Las 10 cosas posiblemente peligrosas que haces en línea

Cuando conduces, usas el cinturón de seguridad. Además, estacionas el auto cerca de una luminaria. Incluso te aplicas protector solar cuando el día está nublado. ¡Prefieres no correr riesgos! Sin embargo, ¿qué sucede cuando te conectas a Internet?

Revisa nuestra lista para comprobar si estás exponiendo tu dinero e identidad a los peligros que plantea la Internet.

1. ***Das por sentado que el sitio de tu banco es seguro.***

Los criminales siguen a tu dinero. Por ello, escribir con rapidez y en forma incorrecta la dirección URL de tu banco o no darte cuenta de que eres redirigido a un sitio web falso puede dar lugar a un incidente de cyberrobo. Evita las extracciones de dinero no deseadas usando la tecnología Safe Money de Kaspersky para identificar sitios web de suplantación de identidad (phishing) y proteger todos los ámbitos de tu experiencia de banca en línea.

2. ***Haces compras en lugares poco confiables.***

Es fácil entusiasmarse cuando encuentras una oferta muy atractiva en línea, pero debes aplicar la cautela antes de hacer clic en "Agregar al carro". Si compras una ganga en un sitio desconocido o haces clic en un resultado de búsqueda en lugar de ingresar directamente la dirección URL, puedes estar comprando la oferta de un cibercriminal. Entonces, ¿cómo puedes comprar en línea de manera segura? Protege todas tus transacciones de principio a fin con la tecnología Safe Money de Kaspersky.

3. ***Solo usas una contraseña.***

Si no creas contraseñas seguras, los hackers pueden apoderarse de tu dinero y de tu identidad en línea. Si usas varias contraseñas, les impedirás acceder a todo tu mundo en línea con una sola palabra. También es fundamental que crees contraseñas seguras. Por fortuna, la función Password Manager de Kaspersky genera contraseñas que almacena en forma segura en todos tus dispositivos. Todos tus sitios estarán seguros y solo tendrás que recordar una contraseña.

4. ***No conoces a todos tus amigos.***

Quizás te parezca bien aceptar solicitudes de amistad de todos los habitantes de tu ciudad natal en Facebook, pero te recomendamos actuar con discreción cuando amplíes tu red social. Cuando aceptas una solicitud de amistad de alguien desconocido, abres las puertas al malware o a los ladrones de identidad a tu círculo más cercano.

5. ***No cuestionas la autoridad.***

Es importante que te muestres un tanto desconfiado cuando te conectes. De hecho, a diario se detectan más de 5000 sitios web comprometidos. Si no cuestionas nunca la legitimidad de las páginas que visitas, los cibercriminales pueden apoderarse de tu dinero y tus datos. También procura evitar hacer clic en anuncios y enlaces inusuales en correos electrónicos o mensajes de texto de remitentes conocidos.

6. ***Eres demasiado sociable.***

Revelar información importante a tus amigos y a una red más amplia de conocidos puede resultar peligroso. Cuando publicas información personal, como tu nombre, el nombre de tu escuela o tus antecedentes familiares, ofreces respuestas a preguntas de seguridad de contraseñas. Ajusta los controles de seguridad para limitar la cantidad de personas que ven tu información.

7. ***No lees la letra pequeña.***

A nadie le gusta leer la letra pequeña. Determinadas empresas en línea se aprovechan de ese espacio para incluir términos que saben que no vas a leer. Si aceptas sus términos y condiciones sin leerlos, puedes entregar involuntariamente tu privacidad en línea a la empresa y a sus filiales.

8. ***Compras y realizas transacciones bancarias a través de redes Wi-Fi públicas.***

Los cibercriminales disfrutan espiando las redes Wi-Fi públicas y engañando a los usuarios para que se conecten a redes fraudulentas. Analiza todos los enlaces Wi-Fi con cautela y usa una VPN (red privada virtual) para cifrar los datos importantes. Cuando compres y realices transacciones bancarias en línea, verifica que la conexión sea totalmente segura usando la tecnología Safe Money de Kaspersky. Si estás operando desde un dispositivo móvil, utiliza tu red celular para las transacciones importantes.

9. ***Liberas tus dispositivos móviles.***

El término "liberar" o "jailbreak" va más allá de agregar funciones al teléfono o a la tablet. También significa eliminar protecciones importantes y abrir las puertas a gran diversidad de malware móvil para que ingrese en tu dispositivo. Para mantenerte seguro mientras te desplazas, evita liberar tus dispositivos y visitar sitios de descarga de terceros, aplicaciones sospechosas y los demás peligros en línea inherentes a ellos.

10. ***Desconoces los sitios que visitan tus hijos.***

Si tienes hijos, debes conocer sus sitios web y redes sociales favoritos. Internet puede ser una prolongación de la vida de tu hijo o hija, de manera que lo más conveniente es que te involucres y los orientes en las conductas adecuadas en línea, el acoso en línea y los desafíos cambiantes de la vida en línea.

Fuente:https://latam.kaspersky.com/resource-center/preemptive-safety/the-ten-potentiallydangerous-things-you-do-online