



La ciberseguridad no es un lujo, es una necesidad

Por Hugo Montoya Díaz

Ilustración: Gustavo Contreras



Frases como “me hackearon” o “fui víctima de un *hacker*” son comunes, pero no siempre ciertas porque muchas veces se trata de una falla o una incomprensión del sistema. Se denomina *hacker* al delincuente que actúa como espía, *cracker*, etc. La realidad es que los genuinos *hackers* somos profesionales en ciberseguridad, curiosos informáticos en pro del bien.

La diferencia entre vigilancia y espionaje responde a varias consideraciones, puesto que las acciones de inteligencia digital son tareas del Estado para detectar y evitar actos delictivos, terrorismo, crimen organizado, espionaje extranjero, fraudes y más. Existen normas y tratados para realizar buenas prácticas de vigilancia cibernética, con respeto y garantía a los derechos humanos, a pesar de la secrecía interna. En ese sentido, la vigilancia tiene una justificación legal.

Este tipo de acciones son realizadas por una estructura técnica muy amplia y con expertos, pero los usuarios comunes también pueden hacer mucho para no ser víctimas. Todos los sitios *milagrosos*, donde regalan dinero o dan apoyos sin condiciones, se descarguen películas, imágenes o *software* sin costo son ilegales. Muchos navegadores tienen filtros de navegación segura y a veces emiten alertas, pero hay aplicaciones que se pueden comprar y evitar riesgos.

Al abrir un sitio, si la dirección no empieza con <https://www> o si tiene demasiados caracteres es falsa, así como los correos desconocidos,

con enlaces no solicitados, mencionando que son de algún banco, o que pidan datos personales y bancarios sensibles. No siempre es fácil identificarlos, las estafas y los ataques son cada vez más sofisticados, por ello es importante tener un *software* de navegación segura y mucha prudencia.

En el caso de las *cookies*, estas son herramientas para recoger datos técnicos de conexión; se usan para conocer a los usuarios y ofrecer productos y servicios en línea, *marketing* digital. No hay problemas con estas si provienen de sitios que ya conocemos, depende de la naturaleza de estos; algunos tienen fines maliciosos. En la mejor de las situaciones, se pueden declinar y con eso salimos de la navegación. A la fecha se sigue regulando su emisión y buscando mejores prácticas en los desarrolladores de páginas web.

Y si alguien piensa que los avisos de privacidad nos protegen, la verdad es que no. Son advertencias de cómo, con quién y para qué fin serán usados nuestros datos. Si se sospecha de un mal uso de nuestra información, se pueden constatar con una solicitud de derechos denominada ARCO (acceso, rectificación, cancelación y oposición) ante una institución autorizada.

Con todo esto ya tenemos una idea de cómo identificar posibles sitios fraudulentos, pero los niños no cuentan con este criterio y por ello es muy importante establecer medidas preventivas. Antes de todo, es responsabilidad de los padres o tutores tener comunicación con sus hijos y conocer las actividades que realizan en los equipos. Los teléfonos inteligentes no son para ellos, quienes los usen deben tener supervisión constante, sistemas de control parental y establecer aplicaciones con perfil infantil (como YouTube Kids), incluso programas especializados para protegerlos de acciones maliciosas.

Además de ello, el sentido común debe estar presente al compartir información en cualquier plataforma. Los usuarios con perfiles personales deben considerar los siguientes puntos para cuidar su integridad digital:

- No aceptar perfiles sin foto o sin antes revisar su historial de imágenes.
- No aceptar invitaciones de personas desconocidas, sin amistades en común o con pocos agregados.
- No publicar información sensible y no subir fotos de niños. Si queremos compartir una foto con ellos, procuremos que estén acompañados para crear un efecto de protección y no dejarlos a merced de la pedofilia digital.
- Tener cautela en las relaciones amorosas, no aceptar propuestas que expongan nuestra intimidad.
- Denunciar cualquier tipo de actividad no apropiada.

A partir de todo lo anterior podemos decir que la ciberseguridad es una especialización enfocada a la protección y defensa de los equipos de cómputo de escritorio y móviles, servidores, teléfonos inteligentes, sistemas electrónicos y magnéticos, así como toda la información que

se almacena, transmite y traspasa en ellos, contra ataques maliciosos, espionaje y vulnerabilidades.

Existen algunas carreras en inteligencia cibernética en México, pero el mapa curricular tarda mucho en renovarse por el tipo de educación (escolarizada y presencial). Las maestrías nacen con mejor contenido, más actualizado y con más práctica que teoría. En línea, en cambio, existe un gran universo de oportunidades de alta calidad que ofrecen organismos e instituciones especializadas y con certificados de reconocimiento internacional. Por tanto, es posible encontrar expertos en el país.

Como reza el dicho popular: “sale más barato prevenir que remediar”, es recomendable invertir en seguridad digital para evitar pérdidas de datos, recursos e integridad personal a causa de extorsiones, secuestros e invasión a la intimidad. Los ataques maliciosos (*ransomware*), por ejemplo, se expresan desde las cuantiosas solicitudes para rescatar información, fraudes, trata de personas, pedofilia, hasta suplantación de identidad para realizar pagos en nuestro nombre o realizar actividades ilegales. Recordemos que los menos protegidos son los más vulnerables, y no actuar a tiempo los pone en peligro. 📞



Hugo Montoya Díaz es experto en ciberseguridad. Graduado de Dirección Estratégica por la Universidad Anáhuac, del máster de Analista en Inteligencia por el Instituto de Seguridad, Ciberseguridad y Geopolítica y de un posgrado con metodología avalada por el FBI, la CIA y otras agencias del extranjero. Está certificado como consultor en ciberinteligencia por organismos internacionales, como la Unesco, y ha ocupado puestos directivos en varias empresas e instituciones, como la Agencia Espacial Mexicana. Actualmente es presidente de la Cámara Nacional de la Industria de la Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI).

