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.

LA ESCALERA DE PROTECCIÓN: DE LA CONTRASEÑA A LAS PASSKEYS

Cada nivel que subís reduce drásticamente la probabilidad de que te roben una cuenta. Identificá en qué escalón estás hoy.

>> SUBÍ DE NIVEL

NIVEL 0 — ZONA DE RIESGO

Contraseña débil o reutilizada

Formada por datos personales, fácil de adivinar, o la misma en varios servicios: si comprometen una, caen todas.

NIVEL 1

Contraseña fuerte

Mayúsculas, minúsculas, números y caracteres especiales. Usá una regla mnemotécnica: por ejemplo, las primeras letras de una frase.

NIVEL 2

Única por servicio + gestor de contraseñas

Una contraseña distinta en cada sistema. Con muchas cuentas, un gestor de contraseñas las recuerda por vos.

NIVEL 3

Autenticación multifactor (MFA)

Un segundo factor además de la contraseña: aunque la roben, no alcanza para entrar.

NIVEL 4 — OBJETIVO

Passkeys

Acceso sin contraseña, ligado a tu dispositivo: no hay nada que robar ni que adivinar mediante phishing.

>> REGLAS QUE APLICAN EN TODOS LOS NIVELES

→ No compartas tus contraseñas

Si por urgencia tuviste que darla, cambiala inmediatamente después.

→ Preguntas de seguridad difíciles

Si cualquiera puede responderlas con datos públicos tuyos, son una puerta de entrada.

→ No las anotes en papeles ni archivos

Ni libretas, ni notas del celular. Si no queda otra, guardá el papel en un lugar muy seguro.

→ Cambio urgente ante actividad extraña

Si detectás movimientos raros en una cuenta, cambiá la contraseña de inmediato. Y renovalas de tanto en tanto sin esperar a que el sistema te obligue.

ATENCIÓN

Cuidá que nadie te observe al escribir tu contraseña: las miradas también roban claves.

GUÍA DE SEGURIDAD DE UN HACKER // INFOGRAFÍA 03/08

TU CELULAR ES TU VIDA: 10 PROTECCIONES ESENCIALES

Fotos, cuentas, banco, mensajes: todo vive en tu teléfono. Estas diez medidas cubren robo, pérdida, apps maliciosas y estafas.

01 Bloqueo con código + autobloqueo

Que solo pueda usarse con tu código o contraseña, y se bloquee solo al dejar de usarlo.

02 Cifrado de datos

Habilitá la encriptación de los datos internos y de las memorias externas.

03 PIN en la tarjeta SIM

Sin PIN, tu línea puede usarse en otro equipo para recibir tus códigos de verificación.

04 Rastreo y borrado remoto

Software que permita ubicar el equipo y, si hace falta, bloquearlo y borrar los datos a distancia.

05 Apps solo de tiendas oficiales

Pasaron verificación de la empresa y de la comunidad. Fuera de ahí, territorio de malware.

06 Opiniones, descargas y permisos

Revisá reseñas y cantidad de descargas antes de instalar. Si los permisos son excesivos, no sigas: consultá con alguien con experiencia.

07 Actualizaciones al día

Sistema operativo y aplicaciones actualizados cierran vulnerabilidades conocidas.

08 Carga segura

No cargues en cualquier lado. En USB públicos usá protección y modo solo carga, sin sincronizar datos.

09 Pantalla discreta

Filtro de privacidad contra miradas indiscretas y notificaciones limitadas con el equipo bloqueado.

10 Copias de seguridad + limpieza

Backup regular. El contenido sensible pasalo a la computadora y eliminálo del teléfono.

>> BONUS: ESTAFAS POR MENSAJE DE TEXTO

! **Smishing**

Los mismos engaños del phishing llegan por SMS y mensajería: premios, "problemas con tu cuenta", encomiendas. Aplicá el mismo protocolo: dudar, no hacer clic, verificar por canal oficial.

SI LO PERDÉS O TE LO ROBAN

Con los puntos 1–4 activados, tu información queda protegida aun sin el equipo en tu poder.

HOGAR DIGITAL SEGURO: WIFI, IOT Y COMPUTADORAS

Las amenazas también llegan a tu casa de forma remota, por internet y redes inalámbricas. Cuatro zonas a proteger.

ZONA 1 El router wifi

Es la puerta de entrada a tu casa digital. Configuralo de forma segura eligiendo las opciones convenientes; si no sabés cómo, consultá a un técnico. Una red sin protección le permite a un intruso acceder a tus dispositivos y datos.

