Phishing

Cómo reconocer los engaños para robar tus datos y qué hacer si caíste.

¿Qué es el phishing?

Es una técnica de **ingeniería social** que usan los ciberdelincuentes para engañarte y conseguir información sensible, como contraseñas, datos bancarios o códigos de verificación.

Se basa en la manipulación: genera urgencia, miedo o apuro para que actúes rápido, sin pensar, y no detectes el fraude.

Hoy el phishing es más sofisticado: usa inteligencia artificial, suplantaciones muy realistas (correos, mensajes o llamadas) y ataques dirigidos, lo que hace más difícil distinguir lo legítimo de lo falso.

Los canales más usados

El correo ya no es el único medio. En 2026, los canales más frecuentes son:

Smishing	Estafas por SMS, WhatsApp, Telegram o redes sociales, con enlaces que simulan venir de bancos, empresas de envíos u otras marcas conocidas.
Vishing	Llamadas en las que se hacen pasar por soporte técnico, bancos u organismos oficiales para obtener datos o códigos de verificación.
Quishing	Códigos QR falsos que llevan a sitios fraudulentos. Aparecen en carteles, correos o lugares públicos, donde se escanean sin verificar.
Phishing con IA	Mensajes, voces o incluso videos (deepfakes) muy realistas, que hacen el engaño más creíble y personalizado.

Cómo verificar un sitio antes de ingresar datos

- **Mirá la dirección:** tiene que empezar con **https://** y no solo con http://. Eso indica que la conexión está cifrada.
- **Buscá el candado:** junto a la dirección tiene que aparecer el ícono del candado. Si hacés clic, podés ver el certificado de seguridad del sitio.
- **Revisá el dominio letra por letra:** por ejemplo, bancociudad.com.ar y no bancociuudad.com. Los atacantes usan errores mínimos para engañar.
- **Ojo: el candado no alcanza.** HTTPS protege la conexión, pero un sitio falso también puede tenerlo. Siempre verificá el dominio.
- **Evitá los enlaces sospechosos:** si un mensaje te apura o te presiona, no hagas clic; escribí vos la dirección del sitio oficial.

Consejos de prevención

- **No te dejes llevar por la urgencia:** frases como “tu cuenta será bloqueada” son una señal de alerta. Los bancos y las empresas nunca piden claves, códigos ni datos personales por correo, mensaje o llamada.
- **Activá el doble factor de autenticación (2FA)** en todas tus cuentas: aunque alguien consiga tu contraseña, esa capa extra puede frenar el acceso.
- **Usá el teclado virtual** en sitios bancarios cuando esté disponible: reduce el riesgo de programas que registran lo que escribís (keyloggers).
- **Ingresá a los sitios escribiendo la dirección** en lugar de hacer clic en enlaces de correos, mensajes o redes.
- **Verificá siempre quién te escribe** antes de responder o compartir datos.
- **Mantené actualizados** el sistema operativo, el navegador y las apps.
- **No compartas códigos de verificación:** ninguna entidad legítima te va a pedir los códigos que recibís por SMS, correo o apps de autenticación.

¿Qué hacer si fuiste víctima?

Cambiá tus contraseñas	De inmediato, desde un dispositivo seguro, con claves fuertes y distintas para cada cuenta.
Activá o revisá el 2FA	Si no lo tenías, activalo. Si ya lo usabas, verificá que no lo hayan modificado.
Llamá a tu banco	Avisá a tu banco o a los emisores de tus tarjetas para bloquear cuentas, desconocer operaciones y recibir ayuda.
Cortá el contacto	No respondas ni sigas interactuando con el mensaje o con quien te contactó.
Analizá tu dispositivo	Escanealo con un antivirus actualizado para detectar y eliminar programas maliciosos.
Revisá tu actividad	Controlá accesos, movimientos bancarios y sesiones abiertas para detectar acciones no autorizadas.
Denunciá	Ante las autoridades, fiscalías especializadas o equipos de respuesta a incidentes.

También podés comunicarte con **BA-CSIRT**, el Centro de Ciberseguridad de la Ciudad, para recibir orientación y reportar el incidente.