Orientaciones para navegar seguro en la red

1. Publica información personal de forma limitada y profesional

No exponer tu vida privada, ni profesional a extraños.

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. (Según Kaspery)

3. Practica la navegación segura

Procura no clicar en imágenes dudosas ni navegar por páginas que no sean seguras, asi evitarás el malware.

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.(Según Kaspery)

5. Ten cuidado con lo que descargas

No descargues aplicaciones o juegos que parezcan sospechosos, pueden contener malware que se intale en tu dispositivo.

6. Elige contraseñas seguras

Elige contraseñas evitando fechas de nacimiento, teléfonos, etc, que incluyan mayúsculas, minúsculas, números y letra.

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.

(Según Kaspery)

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. (Según Kaspery)

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. (Según Kaspery)

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. (Según Kaspery)