NEWSLETTER 1

SEGURIDAD DE LOS PROPIOS DISPOSITIVOS: ORDENADOR, TABLETA Y TELÉFONO MÓVIL

El tema de la seguridad en Internet puede dividirse en cuatro partes: la protección de los dispositivos y la red doméstica, las contraseñas, los navegadores y la navegación en redes wifi.

Para cada una de estas categorías, veremos todo lo que se debe hacer para lograr un nivel mínimo de seguridad hasta que el sistema y todos los datos transferidos a través de la web y la red estén completamente protegidos.

1) Seguridad de ordenadores, tabletas o teléfonos móviles

¿Hay un antivirus instalado? ¿El antivirus se actualiza automáticamente cada día?

Si aún no ha instalado un programa antivirus o si tiene un programa caducado que ya no se actualiza, debe tomar medidas.

Desinstale su antivirus actual y descargue uno de los programas antivirus gratuitos recomendados. Para juzgar un antivirus de forma que todo el mundo pueda entenderlo, debemos tener en cuenta al menos 6 parámetros antes de tomar cualquier decisión. De hecho, un buen antivirus:

- No debe ralentizar demasiado el PC y ser ligero en la memoria RAM.

- Debe detener los virus antes de que puedan actuar (escaneo activo residente).

- No debe detectar demasiados falsos positivos, viendo amenazas donde no las hay.

- No debe hacer que el escaneo bajo demanda o el escaneo automático periódico tarden demasiado: un SSD moderno debe ser escaneado completamente en menos de 2 horas.

- Debe actualizarse automáticamente para poder detener las nuevas infecciones de inmediato y evitar el acceso a partes vitales del sistema.

- Debe ser capaz de bloquear el malware no descubierto (amenazas 0-day), detectando la amenaza sólo por el comportamiento sospechoso de ciertos componentes.

Además de estos parámetros, todos ellos muy importantes cuando se trata de un antivirus, también hay que tener en cuenta la facilidad de uso, la interfaz de usuario, los posibles problemas de usabilidad y la presencia de bugs, errores e incompatibilidades.

- ¿Está instalado un cortafuegos?

Si tienes Windows 7 y navegas por Internet con un router en casa, no necesitas un programa cortafuegos. Si lo necesitas, puedes descargar un cortafuegos gratuito para proteger tu red y bloquear las intrusiones.

- ¿Está Windows (o Mac) actualizado y se actualiza automáticamente y con regularidad?

Muchas personas descuidan u olvidan actualizar Windows con los parches que Microsoft distribuye cada semana. Estas actualizaciones son siempre parches de seguridad que cubren los últimos agujeros que permiten a los usuarios malintencionados entrar en los PC desde el exterior y tomar el control.

Comprueba que el servicio de Windows Update está activo en el Panel de Control.

Incluso los usuarios de Mac no deben subestimar las actualizaciones de seguridad.

- ¿Has establecido un plan de copias de seguridad para tus datos, documentos y fotos?

Para asegurarte de que no pierdes los archivos que creas y guardas en tu ordenador, planifica una copia de seguridad automática para tener una doble copia de seguridad.

Si no tienes demasiados datos de los que hacer una copia de seguridad, puede ser mucho más fácil y rápido hacer una copia de seguridad online en servicios de almacenamiento en la nube como Dropbox y Skydrive.

- ¿Mantienes actualizados los programas instalados en tu ordenador?

Al igual que en el caso de Windows, a menudo se publican actualizaciones de seguridad para los programas.

Para aquellos que lo deseen, hay formas de actualizar automáticamente los programas y el software instalado en su ordenador.

- ¿Cuando se descargan programas, ¿se tiene cuidado en el procedimiento de instalación de no instalar también otros programas "recomendados"?

Por desgracia, muchos programas gratuitos vienen con patrocinadores, el llamado "crapware", en forma de programas no solicitados que se instalan automáticamente.

2) Seguridad del navegador

El hecho de que el ordenador, la tableta o el teléfono móvil estén protegidos contra virus e intrusiones externas no garantiza que la navegación siga siendo segura y privada. Puede que a mucha gente no le importe la privacidad, pero la seguridad sigue siendo primordial.

Sea cual sea el navegador que utilices, debe estar actualizado a la última versión y tener activadas las actualizaciones automáticas. Los navegadores que están al día y tienen actualizaciones automáticas son sin duda Chrome, Firefox, Opera y Microsoft Edge.

- Cuando te conectas con una contraseña a un sitio, ¿siempre compruebas que la dirección empieza por https?

HTPPS es el protocolo de conexión encriptada y se diferencia del http normal en que cualquier dato transmitido en https está encriptado. Esto significa que lo que se escribe en https es ilegible para cualquiera, incluidos los operadores de ese sitio.

