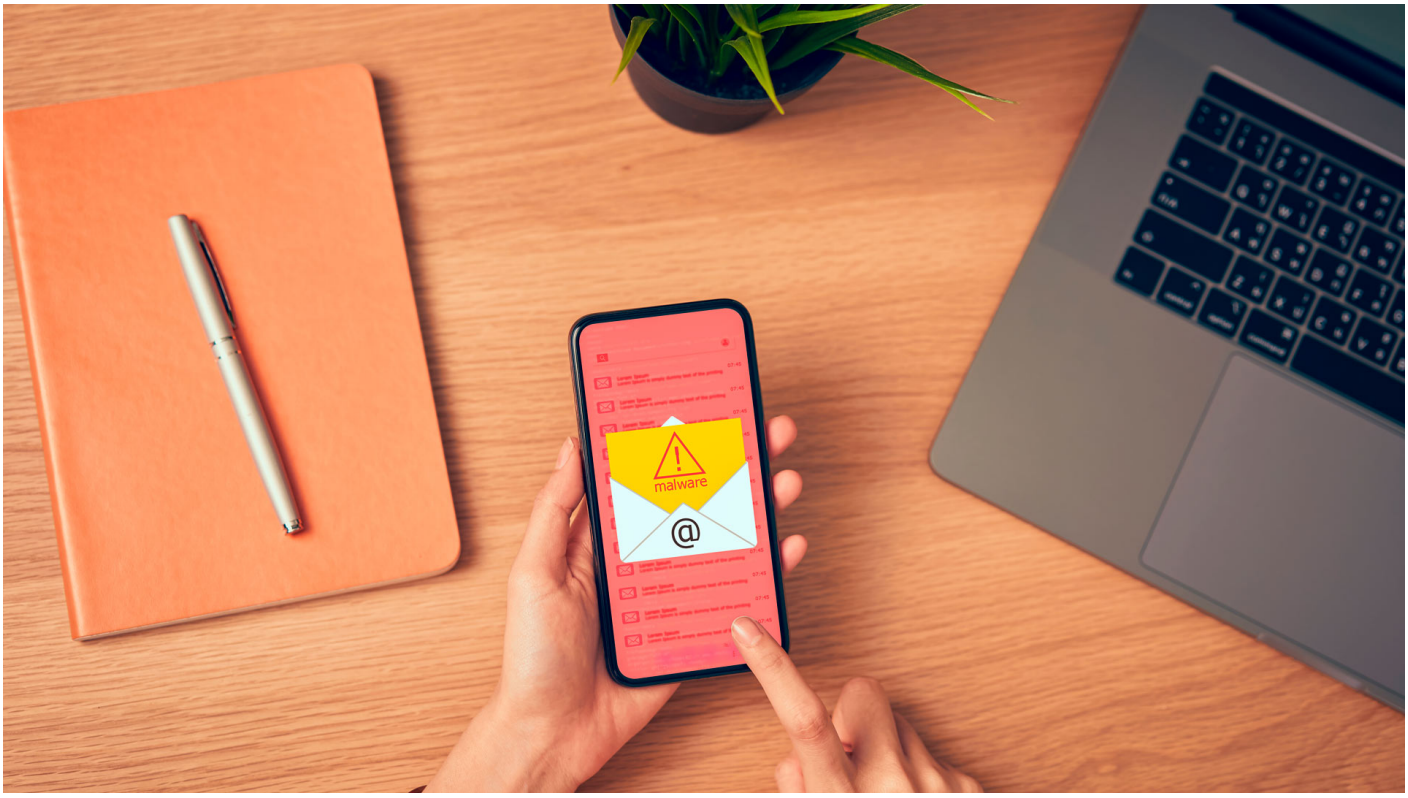
¡Protege tus datos! 10 consejos de ciberseguridad para evitar ataques



¿Qué puedo hacer para **mejorar mi ciberseguridad**? ¿Cómo evito poner en riesgo la información que tengo en mis **cuentas de correo** y **redes sociales**?

Grecia Renovato, especialista en Seguridad de la Información en el Tec de Monterrey, explica que debido a que muchas **actividades se trasladaron a un entorno digital,** los ciberataques se han vuelto más comunes.

*"A raíz de la pandemia **hubo un crecimiento del 200% en ataques cibernéticos**, dado que tanto empresas como instituciones educativas nos fuimos a la modalidad en línea. No fue algo que nos dieran a elegir, sino que la situación nos llevó a eso.*

*"México es el tercer lugar del mundo en **estafas cibernéticas**. Las víctimas no son necesariamente empresarios, también es gente común; probablemente **4 de 10 usuarios son atacados**, pero que se cumpla el cometido, tal vez sean **2 de 10**"*, comentó Grecia.

En el marco del **mes de la concientización sobre ciberseguridad**, la especialista compartió para **CONECTA** 10 consejos que te pueden servir para **evitar ser víctima de los ciberdelincuentes**:


width="900" loading="lazy">

1. Usa contraseñas largas y cámbialas cada 3 meses

Aunque los servicios electrónicos y redes sociales suelen aceptar contraseñas desde 6 caracteres, Renovato sugiere **utilizar passwords de una longitud de al menos 10 caracteres** y que combine letras mayúsculas y minúsculas, números y caracteres especiales.

*“Podemos **utilizar una frase cómo contraseña** (nunca información personal como nombres o fechas), pero sí es importante que tenga un **mínimo de 10 caracteres**.*

“Un ciberatacante, a través de un software, puede descifrar contraseñas cortas hasta en 30 segundos. Entonces, en cuanto más larga sea una contraseña es mejor”, sugirió.

Asimismo, Grecia recomendó **cambiar las contraseñas al menos cada 3 meses**.

2. Evita guardar contraseñas en el navegador

Hoy, con la intención de hacer más amigable la tecnología para los usuarios, algunos **navegadores ofrecen la posibilidad de recordar la contraseña** y las llaves de acceso a los diferentes servicios.

Grecia comentó que **es una práctica que se debería evitar** en lo posible, debido a que los navegadores pueden ser el objetivo de los cibercriminales para hacerse de tus cuentas.

*“**Guardar las contraseñas en el navegador es lo más inseguro,** porque en el momento en el que se infiltren en tu computadora, lo primero que **se llevan son tus cookies** de navegación, y a través de ellas pueden obtener todas tus contraseñas”,* alertó.


width="900" loading="lazy">

3. No te compliques, utiliza un gestor de contraseñas

Renovato platica que uno de los errores más comunes que cometemos los usuarios es **utilizar la misma contraseña para acceder a diferentes servicios y aplicaciones**.

Ante lo difícil que puede representar para los usuarios el **recordar un password** para cada servicio, la especialista recomienda **utilizar un gestor de contraseñas**.

*“Es un programa en el que puedo **guardar diferentes passwords teniendo una contraseña maestra**. Si yo quiero utilizar una de mis contraseñas solamente abro mi gestor, pongo mi contraseña maestra y ya me arroja las demás.*

*“Gratuitamente, el que sugiero uttilizar el **Keepass** porque es fácil de instalar y de usar; además **no ha caído en brechas de exposición de información**”,* añadió.

4. Implementa un doble factor de autenticación

La especialista dice que si quieres robustecer tu seguridad, además de una contraseña larga y compleja, lo ideal es **implementar un doble factor de autenticación** en tus redes sociales, servicios bancarios y servicios como **WhatsApp**.

Se trata de un sistema que **verificación en dos pasos** que ofrecen muchos servicios digitales hoy en día, como medida de seguridad extra.

*“La mayoría de los servicios ya tienen este segundo factor de autenticación, que puede ser un número que va cambiando constantemente, como **un código de 6 dígitos que se va modificando,** tanto para redes sociales como para correos electrónicos.*

*“Por ejemplo, institucionalmente (en el Tec) lo tenemos precisamente como **una llave digital**. Es una doble validación porque mi contraseña es algo que yo sé, se le agrega un segundo código que yo veo o que tengo físicamente y **que un tercero no lo puede tener**”,* explicó.

width="900" loading="lazy">

5. Cuida tu privacidad, también en LinkedIn

Aunque en redes sociales como **Facebook**, **Instagram** o **Twitter** es más común que los usuarios no publiquen datos personales como teléfono o dirección, hay otras como **LinkedIn**, donde suben solicitudes de empleo, algunas veces con **información sensible**.

“Hay información personal que uno como usuario debe decidir a quién, cómo y dónde se debe compartir; hay que cuidar ***qué cosas deben ser públicas o privadas****; incluso, datos como la edad o la fecha de cumpleaños.*

“Es común, por ejemplo, que gente ***pone su currículum con todo y teléfono*** *en* ***LinkedIn****. Ahí debemos ser cautelosos; evidentemente no se debe de compartir de forma abierta, a la vista de todos, porque podría ser víctima de un* ***robo de identidad digital o de extorsión****”,* añadió.

