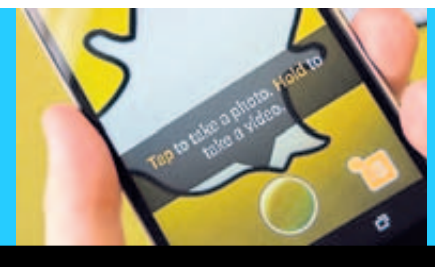
Tecno (F)



Snapchat se actualiza

La aplicación se actualizó el lunes para resaltar el contenido de su sección en vivo y la sección Discover, sobre el de otros.

nuevovivir@granasa.com.ec

ESPIONAJE

NO SE PUEDE EVITAR, PERO SÍ **HACERLO DIFÍCIL**

GIANNELLA ESPINOZA COBOS
espinozag@granasa.com.ec
GUAYAQUIL

Dejar de usar Internet y todas sus maravillas no es la idea. Incluso, algunos empezamos a convulsionar con solo pensarlo. Sin embargo, es hora (de hecho desde sus inicios) de ser conscientes de que en la Red todos los días perdemos un poco más de nuestro derecho fundamental a la privacidad y lo hacemos sin darnos cuenta.

Los gobiernos espían. Las fuerzas de vigilancia espían. Las empresas espían. Todos con un poco de dinero, tiempo, conocimiento e intereses, espían. Lo han dicho Snowden, Assange y también las empresas de seguridad informática. Pero ha sido el caso de la empresa italiana Hacking Team, que provee un sistema de vigilancia a gobiernos y cuerpos policiales de varios países, el que ha puesto a todos a hablar, a preocuparse y a tratar de entender el tema.

¿Qué pasó? Sus sistemas fueron hackeados y los atacantes accedieron a un gran número de documentos con información sensible que han sido colgados en la Red (400GB). Entre estos se encuentran desde correos y documentos que implican a gobiernos como el de Ecuador, hasta la parte más sensible del sistema de vigilancia: el código fuente.

EL DETALLE

Reporteros sin fronteras califica a Hacking Team y su herramienta como uno de los enemigos de Internet por su uso en países autoritarios y represores.

Esta publicación no pretende señalar culpables ni las intenciones del espionaje virtual, pero sí dejar lecciones sobre la seguridad de nuestros dispositivos y nuestra presencia en la red.

Lo dicen los expertos, es casi imposible evitar que las comunicaciones sean interceptadas, pero sí se pueden usar herramientas y tomar precauciones para que sea mucho más difícil. También es básico usar el sentido común.

¿Cómo empezar? No hay aparatos más vulnerables que nuestros dispositivos móviles, esto debido a la cantidad de aplicaciones gratuitas que instalamos a diario (en promedio 5). Entonces podemos empezar por ellos.

DILE NO AL' ROOT'

Los códigos maliciosos llegan en su mayoría con permisos root activados (Android) y el jailbreak realizado (iOS). Estas funciones son las que permiten al usuario tener acceso a una personalización completa de su sistema operativo e incluso con contenido ilegal que no ha sido liberado o autorizado por el fabricante, pero elimina por completo la seguridad del equipo.

EVITA EL WIFI ABIERTO

No confíes ciegamente en las redes wifi abiertas. Muchos códigos maliciosos se propagan por esta vía pública. Es tentadora, pero capaz de extraer buena parte de nuestra información con el simple hecho de subir una foto a Facebook.

NO DESCARGUES TODO

Deja de instalar programas o apps por moda o curiosidad. Asegúrate de que lo que vayas a descargar tenga buenas recomendaciones por los usuarios y que no te solicite más de la información que pudieras dar a un completo desconocido.

CUIDA TUS 'CLICS'

En muchas ocasiones, las infecciones llegan a través de correos o enlaces que circulan a través de mensajes de Facebook de gente desconocida. Duda.

APÓYATE CON EL CIFRADO

Primero, no olvides tener tu sistema operativo actualizado, pues lograrás parchar los agujeros de seguridad. Lo siguiente es probar las aplicaciones para el cifrado de datos (es decir para volverlos ilegibles ante terceros) que te recomendamos en esta página para mantener a salvo tus conversaciones y navegación.