La extensión del navegador HTTPS Everywhere resalta los sitios seguros y se asegura de que siempre permanezca en HTTPS cuando esté disponible (ver el artículo Navegar en https en sitios bancarios, tiendas online, Facebook con una conexión segura).

- ¿Sabes reconocer, a ojo, los sitios peligrosos en los que hay que tener cuidado con los clics?

Si todavía no puedes distinguir un sitio bueno de uno malo a ojo, y siempre eres paranoico o mal hablado con cualquier sitio que no sea el más popular, entonces puedes instalar algunas extensiones como WOT para evitar hacer clic en enlaces peligrosos y sitios sospechosos

- Cuando te conectas a un sitio desde un ordenador que no utilizas sólo tú, ¿siempre cierras la sesión?

Recuerda siempre cerrar la sesión de todas las cuentas que utilices en un ordenador público o compartido con otras personas, incluidos los miembros de la familia.

- ¿Conoce los fundamentos de las estafas y los fraudes en línea?

Saber qué es el phishing, el malware y otros peligros en Internet y que es importante para mantenerse alejado de ellos.

- ¿Proteges tu navegador del rastreo en línea?

Como ya se ha explicado, no ser rastreado en línea por los sitios web significa bloquear la recogida de datos. Esto es posible a través de ciertas extensiones que puede instalar en su navegador.

El mayor nivel de protección y privacidad en Internet es la navegación anónima. Navegar de forma completamente anónima no es útil para todo el mundo y no se puede hacer en todas las situaciones. Puede ser útil cuando estás haciendo algo ilegal (pero bueno como descargar torrents), cuando no quieres compartir tu ubicación geográfica o cuando quieres falsear tu dirección IP para acceder a sitios bloqueados.

Aunque puedes navegar por Internet de forma anónima de varias maneras, la privacidad en línea sólo está garantizada con el navegador TOR.

3) Seguridad de las contraseñas utilizadas en línea

- ¿Utilizas contraseñas difíciles?

Uno de los errores más comunes de los internautas es utilizar contraseñas simples o que hagan referencia a hechos o acontecimientos de su vida personal. Hay que elegir siempre contraseñas imposibles de descubrir y, sobre todo, generar una contraseña fuerte para todos los sitios web, sin dar a nadie la posibilidad de adivinarla (nunca uses tu fecha de nacimiento, tu equipo favorito o el nombre de tu mujer o tu perro).

- ¿Utilizas una contraseña distinta para cada cosa?

Nunca se debe reutilizar la misma combinación de correo electrónico y contraseña en varios servicios, ya que si un pirata informático consigue entrar en esa cuenta de correo electrónico, podrá vulnerar todas las cuentas personales sin dificultad.

Utiliza un programa para crear y gestionar las contraseñas de las cuentas web.

Cuando sea posible (Dropbox, Google, Gmail y Facebook), se puede utilizar la autenticación de dos factores.

Para mayor protección, asegúrate de comprobar los permisos de las aplicaciones en Facebook y Twitter.

4) Seguridad en la red

- ¿Está su red WiFi doméstica protegida con una clave WPA2?

Si no es así, o si no tienes ni idea de lo que es WPA2, debes saber que WPA son las siglas de Wi-Fi Protected Access y que Wi-Fi Protected Access II (WPA2) y Wi-Fi Protected Access III (WPA3) son tres protocolos de seguridad y programas de certificación desarrollados por la Wi-Fi Alliance para proteger las redes informáticas inalámbricas.

- ¿Eres consciente de que cuando te conectas a una red Wi-Fi abierta, todo lo que haces es visible desde fuera de tu ordenador?

Lo único que protege la seguridad de las contraseñas en internet en una red wifi pública es el protocolo HTTPS mencionado en la primera pregunta del punto dos.

- ¿Has comprobado las carpetas compartidas de tu ordenador?

Como se ha demostrado, hackear ordenadores y ver las carpetas compartidas de otros ordenadores es muy fácil. Muy a menudo la operación tiene éxito porque la gente se olvida de excluir el compatir las carpetas o de todo el disco duro del ordenador. Para utilizar un ordenador en completo anonimato y conectarse a la red sin dejar ningún rastro, se puede utilizar un sistema Linux anónimo y privado como Tails.

La seguridad es importante para todos, desde el técnico experimentado hasta el analfabeto informático. El nivel de precauciones que tomes depende de ti, pero ten en cuenta que la seguridad en línea hoy en día es tan importante (si no más) que la seguridad de tu propia casa.

Este proyecto ha sido financiado con el apoyo de la Comisión Europea. Este documento refleja únicamente las opiniones de los socios del proyecto, y la Comisión no se hace responsable del uso que pueda hacerse de la información contenida en el mismo.