ZONA 2 Dispositivos IoT

Cámaras, parlantes, enchufes y electrodomésticos inteligentes pueden ser un canal de acceso a tu red. Elegilos e instalalos con precaución, cambiá claves por defecto y mantenelos actualizados.

ZONA 3 Las computadoras

Mantenimiento preventivo: evitá infecciones de malware y funcionamiento incorrecto. Antivirus activo, sistema actualizado, descargas solo de fuentes seguras.

ZONA 4 Tu información

Copias de seguridad regulares: definí qué archivos resguardar, dónde y cada cuánto. La nube sola no alcanza.

>> EL PLAN DE BACKUP EN 3 PREGUNTAS

¿Q?

¿Qué?

La información que no podés permitirte perder: documentos, fotos familiares, archivos de trabajo.

¿D?

¿Dónde?

Siempre en más de un lugar, esté o no en la nube. Si la nube falla o perdés el acceso, la copia local te salva.

¿C?

¿Cada cuánto?

Con una frecuencia definida y regular, según cuánto cambia tu información. No "cuando me acuerde".

REGLA DE LOS DOS LUGARES

Lo importante vive siempre en dos lugares como mínimo. Todo lo demás es opcional; esto no.

ROBO DE IDENTIDAD Y PROTECCIÓN DEL DINERO

Es uno de los delitos de mayor crecimiento en el mundo: roban tus datos personales para cometer fraudes en tu nombre. Recuperarse es muy difícil; prevenir es la jugada.

>> QUÉ BUSCAN LOS ATACANTES

- DOCUMENTO DE IDENTIDAD
- TARJETAS DE CRÉDITO Y DÉBITO
- RECIBOS Y BOLETAS DE SERVICIOS
- TUS DATOS DIGITALES

>> LÍNEA DE DEFENSA: PREVENIR → DETECTAR → REACCIONAR

1

PREVENIR — Cautela con tu información privada

Evitá que tus datos y documentación personal caigan en manos de terceros. No publiques datos identificatorios, destruí papeles con información sensible antes de tirarlos y entregá tu documento solo cuando sea imprescindible.

▼

2

DETECTAR — Monitoreá cuentas y tarjetas

Revisá movimientos y resúmenes con regularidad. Cargos desconocidos, por pequeños que sean, son la primera señal: los atacantes prueban con montos chicos antes del golpe grande. Activá alertas de consumo si tu banco las ofrece.

▼

3

REACCIONAR — Rápido y con ayuda profesional

Si descubrís que sos víctima: consultá urgentemente a un especialista y tomá medidas de inmediato para evitar que el problema crezca. Avisá al banco, bloqueá tarjetas, cambiá contraseñas de cuentas vinculadas.

>> PROTEGÉ EL DINERO EN EL DÍA A DÍA

→ Compras online solo en sitios confiables

Verificá la dirección exacta del comercio antes de ingresar la tarjeta.

→ Nunca des datos bancarios por mensaje o teléfono

Tu banco no te pide claves, tokens ni códigos por estos canales.

→ No pierdas de vista tus tarjetas

En comercios y restaurantes, que el plástico no desaparezca de tu campo visual.

→ Cuidá los papeles tanto como lo digital

Recibos, boletas y resúmenes contienen datos que sirven para suplantarte.

POR QUÉ IMPORTA

De un robo de identidad es muy complicado recuperarse: pueden endeudarte y cometer delitos en tu nombre.

MENORES SEGUROS EN INTERNET: GUÍA PARA PADRES Y EDUCADORES

La meta no es prohibir la tecnología sino acompañar: los menores pueden saber más de tecnología que un adulto, pero no de sus riesgos.

>> LOS 3 RIESGOS QUE HAY QUE CONOCER

CIBERBULLYING

Acoso entre pares por medios digitales. Pediles que **informen cualquier acoso** o pedido que les resulte extraño o desagradable.

GROOMING

Adultos que se hacen pasar por menores para ganar su confianza. Verificá sus contactos; que **no se comuniquen con extraños** ni usen sus nombres reales en chats de juegos.

SEXTING

Circulación de material íntimo. La regla tiene tres partes: **no producirlo, no compartirlo y no pedirlo**.

>> QUÉ HACER / QUÉ EVITAR

[+] HACER

- » **Control parental y límites de uso**, en especial con niños pequeños
- » **Dispositivos en áreas comunes de la casa**, no en los dormitorios
- » **Diálogo abierto** en familia y escuela sobre lo que ven y viven online
- » **Enseñar los riesgos** como parte de su educación
- » **Dar el ejemplo**: tus acciones en redes deben ser consistentes con lo que les transmitís

[−] EVITAR

- × **Negarles el acceso a internet:** es clave para su aprendizaje y futuro
- × **Que compartan datos identificatorios:** dirección, teléfono, colegio
- × **Operaciones monetarias** online antes de tener edad y criterio para hacerlas sin riesgo
- × **Suponer que "saben más que vos":** dominan la herramienta, no el peligro
- × **Vigilar sin conversar:** el control sin diálogo los empuja al secreto

>> POR EDADES

−10 **Niños pequeños**

Control parental activo, acompañamiento directo, contenidos filtrados, tiempo limitado.

10+ **Adolescentes**

Autonomía guiada: menos filtro, más conversación. Que sepan que pueden contarte cualquier cosa **sin castigo por hablar**.

PARA TRANSMITIRLES

Cuidá tu presente: en el futuro será tu pasado, y si está en internet, cualquiera podrá revisarlo.

¿TE HACKEARON? PROTOCOLO DE RESPUESTA

Robo de cuenta, fraude, suplantación: lo que hagas en las primeras horas define cuánto daño sufrís. Seguí este orden.

1 **NO borres nada — preservá la evidencia**

No elimines ni reenvíes correos, mensajes ni información del incidente. Guardá todo lo que pueda servir como prueba: capturas, e-mails, conversaciones.

▼

2 **Denunciá lo antes posible**

En la dependencia policial o fiscalía más cercana a tu domicilio. La denuncia formal habilita la investigación y te protege si cometen delitos en tu nombre.

▼

3 **Cortá el acceso del atacante**

Cambiá urgente las contraseñas comprometidas y las de cuentas vinculadas (sobre todo el e-mail principal: desde ahí se resetea todo lo demás). Cerrá sesiones abiertas en todos los dispositivos.

▼

4 **Contactá al proveedor por los canales oficiales**

Formulario, soporte o teléfono del servicio. Te pedirán datos para verificar que sos el dueño: fecha estimada de creación, contactos frecuentes, contenido de últimos correos, carpetas y etiquetas. En servicios gratuitos la respuesta puede demorar: insistí.

>> QUÉ NO HACER

[−] ERRORES QUE EMPEORAN TODO

- × Contratar un "hacker" para recuperar la cuenta: es ilegal si no se hace por los medios del proveedor, y suele ser otra estafa
- × Reenviar o difundir el contenido del incidente
- × Esperar que la ley resuelva sola: el rol activo en la protección es tuyo

>> PREVENIR HOY PARA RECUPERAR MAÑANA

ACTIVÁ MFA | CARGÁ DATOS DE RECUPERACIÓN | SEGUNDO ADMINISTRADOR DEL PERFIL | BACKUP DEL PERFIL (DESCARGÁ TUS DATOS)

REGLA

Evidencia primero, denuncia rápido, contraseñas nuevas ya. En ese orden y sin demora.

FUERA DE CASA: WIFI PÚBLICO, CONEXIONES Y VIAJES

Cafés, aeropuertos y hoteles son territorio compartido: redes que no controlás y equipos expuestos. Conductas correctas para cada escenario.

>> TRES ESCENARIOS, UNA REGLA

CAFÉ / SHOPPING

- × Nada de home banking ni compras en wifi ajena si no confiás en la red o el proveedor
- » Ante la duda, usá tus datos móviles
- » No dejes el equipo solo ni un minuto

AEROPUERTO

- × USB públicos de carga: pueden sincronizar datos
- » Cargador propio a la corriente, o modo solo carga con protección
- » Verificá el nombre exacto de la red oficial antes de conectarte

HOTEL

- × No dejes dispositivos a la vista en la habitación
- » Caja de seguridad para lo que no llevás con vos
- » Sesiones cerradas y equipo bloqueado siempre

>> ANTES DE VIAJAR: CHECKLIST DEL EQUIPO

1. **Backup completo**
   Si el equipo se pierde o lo roban, tu información sigue existiendo.

2. **Cifrado de disco activado**
   Medida de seguridad avanzada: sin tu clave, el contenido del equipo es ilegible.

3. **Localización de equipos encendida**
   Rastreo, bloqueo y borrado remoto disponibles desde otro dispositivo.

4. **Viajá liviano de datos**
   Llevá en el dispositivo solo lo necesario: lo que no está, no se puede robar.

>> EN TODO LUGAR PÚBLICO

→ Miradas indiscretas

Filtro de privacidad en pantalla y cuidado al tipear contraseñas rodeado de gente: no seas obvio al ingresarla.

→ Resguardo físico

El robo del aparato sigue siendo el ataque más común. Encima tuyo o bajo llave, sin excepciones.

REGLA DEL TERRITORIO COMPARTIDO

En redes que no controlás, comportate como si alguien estuviera mirando. A veces es cierto.