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

“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.

10 CONSEJOS QUE TE PUEDEN SERVIR PARA EVITAR SER VÍCTIMA DE LOS CIBERDELINCUENTES:

1. Usa contraseñas largas y cámbialas cada 3 meses

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

RM Telecomunicaciones Mompós recomienda 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. **RM Telecomunicaciones Mompós** les informa 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”.

3. No te compliques, utiliza un gestor de contraseñas

Es 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, **RM Telecomunicaciones Mompós** 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.

4. Implementa un doble factor de autenticación

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.RM Telecomunicaciones Mompós 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 son la mejor opción porque te mandan propaganda y puede traer malware dentro.

5. Cuida tu privacidad

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.

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

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. Asimismo, **RM Telecomunicaciones Mompós** 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.

7. Evita las redes wifi abiertas

En cuanto a la manera de cómo los usuarios llegan a Internet, 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.

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, es preferible utilizar los datos de telefonía celular para enviar y recibir información. 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.

9. Actualiza tus software y no uses antivirus gratuitos

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. **RM Telecomunicaciones Mompós r**ecomienda 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.