EN CONTEXTO

El caso de **Hacking Team** ha puesto a todos a hablar y a debatir sobre la privacidad en Internet

EXPRESO pone a disposición herramientas que puede utilizar para evitar las intromisiones

Los expertos aseguran que en la **Red** no estamos nunca 100 % seguros, pero podemos intentarlo

Google figura entre una de las plataformas que nos vuelve más vulnerables en el mundo virtual

6. UN HOSTING DE ARCHIVOS AMIGABLE

En algún momento tendrá que compartir archivos grandes. Si se trata de información sensible, subirla a determinados servicios puede ser arriesgado. Un sistema como BitTorrent Sync, usa un ingenioso sistema de claves secretas y cifrado de 256 bits, para que compartir archivos y carpetas sea fácil y seguro a la vez.

RAFAEL BONIFAZ /
PRESIDENTE DE ASLE

"Cada vez que usas Google le estás contando lo que piensas"

El quiteño activista del Software Libre, la privacidad y las libertades en Internet y actual presidente de la Asociación de Software Libre del Ecuador (ASLE), explica con un ejemplo sencillo, el por qué debemos preocuparnos para la privacidad de nuestros datos en Internet.

"Imagine qué haría si su vecino lo espiara... ¿Se sentiría incómodo? ¿Qué tanto podría saber su vecino de usted si lo espía por la ventana? Pero, ¿qué pasaría si este accede a su computadora, correo electrónico, redes sociales y demás? ¿Cómo podría saber más su vecino? Husmeando en Internet, por supuesto. Todos tenemos algo que esconder, erramos porque somos humanos y todos somos inocentes antes de que se demuestre lo contrario. Vigilar nuestras comunicaciones va contra ese estado de privacidad".

El solo hecho de usar Google nos vuelve vulnerables al espionaje, lo repiten todos los expertos en seguridad... ¿Cuál es la solución en este mundo enREDado? "Cada vez que usas Google, le estás contando lo que piensas... La solución más rápida y sencilla es utilizar el navegador Tor. Luego se puede avanzar a sistemas de chat encriptados, para esto existe software como Jitsi para computadoras con cualquier sistema operativo; y en celular tenemos ChatSecure. Luego se podría avanzar hacia el correo seguro utilizando el software Thunderbird con el complemento enigmail para cifrar los correos".

¿Hay manera de mantenerse a salvo estando en las redes? "Hace más de dos años cerré mi cuenta de Facebook y los invito a hacer lo mismo. Esta empresa forma parte del programa de espionaje de la NSA y es dueña de redes como WhatsApp e Instagram. Si se va a quedar en ellas, al menos use KeePassX, un software le permite gestionar contraseñas seguras para cada sitio".

LUIS LOAIZA /
CTO EN CRIPTEXT

"Cuando usas tecnología gratis pierdes el control de tus datos"

Luis Loaiza, CTO en Criptext, una startup con desarrollo ecuatoriano que brinda soluciones para mensajería segura (correo y chat), señala que las revelaciones sobre Hacking Team, son solo un aviso más de que los gobiernos usan métodos de supervisión y de espionaje con ciudadanos y entre gobiernos.

Pero, no solo se trata de gobiernos. "También lo hacen las empresas privadas", afirma, "al final del día la mayoría de los consumidores usan Internet, comparten sus datos en redes sociales, y no estás pagando para que sean protegidos. Cuando usas tecnología gratis pierdes control de la información que envías o comunicas".

La gratuidad de las apps se compensa con la información que entrega el usuario para poder utilizarlas. Google, por ejemplo, detecta lo que el usuario está hablando y enseguida le arroja sugerencias (ads).

Criptext Mail, una de las soluciones de Loaiza, controla información que comparte el usuario una vez que el usuario da clic en 'enviar'. Deja corregirlo una vez enviado, ponerle fecha de caducidad e incluso borrarlo de Internet. En cuanto a Criptext Chat, disponible por ahora solo con invitación, deja libre de capturas comprometedoras a los usuarios. No las permite y además avisa cuando alguien intenta hacerlas.

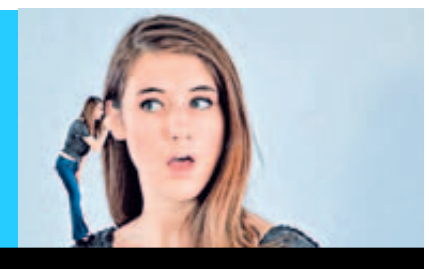
5. UN MAIL CIFRADO

Una cuenta de correo contiene una cantidad inmensa de información personal. Por lo tanto el intercambio debe ser seguro. Existe una extensión para Chrome y Safari llamada Criptext, la cual funciona desde la bandeja de Gmail, es gratuita y permite encriptar sus mensajes, además de tener el absoluto control sobre ellos. Por ejemplo, podrá editarlos una vez enviados y también ponerles caducidad.

