA PREVENCIÓN

- Nunca proporciones tus datos personales y sensibles.
- Desconfía de lo urgente.
- Verifica la fuente.
- No hagas clic en enlaces sospechosos.

CUIDAR TU CELULAR TAMBIÉN ES CUIDAR TU INFORMACIÓN, AL IGUAL QUE TU CONTRASEÑA. NO CONFÍES EN NADIE,
LA SEGURIDAD DIGITAL DEPENDE DE TI

BOLIVIA
AGETIC
BOLIVIA