¡En líne@ y seguro! 3 consejos de experto Tec para navegar sin miedo

“La nueva realidad que vivimos es trabajar remotamente y no nos damos cuenta de la vulnerabilidad que tenemos en nuestros accesos electrónicos”, aseguró **Martín Moscosa**, profesor del **Tec Guadalajara**.

La **vulnerabilidad cibernética**, tanto computadoras como en dispositivos móviles, proviene principalmente del mal manejo de la **seguridad** por parte de los usuarios.

*“El hackeo viene más allá de las computadoras o los sistemas de los ‘hackers’, sino por la **debilidad o la mala configuración** que podemos tener como usuarios”*, agregó.

Es por ello, que el **profesor de Ciencias Computacionales** compartió **3 consejos claves para mejorar nuestra seguridad en línea**.

width="900" loading="lazy">

1. ***Password* a *passphrase***

“Poner una contraseña de una palabra de 6 a 8 caracteres puede ser hackeada en 6 a 8 horas o en un máximo de un día.

*“La **nueva tendencia en tecnología** es utilizar **passphrases**: poner un enunciado con espacios, mayúsculas y minúsculas”*, aseguró Moscosa.

El ingeniero recomendó pasar de una **contraseña** de palabra a una frase o enunciado más largo que sea fácil de recordar.

*“Una **canción**, un **dicho popular** o un **poema** que nos gusta es algo sencillo de recordar como humanos”,* recomendó el ingeniero.

Una frase, de 12 a 16 dígitos, como contraseña con **caracteres especiales**, letra y números **aumenta la seguridad** y evita en gran medida **ataques cibernéticos.**

*“Esto significa que si una computadora tardaba en hackear una contraseña de una palabra en 8 horas, ahora con una frase tarda 2, 4 o incluso **hasta 100 años en hacerlo**”*, puntualizó.

“El hackeo viene más allá de las computadoras o los sistemas de los ‘hackers’, sino por la debilidad o la mala configuración que podemos tener como usuarios”.

2. ***Two-factor authentication***

Una manera de evitar el ***phishing,*** un tipo de hackeo por medio de **páginas falsas** para obtener información, es configurar nuestras cuentas con una **autenticación de 2 pasos.**

*“Por medio del ‘**Two-factor authentication’** garantiza que quien acceda a la cuenta no sólo conozca la contraseña, sino que garantiza que el dueño sea quien está accediendo”*, señaló Moscosa.

Esto se logra por medio de un **segundo elemento de autenticación** que se envía al **teléfono, correo electrónico** o algún otro medio que valida que somos los **dueños de la información.**

El **código de autenticación** que se envía sólo será válido por **5 minutos**, lo que evitará que pueda ser **robado o reutilizado.**

3. YubiKeys

Una **YubiKey** es una **llave física de USB** que, por medio de la **huella digital o el toque de los dedos**, permite tener acceso a la cuenta.

“Esto elevará por mucho la seguridad que tenemos en nuestra cuenta”, destacó Moscosa.

Las YubiKeys son altamente recomendables para resguardar **información por parte de empresas**, aunque también son utilizadas por usuarios para mejorar su **seguridad y privacidad.**

width="890" loading="lazy">

¿Por qué debería de preocuparme mi seguridad cibernética?

Tener diversos elementos de seguridad, como los que se han mencionado anteriormente, aumentará nuestra **seguridad y privacidad en la red** para que **nuestra información no sea robada**.

La información que se recopila como **internautas** puede poner en riesgo no sólo la seguridad de los usuarios, sino de grandes corporaciones para las que trabajamos.

*"La manera más fácil de **entrar a grandes instituciones** no es por medio del director o CEO, sino de los **empleados e incluso de conocidos** que ni siquiera trabajan ahí"*, aseguró Moscosa.

De acuerdo al experto, a pesar de que la seguridad en la información no siempre es vista como algo primordial por los usuarios, ésta puede representar cierto **valor emocional y hasta económico.**

*"**Nuestra información es muy valiosa**, nos pueden estar quitando nuestros ahorros e incluso fotos o videos para alimentar bases de datos de inteligencia artificial sin nuestro consentimiento...*

*"De la misma manera que vemos vivir más sano, debemos de llevar también **una vida más sana en la nube** para ser más responsables de la información que manejamos"*, concluyó el profesor.


width="900" loading="lazy">

***Martín Moscosa Martínez**

Es director de **Wizeline Academy** y profesor del Tecnológico de Monterrey, campus Guadalajara.

Es egresado de Sistemas Computacionales del Tec y cuenta con Maestría en Ciencias en la Escuela de ***Management and IT*** **en St. Andrews**, Escocia. Se especializa en ambientes de

emprendimiento.

Ha participado en diversos proyectos como consultor; uno de los más significativos fue en **Moscú, Rusia**, donde colaboró en la **adquisición de una empresa gubernamental** al sector privado, lo que impactó al sector energético.

Es socio fundador de uno de los “coworkings” más grandes de la ciudad: **Epicnest**, que permite a los emprendedores incubar sus empresas, no solo a nivel local, sino también de **Francia, Alemania, España, Argentina** y más.

Actualmente es director del Capítulo Guadalajara de la comunidad de emprendimiento: ***Startup Grind,*** donde mensualmente se apoyan a más de 10 millones de emprendedores en el mundo.

Es especialista en múltiples temas de tecnología como internet, redes sociales, cómputo y sus aplicaciones, **telecomunicaciones, apps y web.**

LEE TAMBIÉN: