6 hábitos básicos para tu seguridad digital.

Por: Paul Aguilar. PROTEGE.LA. 27/11/2020

Image not found or type unknown

Image not found or type unknown

Image not found or type unknown

¿Cómo cuidar tu información y cuentas en línea?

Para reforzar tu seguridad digital, te compartimos 6 cuidados digitales que puedes comenzar hoy

1. Respaldos

Los respaldos permiten contar con copias actualizadas de nuestra información, en caso de robo, daño o extravío de dispositivos (como computadora y celulares). Para hacer respaldos:

- Haz copias actualizadas de tu información y archivos cotidianos en la nube
- La Información y archivos históricos, de preferencia hazlos en discos externos o en USB.
- Respalda de manera cifrada información sensible, para esto puedes utilizar herramientas como Cryptomator que crean una “caja de seguridad” para guardar archivos o carpetas. (aquí te dejamos cómo descargarlo y una guía)

2. Antivirus

Las infecciones a través de programas maliciosos, pueden suceder por dar clic en algún enlace, descargar o abrir un programa o archivo infectado, o conectar una

USB infectada a tus equipos.

Para estos casos, la primera barrera es tener un antivirus instalado, si no tienes alguno, puedes conseguir uno gratuito o de paga. No olvides configurarlo para que se actualice y realizar escaneos de manera periódica.

Recuerda también que los virus no solo infectan computadoras, también celulares.

3. Contraseñas

Las contraseñas son las llaves de acceso a nuestro espacio digital, ya sea para el celular, computadora y nuestras cuentas en línea. Para proteger tu información y equipos:

- Bloquea el acceso de tu computadora, tablet y celular
- Utiliza contraseñas únicas y privadas para tus cuentas
- Utiliza frases o más d3_10_C4R4CT3R3$
- Si la memoria falla, usa un gestor de contraseñas como KeePass. (Te recomendamos leer ¿Qué es un gestor de contraseñas y para qué sirve?)
    - Para equipos de computo puedes utilizar KeePassXC.
    - Para Android puedes utilizar Android2KeePass.
    - Para iOS puedes utilizar miniKeePass
- Activa la verificación de 2 pasos y guarda los códigos de recuperación en un lugar seguro, como tu gestor de contraseñas.

Otros recurso:
– ¡Es momento de elegir contraseñas nuevas y seguras!

4. Actualizaciones

Las actualizaciones permiten arreglar los problemas de seguridad que existen en programas, apps y los sistemas operativos de computadoras y celulares. Mantén al día las actualizaciones en todos tus dispositivos y procura no posponerlas.

5. No te dejes engañar

Los engaños digitales están a la orden del día y se basan en suplantar una identidad con tal de obtener información para otros fines maliciosos. Esta técnica que busca engañarte se conoce como *phishing*. El *phishing* busca que des clic a algún enlace

malicioso, abras algún archivo infectado, o compartas información privada, personal o financiera. Para esto:

- Evita dar clic a correos o mensajes que te pidan:
  - información personal y contraseñas
  - descargar archivos y enlaces sospechosos
- Verifica la fuente del correo, página o enlace
- Si sospechas de su procedencia y contenido, ignóralo.

Otros recursos:
– Sobre phishing y otros engaños digitales
– Tipos de phishing, cómo identificarlos y protegerte

6. Comunicaciones cifradas

Para que tus comunicaciones en línea viajen de forma segura, añade una capa de protección extra con herramientas que cuenten con cifrado de punta a punta. Esto aplica en:

- Chats
- Correos y envío de archivos
- Llamadas y video-llamadas
- Y en sitios y páginas webs que cuenten con HTTPS en la dirección o URL

El cifrado de punta a punta significa que solo tú y la persona con la que te estás comunicando pueden acceder a tus mensajes o archivos, lo que garantiza que nadie de por medio (ni el proveedor de servicios) accedan.

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: Netec.

Fecha de creación
2020/11/27