Características de seguridad en las redes sociales

Para iniciar debe tener en cuenta las redes sociales que usa y la cantidad de información que comparte al día junto con la veracidad de la misma, posterior a eso se deben tener en cuenta las siguientes condiciones de seguridad para el buen uso de las redes sociales.

Utilizar una contraseña robusta

De este modo es posible prevenir que algún atacante descubra fácilmente nuestra contraseña. Es importante mencionar que la contraseña es la llave para acceder a nuestro perfil de redes sociales de modo que si un atacante lograra descubrirla podría secuestrar la cuenta y nuestros contenidos.

No aceptar contactos desconocidos

Aceptar contactos desconocidos incrementa las posibilidades de **recibir mensajes spam o mensajes con links a sitios fraudulentos** o con contenido malicioso.

Reportar cualquier caso de *spam* o abuso

Es importante reportar los mensajes spam a nuestro proveedor de redes sociales pues **esto ayudará a prevenir que se sigan multiplicando estos ataques** utilizando una misma cuenta.

No almacenar contraseñas

El uso de equipos compartidos requiere que **no se guarden las contraseñas** de acceso en el sistema.

Cerrar la sesión

Cuando se termine de utilizar el servicio.

Mantener actualizado el navegador

Esto permitirá **estar protegido contra ataques** que aprovechan fallas en el navegador de Internet.

Procura no visitar sitios en los que en los que se soliciten datos personales o contraseñas

Muchas veces los **equipos compartidos pueden contener herramientas maliciosas** capaces de capturar todo lo que escribes, incluyendo usuarios y contraseñas, de este modo podrían posteriormente entrar a tu cuenta y realizar los cambios que deseen.

¿Público o privado?

Muchas redes sociales comparten los contenidos de forma pública. **Algunas ofrecen privacidad como una configuración global para hacer un perfil público o privado**, mientras que otras dan más opciones, permitiendo de esta manera hacer las publicaciones individuales públicas o privadas. Debemos de asegurarnos que estas configuraciones cumplan con nuestros objetivos para aceptar los términos del servicio.

Si es posible, implementar una doble autenticación

Algunos servicios como Facebook y Twitter ofrecen una autenticación de dos factores como una medida de seguridad. Normalmente, para iniciar sesión en un servicio, ingresamos una contraseña, que es lo común cuando utilizamos una red social. **Al habilitar una autenticación de dos factores, además de una clave, se introduce un dato que tenemos sólo nosotros, generalmente en forma de un número generado aleatoriamente**, o *token* que puede enviarse a nuestro dispositivo móvil a través de un SMS. De esta manera hace más difícil que alguien entre a nuestra cuenta porque se necesitaría el token o el número secreto.

Las cosas gratis, no son gratis

Muchos estafadores intentarán seducir con la idea de que puedes ganar accesorios o tarjetas de regalo gratis si completas una encuesta, instalas una aplicación o si compartes una publicación en tu red social. Mediante estas técnicas los usuarios revelan su información personal.

¿Quieres más seguidores y "Me gusta"?

Siempre hay un precio que pagar al tratar de conseguir más seguidores o "Me gusta". Ya sea pagando dinero para tener seguidores y/o "Me gusta" falsos, u otorgar voluntariamente los datos de la cuenta y convertirse de esta manera en un bono social. **Estos esquemas no valen la pena porque ponen en riesgo la información de la cuenta.**

De esa forma puedes navegar con tranquilidad en las redes sociales, recuerda que a pesar de no ser una red social con el correo electrónico personal e institucional se debe aplicar la gran mayoría de estas recomendaciones.

Vive #Cyberseguro #ViveSena.

Características de seguridad en las redes sociales