Ciberseguridad: Cinco claves para evitar robos en internet

El número de usuarios de internet y redes sociales continúa creciendo exponencialmente mes a mes, tal como lo muestra el informe Digital 2022, realizado We Are Social, la agencia creativa especializada en social y Hootsuite, líder mundial en gestión de redes sociales, el cual señala que el número de usuarios de internet en el mundo alcanzó los 4,950 millones de personas este año, lo que representa al 62,5% de la población mundial (7.910 millones de personas).

Y es por esto, que la seguridad y la privacidad son dos aspectos importantes para los usuarios, pues cada vez que se conectan a Internet pueden poner en riesgo su identidad y datos, por errores o malas prácticas comprometiendo su seguridad y la de sus dispositivos.

Es por ello que Pere Blay Serrano, Director del Máster en Ciberseguridad de **VIU – Universidad Internacional de Valencia**, destaca 5 claves importantes para mantener la información segura en la internet y así evitar ataques cibernéticos:

1. Configurar con quién se comparte la información

Es común en redes sociales que, por defecto, se comparta todo aquello que publicamos con cualquier navegante. Sin embargo, es importante configurar la información, para que sea compartida con personas de confianza. De igual forma, es

recomendable utilizar servicios VPN (Redes privadas virtuales), por ejemplo, para así poder cifrar nuestra conexión y mantener nuestra red Wi-Fi con una contraseña fuerte, evitando que intrusos lleguen a acceder a nuestros datos online.

2. Cifrar datos y evitar compartir información sensible

Especialmente cuando vayamos a compartir algo a través de Internet o subirlo a la nube, es importante cifrar esos archivos con alguna de las herramientas que podemos utilizar para que no sea de fácil acceso a desconocidos.

3. No compartir o abrir información que envían desconocidos

Es importante no reenviar mensajes, fotos o videos que comparten desconocidos a nuestros correos electrónicos o dispositivos móviles, ya que estos links pueden contener virus que atacan directamente nuestra información personal, dejándonos vulnerables ante cualquier amenaza.

4. Usar siempre pseudónimos para no ser identificados con facilidad

Usar contraseñas seguras y diferentes: de esta manera, en caso de que algún intruso logre averiguar nuestra identidad, no podrá acceder fácilmente a nuestras cuentas. Podemos utilizar gestores de contraseñas o incluso generar claves complejas.

También es interesante utilizar la autenticación de dos factores siempre que sea posible.

5. No aceptar sugerencias de amistad o contactos de desconocidos

Es indispensable contrastar estas solicitudes con nuestros conocidos, para evaluar si realmente ellos nos han solicitado amistad o ser parte de nuestra lista de contactos, evitando que sean perfiles falsos.

El experto de VIU recalca que los delincuentes cibernéticos buscan en su mayoría, realizar extorsiones o estafas localizando información disponible en las redes sobre nuestros familiares, trabajo o lugares que frecuentamos; esto con el principal objetivo de disfrazar e-mails dirigidos a nosotros y que parezcan que provienen de alguien conocido.

Pero destaca que la mayoría de ataques se hacen «a ciegas», a través de phishing, usando entornos similares a los de bancos, por ejemplo, para conseguir las credenciales de usuarios o con mensajes SMS de supuestas empresas de paquetería, pidiendo información o dinero para entregar un paquete y enfatiza en actualizar los dispositivos.

“Es necesario mencionar, que es importante actualizar siempre los dispositivos según lleguen las actualizaciones, instalar software únicamente de markets oficiales y usar algún antivirus para evitar estos ataques”.

Finalmente, se debe tener en cuenta que es posible saber si nuestra información ha sido vulnerada, solamente con evidencia de actividad sospechosa o a través de sitios como” HAve I been Pwned», en los que se puede comprobar si la información ha sido expuesta e incluso permite generar alertas si las credenciales se encuentran en alguna brecha.

En caso de vivir esta situación, no olvide contactarse con las entidades encargadas tan pronto detecte un movimiento extraño, para generar el bloqueo de los productos y evitar robos.