Ciberataques

Qué son, quiénes los hacen y cómo protegerte.

Cada vez hacemos más cosas por Internet: trabajamos, estudiamos, hacemos trámites, compramos y nos comunicamos. Eso también abre oportunidades para los ciberdelincuentes, que buscan obtener información, dinero o acceso a cuentas y dispositivos.

¿Qué es un ciberataque?

Es una acción realizada con herramientas digitales para comprometer la seguridad de una persona, empresa u organización.

Las consecuencias pueden ser muy distintas: robo de datos personales o contraseñas, interrupción de servicios, instalación de software malicioso o fraudes. Muchas veces no buscan destruir sistemas, sino aprovechar una oportunidad para obtener un beneficio.

¿Quiénes están detrás?

Personas o grupos con distintos objetivos. Algunos buscan ganar dinero con estafas, robo de información o extorsiones. Otros atacan de forma coordinada a organizaciones, y hay grupos que los usan para difundir mensajes políticos, sociales o ideológicos.

Aunque las motivaciones cambien, la mayoría aprovecha lo mismo: **errores humanos, contraseñas débiles o sistemas sin actualizar.**

¿Cómo llegan a las víctimas?

A diferencia de lo que muestra el cine, muchos ataques no requieren técnicas complejas. Suelen usar métodos simples para engañar o aprovechar fallas conocidas:

Phishing	Correos, mensajes o sitios falsos que parecen legítimos para robar contraseñas, datos bancarios o códigos de verificación.
Malware	Software malicioso que roba información, espía la actividad o permite accesos no autorizados. Incluye el ransomware, que bloquea o cifra archivos y pide un pago para recuperarlos.
Contraseñas comprometidas	Claves débiles, repetidas en varios servicios o expuestas en filtraciones que facilitan el acceso a cuentas personales y laborales.
Vulnerabilidades	Fallas de seguridad en sistemas operativos, aplicaciones o dispositivos que no se actualizaron.
Ingeniería social	Técnicas de manipulación que generan confianza, urgencia o miedo para que la víctima haga algo que compromete su seguridad.

¿Cómo reducir los riesgos?

No existe la protección absoluta, pero algunos hábitos reducen mucho las posibilidades de sufrir un incidente:

- Mantené actualizados tus dispositivos y aplicaciones.
- Usá contraseñas únicas y seguras para cada servicio.
- Activá el segundo factor de autenticación (MFA) siempre que puedas.
- Desconfiá de mensajes inesperados que piden datos personales o te apuran para actuar.
- Revisá bien los sitios web antes de ingresar contraseñas o datos bancarios.
- Hacé copias de seguridad periódicas de tu información importante.

¿Qué hacer si fuiste víctima?

Cambiá las contraseñas de las cuentas afectadas, cerrá las sesiones abiertas en otros dispositivos y guardá las evidencias. Actuar rápido ayuda a reducir el impacto.

La prevención sigue siendo una de las herramientas más efectivas para proteger tu información. Desde **BA-CSIRT** te acompañamos para que te muevas con más seguridad en el entorno digital.