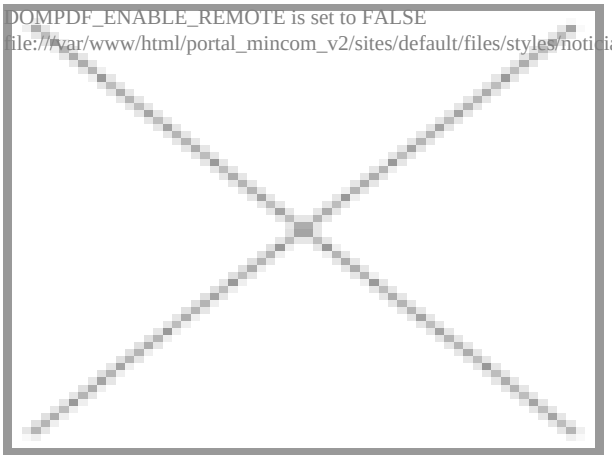

Source:
Tomado de la Pupila Insomne Omar Pérez Salomón

La tendencia creciente en el número de personas con teléfonos celulares, de los trámites en línea y en el uso de pagos electrónicos, requiere reforzar la seguridad del equipo y de sus propietarios, en particular sus datos1 y metadatos2.

Conozco personas que le han extraído de su tarjeta bancaria altas sumas de dinero y otras que en redes sociales digitales le han suplantado su identidad y provocado que familiares y amigos suministren una cantidad nada despreciable de efectivo, supuestamente solicitado por el titular de la cuenta.

Si bien es cierto que las aplicaciones han adquirido mayor relevancia en las interacciones en la red, las malas prácticas en el uso de estas tecnologías exponen a muchas personas a estafas, robo de identidad y daños físicos por parte de hackers que buscan información personal que puedan utilizar para cometer estos ciberdelitos.

La falta de seguridad y protección de la conexión y privacidad en internet implican otros riesgos y amenazas, relacionadas con la publicación de imágenes, videos y comentarios personales molestos que, una vez en línea, son casi imposibles de borrar; y la conexión con personas que dejan una huella desagradable en ti, tal y como se refleja en la serie 1er grado que por estos días transmite la televisión cubana.

Como es de suponer muchas son las reglas y pautas de seguridad a seguir en la red de redes. Sobre este particular estaremos compartiendo con Daniel Ramos Fernández, jefe de la división de operaciones de seguridad de la Empresa de Telecomunicaciones de Cuba (ETECSA) y experto en sistemas informáticos y ciberseguridad.

OPS: Creo que la recomendación más importante que podemos hacer es aquella que va dirigida a:

1. Tener la capacidad de pensar
A la hora de acceder y navegar por internet se requiere tener la capacidad de pensar, analizar y contrastar la información que recibes, determinar qué sitios visitar, cómo encontrar el contenido que buscas, el antivirus que debemos instalar. No permitas que en tu mente predominen los reflejos condicionados que hagan que repitas como un loro lo que transmiten determinados medios y personas en las redes sociales digitales. Ello te permitirá identificar e interactuar oportunamente con las amenazas.

Mientras más conocimientos adquieras disminuirá el predominio de los instintos en tu actuación en la red. Reflexiona sobre tu responsabilidad en lo que compartes y la imagen que proyectas.

Es imprescindible que conozcas y aprendas cómo funcionan los diferentes servicios, productos de internet y

redes sociales, para así evitar que accedas a páginas o contenidos inapropiados, maliciosos o seas objeto de algún ciberdelito. En caso de ser necesario es preferible que consultes con algún entendido en estos asuntos.

DRF: A partir de las experiencias de especialistas y estudiosos en esta materia, proponemos las siguientes normas a seguir para proteger la conexión y privacidad en internet, que por supuesto no son las únicas, no son difíciles de aplicar ni se precisa que seas experto en el uso de estas tecnologías. Como sugería Omar, es vital que pienses, reflexiones sobre cada paso que des en la red de redes:

2. Controlar el tiempo que usas internet
Es muy importante para tu salud y bienestar relacionarte en espacios físicos con familiares, amigos, otras personas y no crear dependencia en el uso de internet. Establece los horarios para el uso de la red de redes.

3. Divulgar datos personales de forma limitada
Es recomendable que seas sensato y prudente en el momento de exponer tus datos personales en la red. Como mencionabas, los hackers buscan saber todo de ti y tomar el control de tu información para realizar estafas y robo de identidad. Para nadie es un secreto que las empresas propietarias de servicios en internet y de las redes sociales recolectan los metadatos y datos de sus usuarios: información con las opiniones, gustos, formas de pensar, patrones de comportamiento, es decir, un conocimiento valioso sobre nuestro comportamiento, idiosincrasia y cultura, y proveerlo a empresas con el objetivo de realizar análisis de mercado y publicidad comercial, así como a los Servicios Especiales y Agencias de gobiernos imperialistas.

