Malware

Cómo funcionan las amenazas digitales y cómo protegerte.

¿Qué es el malware?

Es software malicioso creado para dañar dispositivos, robar información o entrar a sistemas sin autorización. Puede afectar computadoras, celulares, tablets y otros equipos conectados a Internet.

Muchas veces, los ciberdelincuentes aprovechan errores cotidianos: abrir un archivo sospechoso, descargar programas de sitios no confiables o ingresar datos en páginas falsas.

Tipos más comunes

Virus	Infectan archivos o aplicaciones y se replican dentro del sistema. En general necesitan que la persona ejecute un archivo o haga algo para propagarse.
Troyanos	Se hacen pasar por programas legítimos o inofensivos, pero permiten que un atacante acceda al dispositivo o robe información.
Ransomware	Bloquea o cifra los archivos y exige un pago para recuperarlos.
Spyware	Software espía que recopila información del dispositivo o de tu actividad sin tu consentimiento.
Adware	Muestra publicidad invasiva o redirige la navegación hacia sitios sospechosos.
Gusanos (worms)	Se propagan solos entre dispositivos y redes, sin que nadie tenga que hacer nada.

¿Qué daños puede causar?

- Robo de contraseñas o información personal.
- Acceso no autorizado a cuentas o dispositivos.
- Pérdida o cifrado de archivos.
- Uso de tu equipo para enviar spam o lanzar ataques.
- Un dispositivo más lento.
- Ventanas emergentes, anuncios o comportamientos extraños.

A veces, la infección pasa desapercibida durante un tiempo.

Cómo proteger tus dispositivos

- **Mantené todo actualizado:** las actualizaciones del sistema y de las apps corrigen fallas que los atacantes aprovechan.
- **Usá herramientas de protección:** un antivirus o solución antimalware ayuda a detectar amenazas y bloquear comportamientos sospechosos.

- **Descargá solo de sitios oficiales:** instalá programas y apps desde tiendas oficiales o páginas confiables.
- **Desconfiá de mensajes inesperados:** no abras enlaces ni adjuntos sospechosos, aunque parezcan venir de alguien conocido.
- **Revisá los permisos:** antes de instalar una app, fijate a qué información y funciones pide acceso.
- **Hacé copias de seguridad:** un backup actualizado te permite recuperar tu información ante un ransomware o una falla.
- **Usá contraseñas seguras:** claves únicas para cada servicio y autenticación multifactor.

Cualquier dispositivo conectado puede ser blanco de una amenaza. La prevención, la actualización constante y el uso responsable de la tecnología son las mejores herramientas para navegar más seguro. Desde **BA-CSIRT** te acompañamos.