Facebook la app preferida

Es la herramienta más utilizada, con una presencia del 70,2 % entre los teléfonos iOS y Android de los usuarios americanos.

CASA ADENTRO
Hablar en solitario no evidencia locura



PABLO RAMOS/
ESPECIALISTA EN ESET LATINOAMÉRICA

"Da Vinci, el código liberado de Hacking Team, no es el fin del mundo"

Da Vinci, una de las herramientas de espionaje que la italiana Hacking Team, ha diseñado para gobiernos y fuerzas de seguridad y que fue liberada por hackers para el uso de cualquier delincuente virtual, es capaz de leer y capturar mails y chats, grabar las pulsaciones del teclado, acceder al disco duro; a llaves de seguridad cifradas e incluso al audio y a la imagen de la webcam.

Según Pablo Ramos, argentino, especialista en seguridad informática de ESET Latinoamérica, compañía dedicada al desarrollo, investigación y comercialización de soluciones de protección y seguridad informática, no deja de ser un malware. Es decir que lo que se propaga no es ni más ni menos que un código malicioso que puede evitarse con una solución de seguridad.

"No existe un código malicioso del que nunca podamos librarnos. No es el fin del mundo. Detectar, prevenir y eliminar es la misión de los laboratorios de seguridad", añade.

Para esto recomienda que los usuarios de la Red adquieran una solución como ESET Mobile Security y la instalen en sus equipos para librarse de este tipo de malware, además que mantengan actualizado su sistema operativo y utilicen contraseñas fuertes. Otro consejo, dice, que desconfíen de los correos electrónicos que lleguen de direcciones desconocidas, al igual que de sus archivos adjuntos.

El experto aclara que no juzga a los gobiernos que usan herramientas de espionaje, siempre y cuando estas sean las permitidas por la legislación y se trate de situaciones que supongan un potencial peligro para la seguridad de una nación.

1. UNA CONEXIÓN SEGURA

Ninguna conexión asegura una privacidad y anonimato totales, pero puede acercarse a ello con anonimizadores y cifrado de datos. Tor, un software disponible para muchos sistemas operativos, encamina su tráfico por una serie de nodos, que hacen la navegación sea anónima. Su paquete instalable, es muy fácil de usar y configurar.

2. UN NAVEGADOR 'PRUDENTE'

El navegador es quizá el programa donde más tiempo pasamos. Debe ser seguro. Tor Browser se trata de una opción basada en Mozilla Firefox que viene preconfigurado para usar el servicio de anonimato Tor. También puede usar SRWare Iron, una versión segura de Chrome que no envía datos a Google.

3. UN BUSCADOR QUE GUARDE SECRETOS

La navegación comienza casi siempre con una búsqueda. Y las búsquedas dicen muchísimo del usuario. El buscador independiente DuckDuckGo se ha planteado como una de las mejores alternativas a Google: sus resultados tienen una calidad análoga y no almacena las búsquedas, lo que impide asociarlo con ellas.

4. UNA APP DE MENSAJES CONFIABLE

¿WhatsApp? No, no es app segura. Para teléfonos móviles, las más interesantes son Wickr (iOS), Gryphn (Android), Criptext Chat (Android e iOS), las cuales permiten cifrar tus mensajes con un algoritmo muy potente y no almacenan las conversaciones en el teléfono.

EL PERSONAJE

SATORU IWATA
EXPRESIDENTE DE NINTENDO

'The game is over' para Satoru Iwata

Su muerte golpeó a los gamers (amantes de los videojuegos). En especial a los seguidores de Nintendo. En las redes sociales, sus fans le agradecieron por su rebeldía, por pensar en la experiencia de juego antes de cómo se verían los gráficos, pero sobre todo por cuidar a Mario y a la pandilla.

Satoru Iwata (japonés), una de las figuras más importantes en la industria de los videojuegos y presidente del grupo Nintendo, falleció el 11 de julio a los 55 años.

Considerado un genial desarrollador, empezó a trabajar en la empresa creadora de Mario en 2000 y la dirigió desde 2002, lo que le significó una brillante carrera en la empresa japonesa. Logró darle un nuevo impulso con el lanzamiento al mercado de consolas tan emblemáticas como las gamas DS (portátiles) y Wii (modelos de salón).

Fue él quien amplió la gama de jugadores extendiéndola a las mujeres y las personas de edad. También quien se opuso a los recortes de personal a los que se veía obligada la compañía debido a los malos resultados financieros en 2014, argumentando que era imposible crear juegos que sorprendan al mundo con empleados que tengan miedo de mantener su empleo.

Iwata no era solo el cuarto presidente de una compañía de videojuegos, ni alguien con muy buena oratoria, era un "gamer de corazón"... En la Game Developers Conference de 2005, dijo: "En mi tarjeta de visita, soy un presidente de empresa. En mi mente soy un programador de juegos. Pero en mi corazón soy un jugador".

Prueba de ello es que programó desde cero el sistema de combate de Pokémon Stadium para Nintendo 64 en solo una semana. Arregló casi sin ayuda y en tres semanas uno de los juegos abanderados de GameCube, Super Smash Bros y Melee, que estaba inundado de errores y a punto de ser retrasado. Lo hizo siendo ya presidente de la compañía. También se puso en primera línea de fuego y siempre fue capaz de pedir disculpas cuando alguno de los lanzamientos no cumplían las expectativas.

Una de sus últimas decisiones importantes, a nivel empresarial, fue asociarse al grupo de apps móviles, DeNa. Con ello, buscaba explotar a los célebres personajes de Nintendo, como Mario Bross y Pikachu. Su sueldo base era de $ 770 mil al mes, pero podía alcanzar los $ 2.11 millones, con bonos y beneficios de la empresa.

¿Su reemplazo? La compañía ha dado dos nombres hasta ahora, Shigeru Miyamoto, creador de diversos juegos y personajes, y Genyo Takeda, uno de los actuales dirigentes de Nintendo.

MÁS DE ÉL

Estudios. Al terminar la secundaria ingresó al Instituto Tecnológico de Tokio y se graduó en Informática.

SE ACERCA CAMPUS PARTY QUITO 5

El encuentro de tecnología, Campus Party Quito, se realizará por quinto año consecutivo, del 30 de septiembre al 4 de octubre, el Centro de Exposiciones y Convenciones Mitad del Mundo Cemexpo. La temática de esta nueva edición será el universo y los planetas, para rendir tributo al aniversario número 150 del escritor francés Julio Verne y su obra 'De la Tierra a la Luna'.

NOVEDAD

LG AMPLÍA GARANTÍA

LG Electronics ha extendido la garantía de sus acondicionadores de aire residenciales, con tecnología Inverter Compressor, a 10 años. Esta tecnología, que ofrece un rendimiento de refrigeración potente mientras opera en casi en silencio, tiene control absoluto en la salida del aire, permitiendo que el acondicionador reduzca el consumo de electricidad de la casa y por ende el valor de la planilla.

EPSON CON TRES PREMIOS TIPA 2015

Epson, compañía global dedicada a la impresión e imagen digital, recibió tres premios en el TIPA Awards 2015, el cual reconoce la innovación tecnológica, el diseño y la facilidad de uso en productos de imagen para la industria fotográfica.

Las categorías reconocidas fueron: mejor impresora (SureColor SC-P600), mejor proyector (EH-LS10000) y mejor escáner fotográfico (Perfection V850 Pro).

SABER +

ENCUÉNTRELO EN NUESTRAS VERSIONES
IPAD Y ANDROID

¿DE QUÉ SE TRATA EL CIFRADO DE DATOS?
Entérese cómo puede volver ilegibles sus conversaciones.

LO QUE LOS HACKERS OPINAN SOBRE HACKING TEAM
Lea los comentarios de hackers sobre el caso.

+@ INTERACTIVO

PREGUNTA: ¿JUSTIFICA DE ALGUNA FORMA QUE LOS GOBIERNOS ESPÍEN A SUS MANDANTES?

Le preguntamos a nuestros lectores, a través de las redes sociales, si encontraban justificación al hecho de que los gobiernos espíen a sus mandantes y esto fue lo que nos dijeron:

- Daniel García: "No encuentro justificación. La privacidad de los mandantes, también de los consumidores, debe ser inviolable y no solo en la red".

- Juan Javier Castro: "Solo si estuviera amparado por la ley y se justificara la intromisión con una amenaza a la nación".

- Dayanna Avilés: "No hay justificación. Pero, los usuarios debemos ser prudentes y coherentes con lo que publicamos o enviamos por Internet".

- Rolando Romero: "Lo admito con previo aviso y orden judicial. Caso contrario es solo un abuso más".