4. Utilizar contraseñas robustas
En todos los servicios en la red de redes se precisa utilizar contraseñas robustas, siempre que sea posible, las de autenticación de dos factores. Es importante que sea única para cada servicio, de tal manera que si algún hacker logra identificar alguna de ellas, no afecte a las demás cuentas. También debes cambiar tus contraseñas periódicamente y evitar relacionarlas con tu información y datos personales.
Según la empresa rusa de seguridad informática Kaspersky Lab, una contraseña segura es aquella que es única y compleja, de al menos 15 caracteres y que incluya letras, números y caracteres especiales.
No es conveniente guardar las contraseñas en el bloc de notas del móvil, o en una carpeta de la computadora para evitar su uso por extraños en caso de pérdida del dispositivo o si alguien llega a tener acceso, ya sea físico o remoto a nuestro equipo.

5. Crear copias de seguridad
Es aconsejable hacer una copia de seguridad de toda la información que tengas en los dispositivos o en la nube. Este es un paso muy importante para evitar la pérdida de datos e información valiosa para usted. Recuerde que está el riesgo de que perdamos el dispositivo, sufra alguna avería, se introduzca un virus malicioso que borre nuestra información o cifre nuestras carpetas para pedir un rescate económico a cambio de su restauración.

En este sentido aconsejamos crear copias de seguridad de manera frecuente.

6. Practicar la navegación de forma segura
Evita visitar sitios con contenido dudoso. Los ciberdelincuentes los utilizan como cebo y un descuido de tu parte podría exponer datos personales o infectar tu dispositivo con virus maliciosos. No descargues aplicaciones o juegos que procedan de un sitio confuso ya que pueden incluir virus, lo mejor es descargarlos de sitios oficiales como ApKalis, Google Play o App Store. También es recomendable estar alerta con los correos electrónicos y mensajes que se reciben y con la interacción con personas desconocidas, pues tras ellas pueden esconderse fraudes o acosos.

Cualquier operación de comercio electrónico debes hacerlo en sitios seguros. Recuerda que los hackers están siempre buscando información sobre tarjetas o cuentas bancarias. Según Kaspersky Lab debes suministrar esta información solo a aquellos sitios que te ofrecen conexiones seguras y cifradas. 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. Si vives en Cuba utiliza las pasarelas de pago electrónico Transfermóvil y Enzona.

Los navegadores web y los sistemas operativos móviles disponen de ajustes para proteger tu privacidad en línea. Activa estas garantías de privacidad y mantenlas activadas.

7. Mantener actualizados los dispositivos y aplicaciones

Es importante tener nuestros dispositivos, navegador, sistema operativo, softwares o aplicaciones con las últimas versiones. Ello contribuirá a reforzar nuestra seguridad en la Red. Las actualizaciones se suelen realizar para solucionar problemas o brechas de seguridad mediante parches que protegen tu equipo de cómputo o dispositivo móvil de ataques cibernéticos.

8. Cerrar la sesión de programas y dispositivos
Es conveniente cerrar la sesión de cualquier programa y dispositivo cuando lo termines de usar, con más razón si utilizamos un equipo que no sea nuestro, teniendo en cuenta que puede tener algún virus malicioso que registre nuestros datos.

OPS: Permíteme sugerir una medida que es esencial en la protección de los equipos y conexión.

9. Instalar y mantener actualizado el programa antivirus

Tener un antivirus actualizado en tu dispositivo te da la posibilidad de detectar y eliminar la mayor parte de los programas informáticos maliciosos usados por los delincuentes cibernéticos y otras amenazas. Para preservar los equipos y datos personales periódicamente se debe realizar un análisis completo con el antivirus.

Esto hay que aplicarlo tanto en equipos de escritorio como en dispositivos móviles. Es cierto que existe una tendencia a instalar antivirus en los móviles; pero aún es muy bajo el por ciento de los usuarios que lo utilizan. Recomendamos utilizar las soluciones de seguridad que ofrece la empresa Segurmática.

DRF: Me queda mencionar algunas cuestiones acerca de la conducta a seguir en el acceso a las redes sociales digitales.

10. Usar de forma responsable las redes sociales digitales
Las redes sociales digitales es el espacio virtual más utilizado por los internautas a nivel mundial y en Cuba tiene igual comportamiento. Recordemos que durante el año 2022 Facebook alcanzó 4,1 millones de suscriptores, Youtube y WhatApp 3,9 millones, Telegram y Twitter 3,7 millones.

Utiliza las redes que te interesen por su perfil profesional o de entretenimiento y que puedas manejar con facilidad. En la medida que seas usuario de varias de ellas te será más difícil proteger tus datos. Para cada red social usa al menos dos métodos de verificación de identidad, una contraseña y correo electrónico diferente y no permitas que aplicaciones externas accedan a alguna de ellas.

1Se refiere a la información y contenido implícito en una llamada telefónica, correo electrónico, en el acceso a una plataforma de internet o red social digital.
2Permiten conformar los patrones de comportamiento de los usuarios en la red. Así, los números telefónicos y direcciones electrónicas de origen y destino desde donde se realiza una comunicación, las direcciones IP desde donde te conectas y de los sitios visitados, el nombre de los perfiles y cuentas que tienes en las redes sociales digitales, su localización física, la cantidad de segundos de la llamada, de palabras del e-mail o de minutos de acceso a un sitio o red social digital, conforman los metadatos.

https://bit.ly/3Cv3FyL [1]

Links

[1] https://bit.ly/3Cv3FyL