Buenas prácticas para prevenir los virus

Instalar y actualizar el antivirus

Este tipo de programa protege contra virus, spyware[1], troyano[2], phishing[3], y ataques de spam[4].

Desconfiar de archivos y enlaces contenidos en mensajes

Atención sobre mensajes por redes sociales y por email. Preferentemente desactivar la recepción de email con texto enriquecido (HTML) de forma predeterminada hasta confirmar que se puede confiar en el remitente.

Actualizar el software de la compu y del celular

- Sistema operativo: Microsoft Windows.
- Navegadores de internet: Microsoft Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox y otros.
- Utilitarios: Microsoft Office, Adobe Acrobat Reader y otros.

Evitar descargar archivos de origen dudo

Corre electrónico que no se espera, sitios web en los que no se confía, sitios web no seguros, plataformas de uso compartido para piratear música o películas.

Prestar atención cuando se instalan programas

Rechazar o cancelar solicitudes para instalar programas no justificados. Igual criterio para el acceso a información personal.

Colocar cortafuego (firewall)

Su función es controlar los datos que salen y entran entre tu computadora e internet. Microsoft Windows Defender, incluido en Windows 10, incluye antivirus y cortafuego.

Intentar estar siempre informados

La información es clave para conocer riesgos y prevenir sorpresas (virus o amenazas que circulan entre los usuarios). Ante la duda, consultar a seguridad.informacion@conicet.gov.ar.

Evitar el uso de memorias externas cuya procedencia se desconoce

El uso de pendrive, discos rígidos externos o memorias extraíbles es realmente riesgoso.

Usar cuentas de usuarios separadas

---

[1] Spyware: dispositivos o software que capturan los datos o el comportamiento de un usuario sin obtener el consentimiento [ISO 20252:2019].
[2] Troyano: programa malicioso que se hace pasar por una aplicación benigna [ISO/IEC 27039:2015].
[3] Phishing: estafa mediante la cual se engaña a un usuario de correo electrónico para que revele información personal o confidencial que el estafador puede usar de manera ilícita [ISO/IEC 29115:2013].
[4] SPAM: correos electrónicos no solicitados, que pueden llevar contenido malicioso y/o mensajes fraudulentos [ISO/IEC 27033-1:2015].

Usar una cuenta para el trabajo normal de la computadora. Y, otra, para tareas de administración como instalar, configurar, cambiar preferencias, o actualizar programas.

Hacer copias de seguridad

Verificar que los archivos originales están libres de virus antes de hacer la copia. Luego, realizar la copia y guardar esta en una ubicación diferente al equipo donde están los archivos originales. Esta práctica previene la pérdida de archivos no sólo por virus.