6. Mantente escéptico, en la red no todos son quienes dicen

Renovato dijo que es recomendable que los usuarios se mantengan alerta, y es preferible **desconfiar del destinatario o emisor de la información**, pues es común que los ciberdelincuentes utilicen **identidades falsas** para engañar a sus víctimas.

“Hay que ser un poco escépticos, sobre qué información se comparte, con qué finalidad y a quién se comparte.

“Por ejemplo, en los correos que recibes hay que ***verificar la entidad de quién está emitiendo la información****. Identificar realmente al emisor y más si es un correo o* ***información que no estás esperando****”,* añadió.

Asimismo, recomienda **evitar seguir links desde correos,** ya que pueden llevar a webs falsas, inseguras o descargar software malicioso, y aunque cueste un poco más de trabajo, **escribe la URL de un sitio directamente en el navegador**.

width="900" loading="lazy">

7. Evita las redes wifi abiertas

En cuanto a la manera de cómo los usuarios llegan a Internet, la especialista dijo que hay que **evitar las redes wifi abiertas** que comúnmente se ofrecen de manera gratuita en lugares públicos, como centros comerciales, parques, aeropuertos, etcétera.

*“Hay que **llegar a Internet a través de una conexión segura**, a través de una conexión desde casa, y no confiar cuando me conecto en un cibercafé, un aeropuerto o en una plaza. Hay redes que levantan los ciberdelincuentes donde pueden ver la navegación de los usuarios.*

*“Desde el momento en que te conectas a **una red inalámbrica abierta** le estás dando **acceso a un tercero a ver tu dispositivo**. El mejor lugar para conectarte es una red que tú conoces y aún así, debes asegurarte que se llama como la conoces normalmente”,* explicó.

“Hay información personal que uno como usuario debe decidir a quién, cómo y dónde se debe compartir; hay que cuidar qué cosas deben ser públicas o privadas".

8. Usa tus datos o una VPN para navegar seguro

En caso de que no estés en condiciones de conectarte a una red segura, por ejemplo, durante un viaje, Grecia sugirió **utilizar los datos de telefonía celular** para enviar y recibir información.

*“Si estoy fuera de casa, necesito conectarme y requiero Internet de urgencia, además tienes un celular con datos móviles, una de las formas seguras es que le **compartas internet** desde tu dispositivo móvil”,* dijo la especialista.

Otra opción es a través de una conexión **VPN (Virtual Private Network)**, un servicio -preferentemente de paga o institucional- que ofrece la posibilidad de una navegación segura.

*“Es una **conexión privada**. A través del **VPN**, dónde te encuentres conectado será **como un túnel en el que tú vas a poder navegar** y todo lo que pase a través de él será de forma segura. Le cierras la puerta a quien intenta ver tu navegación”,* explicó.

9. Actualiza tus software y no uses antivirus gratuitos

Grecia recomienda mantener actualizados tus equipos, con las **últimas actualizaciones de seguridad**, ya sea computadora, *tablet* o *smartphone*.

*“Además, con un antivirus que te ayude a poder llegar a Internet de manera segura. En el caso de **antivirus gratuitos no los recomiendo** porque te mandan propaganda y puede traer malware dentro.*

*“Ahorita institucionalmente (en el Tec) promovemos en uso de **SEP Mobile** en cuanto a dispositivos móviles, y en equipos institucionales mantenemos un esquema de **Symantec Antivirus**”,* señaló.

Además, comentó que para **colaboradores y estudiantes del Tec** también está disponible la opción de tener antivirus **Symantec no administrado** en equipos de casa **y SEP Mobile** en teléfonos como un beneficio que **pueden solicitar a través de Tecservices**.

width="900" loading="lazy">

10. Respalda tu información personal en la nube

Ante el riesgo de robo de información por ciberdelincuentes para extorsionar, secuestrar o suplantar tu identidad digital, la especialista recomienda hacer **respaldos en espacios de almacenamiento seguro** en la nube.

*“La **identidad digital es quiénes somos ante internet**; hoy en día el usuario no tiene la cultura de realizar un **respaldo de información**, pero siempre es importante contar con un respaldo de estos datos personales.*

*“Recomiendo la nube porque un disco duro sufre el mismo peligro que la computadora; se puede estropear y eso nos va a llevar a un proceso de recuperación. Ahorita, nubes como **Google** o **One Drive** son **opciones seguras para respaldar** tu información”,* dijo.

LEE TAMBIÉN: