10 costumbres a desechar para mejorar la ciberseguridad

mexus aggity

El ser humano es un animal de costumbres. Nos cuesta mucho alterar nuestra forma de actuar con según qué cosas, especialmente si llevamos haciéndolas desde hace infinidad de años. Hay un refrán que dice: «a un perro viejo no se le pueden enseñar trucos nuevos«. Bueno, esto es una falacia, sobre todo si esos trucos están relacionados con nuestra ciberseguridad. Este concepto, nuevo para muchos, se ha tornado de vital importancia en los últimos años y cada vez forma más parte intrínseca del vocabulario diario. ¿A qué se ha debido? Pues es muy sencillo: el aumento de la ciberdelincuencia.

Esta situación ha provocado un cambio de paradigma a nivel general, especialmente a la hora de llevar a cabo buenas prácticas en las redes. Por desgracia, seguimos cayendo en los mismos errores. 10 costumbres a desechar para mejorar la ciberseguridad.

Ahora bien, ¿Cómo podemos dejar atrás esas costumbres tan feas? Pues muy fácil, siguiendo una sencilla guía de cosas que no debemos hacer y que les describimos en las próximas líneas. Un decálogo que puedes imprimir y colgar en tu zona de trabajo/ocio particular.

A fin de cuentas, la mejor forma de frenar a los ciberdelincuentes es llevar unos hábitos cibersaludables. Cuantas más puertas cerradas se encuentren, menos veces podrán entrar. Dicho esto, vamos a empezar por el primero de todos, y uno muy habitual.

Utilizar software obsoleto

Uno de los errores más comunes que cometemos es contar en nuestro sistema con software obsoleto. Bien porque han salido nuevos programas, o porque la versión del último producto no ha sido actualizada, solemos dejar estas cosas olvidadas. Luego vienen los problemas en forma de, por ejemplo, las vulnerabilidades. Todo software que se precie cuenta con fallos en su código que los ciberdelincuentes pueden explotar en cualquier momento. Las actualizaciones de firmware sirven para «tapar esos agujeros» lo mejor posible y evitar que puedan ser usados en perjuicio de sus usuarios. Así pues, nunca está de más comprobar si tenemos el último firmware instalado; en caso contrario, lo tenemos que actualizar en el acto, especialmente si aún contamos con la versión 1.0 y el producto va ya por la 10.0...

Tener una mala higiene de contraseñas

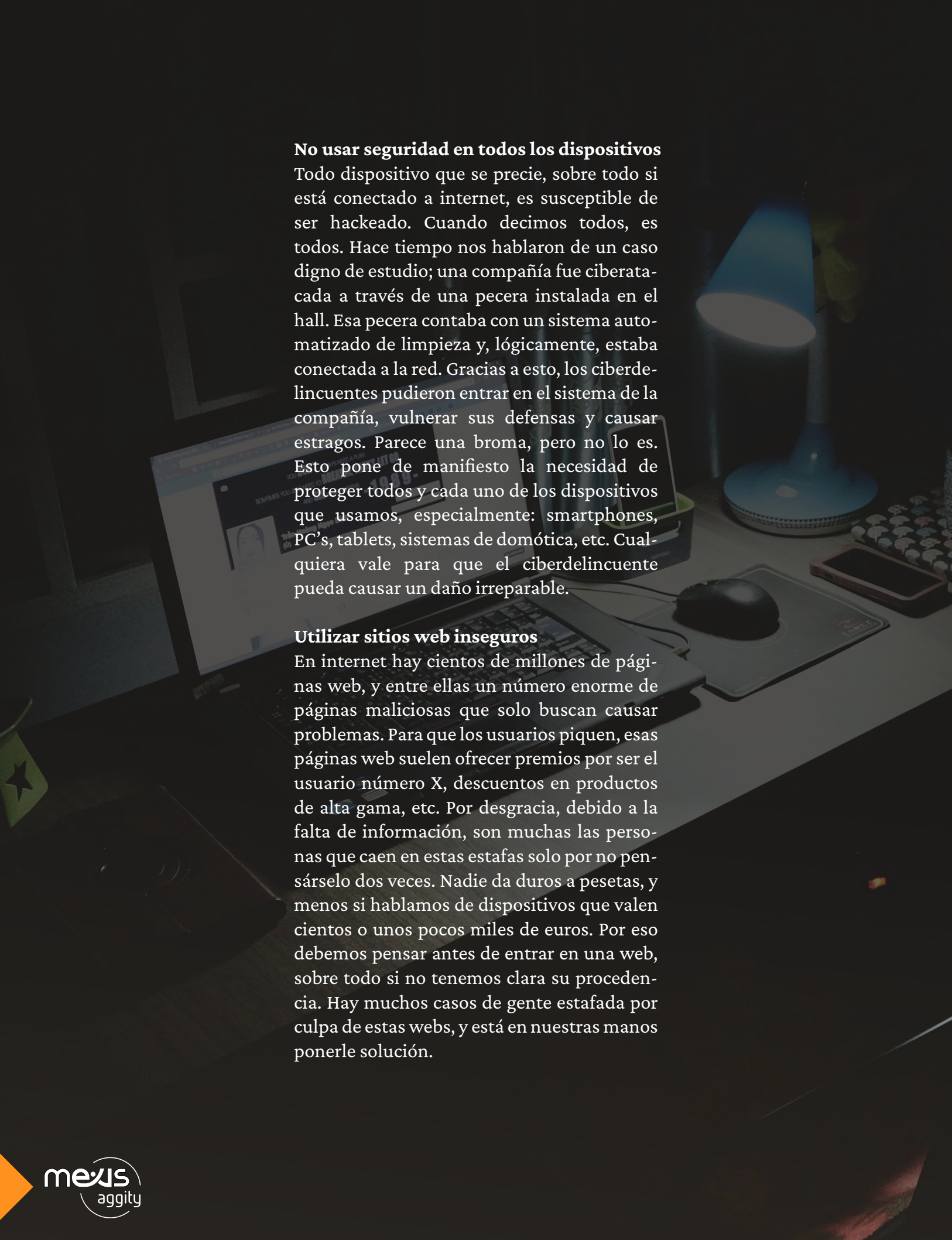
Otra mala costumbre muy común, y que sigue causando problemas año sí y año también, son las contraseñas débiles. No nos cansaremos jamás de repetirlo, pero 1234567890 no es una contraseña segura; nuestro nombre, el de nuestra pareja o el de nuestra mascota tampoco lo es. Tampoco es seguro estar con la misma contraseña durante años; a fin de cuentas, toda contraseña puede ser descubierta en cualquier momento. Su nivel de seguridad ha ido cayendo con el tiempo, sobre todo por nuestras malas prácticas. ¿Qué se recomienda entonces para solventar este problema? Pues muy sencillo. Cambiar de contraseña cada cierto tiempo (un mes, dos meses), hacer uso de contraseñas que incluyan letras, números y símbolos que no sean excesivamente largas. 10 costumbres a desechar en 2022 para mejorar la ciberseguridad.

Conectarse a Wi-Fi público

El Wi-Fi público, el cual podemos encontrar en centros comerciales y otras zonas, permite a los usuarios de smartphone no tener que usar los datos móviles. Pero claro, no todas las redes Wi-Fi públicas cuentan la seguridad que deberían. Los ciberdelincuentes, que se las saben todas, pueden andar cercar y crear una cuenta Wi-Fi alternativa con el mismo nombre para que los usuarios se conecten. ¿Qué pasaría si un usuario se conectara a una red Wi-Fi de dudosa procedencia? Uno de los problemas más repetidos es el hackeo del terminal para acceder a apps, datos del usuario, etc. ¿Se recomienda, por ende, no conectarse a este tipo de redes? No, lo que se recomienda es precaución, y si dudamos mejor hace uso de los datos móviles cuando sea necesario.

No pensarlo dos veces antes de hacer clic

Una de las prácticas preferidas de los ciberdelincuentes es el phishing y el smishing. El Phishing, como bien sabemos, es la práctica por la cual el ciberdelincuente intenta acceder a nuestro sistema a través de un e-mail con malware adjunto. En cuanto al Smishing, hablamos del envío de SMS con enlaces a páginas web fraudulentas. A pesar del uso abusivo que se hacen de estas ciberestafas, los usuarios sieguen cayendo en la trampa, sobre todo cuando se uso de cebo a bancos, empresas de mensajería, etc. El cliente, asustado ante el mensaje recibido o el paquete bloqueado, no duda en descargar el archivo adjunto o pinchar en el enlace. Una vez hemos caído en la trampa, los problemas sufridos pueden ser muy variados: hackeo del dispositivo infectado, robo de información, toma de control del sistema...



No usar seguridad en todos los dispositivos

Todo dispositivo que se precie, sobre todo si está conectado a internet, es susceptible de ser hackeado. Cuando decimos todos, es todos. Hace tiempo nos hablaron de un caso digno de estudio; una compañía fue ciberatacada a través de una pecera instalada en el hall. Esa pecera contaba con un sistema automatizado de limpieza y, lógicamente, estaba conectada a la red. Gracias a esto, los ciberdelincuentes pudieron entrar en el sistema de la compañía, vulnerar sus defensas y causar estragos. Parece una broma, pero no lo es. Esto pone de manifiesto la necesidad de proteger todos y cada uno de los dispositivos que usamos, especialmente: smartphones, PC's, tablets, sistemas de domótica, etc. Cualquiera vale para que el ciberdelincuente pueda causar un daño irreparable.

Utilizar sitios web inseguros

En internet hay cientos de millones de páginas web, y entre ellas un número enorme de páginas maliciosas que solo buscan causar problemas. Para que los usuarios piquen, esas páginas web suelen ofrecer premios por ser el usuario número X, descuentos en productos de alta gama, etc. Por desgracia, debido a la falta de información, son muchas las personas que caen en estas estafas solo por no pensárselo dos veces. Nadie da duros a pesetas, y menos si hablamos de dispositivos que valen cientos o unos pocos miles de euros. Por eso debemos pensar antes de entrar en una web, sobre todo si no tenemos clara su procedencia. Hay muchos casos de gente estafada por culpa de estas webs, y está en nuestras manos ponerle solución.

Compartir el trabajo y la vida personal

Cada vez es más complicado separar la vida laboral de la vida privada por culpa de los dispositivos. Muchos usamos los smartphones para todo: tenemos contactos de familiares y amigos, pero también de compañeros de trabajo o clientes. Este error se repite más y más, y no tenemos en cuenta que el dispositivo que usamos para todo podría no contar con las medidas de seguridad necesarias. Si nuestro smartphone u ordenador personal es hackeado, y en ellos tenemos todo lo mencionado con anterioridad, el problema al que nos enfrentamos es de una gravedad extrema. Se trata de una situación que, por desgracia, se repite cada vez más en muchos ámbitos ya que vivimos conectados las 24 horas. Nos cuesta desconectar, especialmente en trabajos que requieren mucha atención.

Dar información por teléfono.

Las estafas telefónicas siguen estando a la orden del día. Los ciberdelincuentes usan cualquier medio que esté a su alcance para conseguir información de las víctimas. Esto no es nuevo, pero nunca está de más recordar que jamás debemos dar información por teléfono: cuentas de correo electrónico, si tenemos perfiles en redes sociales, a qué nos dedicamos, etc. Quizás sea algo innecesario decirlo, pero tampoco debemos proporcionar contraseñas si nos las piden. Cuanta menos información facilitemos, especialmente si sospechamos de las intenciones del que está al otro lado del apartado, mejor para nosotros. Esto mismo es algo que podemos extrapolar a otros ámbitos, como las redes sociales por ejemplo y donde la Ingeniería Social está muy activa.

No realizar backups

¿Puede un ciberataque borrar todos y cada uno de los datos almacenados en un sistema o servidor? Sí, puede. Es más, uno de los movimientos favoritos de los ciberdelicuentes si una empresa no paga el rescate es borrar los datos; el otro es publicarlo en la red de redes. Este movimiento puede suponer un enorme quebradero de cabeza, especialmente si no posee un backup. No contar con una copia de seguridad de los servidores, por ejemplo, es algo que suele ser bastante común por desgracia. No hablamos ya solo a nivel empresarial, sino también a nivel de usuario. En nuestro dispositivo guardamos fotos, documentos, audios, vídeos y litros contenidos que pueden ser borrados por los ciberdelincuentes. Para evitar perderlos para siempre, lo mejor es realizar un backup y protegerlo en la nube, o un dispositivo externo tipo Memoria USB o HDD.

No proteger su hogar inteligente

La conexión total a internet es algo que ha llegado incluso a los hogares. La domótica, gracias al avance de la tecnología, ha dado un paso gigantesco y cada vez son más los hogares que cuentan con dispositivos capaces de controlar ciertos aparatos. Ahí tenemos a Echo Dot de Amazon, que nos permite encender/apagar la televisión, el aire acondicionado, la luz de diferentes cuartos y más. Estos dispositivos están conectados a internet, por lo que el riesgo de ser ciberatacados a través de ello es bastante elevado. Ya hay casos en los que un ciberdelincuente se vale de las vulnerabilidades de un software para entrar en nuestra casa. Como es evidente, esto nos obliga a extremar las precauciones mientras los estamos usando y protegernos como es debido.

Fuente de información: cybersecuritynews