Seguridad Informática en la Web

Hay varios factores que tenemos que tener en cuenta el tiempo de estamos conectados o interactuando con en internet en diversas plataformas como redes sociales , búsquedas, registros para portales web, siempre que podamos tenemos que ser responsables con la información nuestra que vamos a compartir en el internetl

A continuación te aconsejamos :

1. Publica información personal de forma limitada y profesional

Los posibles empleadores o clientes no necesitan saber el estado de tu relación personal o la dirección de tu casa. Lo que necesitan saber es información sobre tu experiencia laboral y tus conocimientos profesionales, y cómo ponerse en contacto contigo. No proporcionarías información puramente personal a extraños individualmente, por lo tanto, no la proporciones a millones de personas online.

2. Mantén la configuración de privacidad activada

A los responsables de marketing les encanta saber todo acerca de ti, al igual que los hackers. Ambos pueden aprender mucho de tus hábitos de navegación y el uso que haces de las redes sociales. Pero puedes tomar el control de tu información. Como señala Lifehacker, tanto los navegadores web como los sistemas operativos móviles disponen de ajustes para proteger tu privacidad online. Los principales sitios web, como Facebook, también tienen ajustes de mejora de la privacidad disponibles. Estos ajustes son a veces (deliberadamente) difíciles de encontrar, porque las empresas quieren tu información personal por su valor de marketing. Asegúrate de que has activado estas garantías de privacidad y de mantenerlas activadas.

3. Practica la navegación segura

No elegirías caminar por un vecindario peligroso, por lo tanto, no visites barrios peligrosos online. Los cibercriminales utilizan contenido morboso como cebo. Ellos saben que las personas a veces se sienten tentadas ante el contenido dudoso, y pueden bajar la guardia cuando lo buscan. El "demi monde" de Internet está plagado de problemas ocultos, donde un clic descuidado podría exponer datos personales o infectar tu dispositivo con malware. Al resistirte al impulso, los hackers ni siquiera tendrán la mínima oportunidad.

4. Asegúrate de que tu conexión a Internet es segura

Cuando te conectas online en un lugar público, por ejemplo, mediante el uso de una conexión Wi-Fi pública, PCMag señala que no tienes control directo sobre tu seguridad. Los expertos en ciberseguridad corporativa muestran preocupación por los "endpoints", es decir, los lugares en los que una red privada se conecta con el mundo exterior. Tu endpoint vulnerable es tu conexión a Internet local. Asegúrate de que el dispositivo es seguro y, en caso de duda, espera a conectarte en un momento mejor (es decir, hasta que seas capaz de conectarte a una red Wi-Fi segura) antes de proporcionar información como el número de tu cuenta bancaria.

5. Ten cuidado con lo que descargas

Uno de los principales objetivos de los cibercriminales es engañarte para que descargues malware, es decir, programas o aplicaciones que incluyen malware o tratan de robar información. Este malware puede disfrazarse como una aplicación: desde un juego popular a una aplicación que comprueba el tráfico o el clima. Como aconseja PCWorld, no descargues aplicaciones que parezcan sospechosas o procedan de un sitio en el que no confías.

6. Elige contraseñas seguras

Las contraseñas son uno de los mayores puntos débiles de toda la estructura de seguridad en Internet, pero actualmente no hay manera de omitirlas. Y el problema de las contraseñas es que las personas tienden a elegir aquellas que son fáciles de recordar (como "contraseña" y "123456"), y que también son fáciles de adivinar para los ciberladrones. Selecciona contraseñas seguras que sean más difíciles de desmitificar para los cibercriminales. El software Password Manager puede ayudarte a administrar varias contraseñas para que no las olvides. Una contraseña segura es aquella que es única y compleja, de al menos 15 caracteres y que incluya letras, números y caracteres especiales.

7. Realiza compras online en sitios seguros

Cada vez que realices una compra online, necesitas proporcionar información sobre la tarjeta de crédito o la cuenta bancaria, justo lo que los cibercriminales más desean tener en sus manos. Suministra esta información solo a aquellos sitios que te ofrecen conexiones seguras y cifradas. Tal como indica la Universidad de Boston, puedes identificar los sitios seguros mediante la búsqueda de una dirección que comience

por *https:* (la S proviene de *seguro*) en lugar de comenzar simplemente por *http:*. También pueden incluir el icono de un candado situado junto a la barra de direcciones.

8. Ten cuidado con lo que publicas

Internet no tiene una tecla Suprimir, como descubrió el joven candidato de Nuevo Hampshire. Cualquier comentario o imagen que publicas online puede permanecer online para siempre, porque eliminar el original (por ejemplo, de Twitter) no elimina las copias que otras personas puedan tener. No hay ninguna manera de "borrar" un comentario que desearías no haber compartido, o deshacerte de ese vergonzoso selfie que te hiciste en una fiesta. No publiques online nada que no quieras que vea tu madre o un empleador.

9. Ten cuidado con quien conoces online

Las personas que conoces online no siempre son quienes dicen ser. De hecho, incluso pueden no ser reales. Como indica InfoWorld, los perfiles de redes sociales falsos son una forma popular entre los hackers de atraer a los usuarios incautos de Internet y robarles la cartera online. Se aconseja que seas tan prudente y sensato en tu vida social online como lo eres en tu vida social en persona.

10. Mantén actualizado el programa antivirus

El software de seguridad en Internet no puede protegerte contra toda amenaza, pero detectará y eliminará la mayor parte del malware, aunque debes asegurarte de que esté actualizado. Asegúrate de estar al día con las actualizaciones del sistema operativo y las actualizaciones de las aplicaciones que utilizas. Proporcionan un nivel de seguridad vital.