¿Tus cuentas están en peligro?

Hoy en día, las personas administran docenas de cuentas en diferentes proveedores de servicios. Hay momentos en los que te olvidas de algunos, solo para redescubrirlos más tarde.

Pero a medida que avanzan las tendencias, los usuarios pueden omitir el aspecto potencialmente más crucial: su seguridad. Las cuentas suelen ser el objetivo de los ciberdelincuentes, con la esperanza de romper los mecanismos de protección que las protegen.

Dependiendo de cuán continuamente monitoree sus cuentas, es posible que ni siquiera se dé cuenta si una de ellas es atacada o, peor aún, pirateada.

1. Vigilancia de los usuarios cuando se trata de datos personales.

Numerosas historias sobre la superficie de recuperación de datos cuestionables. El raspado es una de las técnicas que utilizan los piratas informáticos para extraer datos de varias fuentes.

También sucede en las redes sociales, cuando los piratas informáticos obtienen y categorizan información sobre sus objetivos. La verdad es que incidentes similares ocurren todos los días, y las cuentas de las personas son algo que los piratas informáticos buscan con frecuencia.

Una de las mayores preocupaciones es que es posible que los usuarios no sepan lo suficiente sobre la importancia de sus datos. Es probable que los usuarios más

atentos utilicen herramientas como redes privadas virtuales o administradores de contraseñas para fortalecer su información.

Sin embargo, es posible que los usuarios no tengan idea de que sus cuentas se han visto comprometidas. Una de las razones es que no saben qué señales indican peligro. Así, los saltan como insignificantes en lugar de profundizar en sus orígenes.

2. ¿Cuáles son los factores clave que conducen a las filtraciones de datos?

No hay uno, sino muchos factores que conducen a las filtraciones de datos. Estos se deben tanto a los usuarios como a los proveedores de servicios.

Como los datos de un usuario se pueden usar de varias maneras no amigables, se debe tener cuidado al usar la web. Aquí hay algunos aspectos clave que pueden conducir a violaciones de datos.

3. Contraseñas débiles.

Uno de los factores más comunes que conducen a violaciones de datos son las contraseñas débiles de los usuarios. No solo esto, sino que muchos de nosotros también tendemos a establecer la misma contraseña para casi todas las cuentas en línea. La reutilización de contraseñas es muy peligrosa en términos de seguridad.

Si alguna de sus cuentas fuera pirateada, sería pan comido para el hacker tener en sus manos otras cuentas. Por lo tanto, los usuarios deben concentrarse en establecer una contraseña segura.

4. Software no seguro.

Muchas personas no instalan las últimas actualizaciones para corregir vulnerabilidades en nuestro sistema. Y este es el aspecto que de alguna manera se convierte en una forma lucrativa para que los piratas informáticos se hagan con sus datos.

Existe una alta probabilidad de que ni siquiera sepa que sus datos han sido pirateados. Los atacantes pueden aprovechar las vulnerabilidades para acceder a su red, cuentas o dispositivos.

5. Conexión a redes desconocidas.

Es posible que no todas las redes a las que te conectes te pertenezcan. Gerentes desconocidos lo controlan, y su confiabilidad es cuestionable. Si eres fanático del Wi-Fi gratuito, acceder a él sin una VPN puede ser un error.

Después de todo, sus datos pueden viajar sin cifrar, lo que significa que terceros pueden capturar sus credenciales.

Por lo tanto, la instalación de una VPN le permite conectarse a cualquier red de forma segura cifrando y redirigiendo sus datos.

6. Confiar en sitios web no seguros

Si está buscando en un sitio web sospechoso que ofrece ofertas sospechosas, está invitando a problemas.

Los estafadores usan toneladas de trucos para atraer a los usuarios a su trampa, y usar estos sitios es uno de ellos. Los usuarios terminan dando mucha información confidencial mientras optan por algunos servicios dudosos que ofrecen estos sitios.

Por lo tanto, debe verificar si el sitio es seguro o no. Una forma sencilla de hacerlo es comprobando la dirección web. Debe tener una extensión HTTPS en lugar de HTTP junto con un candado. Sin embargo, nunca debes bajar la guardia, incluso en sitios HTTPS.

7. ¿Qué tienen que hacer los proveedores de servicios?

Si bien a veces los usuarios son responsables de que sus cuentas se vean comprometidas, no siempre es así. Los proveedores de servicios y los propietarios de la plataforma son igualmente responsables si los datos de los usuarios se ven comprometidos. Aquí hay algunas cosas que los propietarios de la plataforma deben hacer para proteger los datos de los usuarios. ¿Por qué algunos usuarios no pueden realizar las acciones requeridas si sus datos se ven comprometidos o por motivos de seguridad?

Una respuesta clara es que los propietarios de la plataforma no transmiten sus métodos y consejos. Usar un lenguaje altamente técnico y confuso mientras se informa a los usuarios puede hacer algo más que lo requerido.

Por lo tanto, los propietarios de la plataforma deben definir un conjunto de instrucciones claras y comprensibles para que todos los usuarios puedan comprenderlas bien.