Publicado en Madrid el 07/02/2022

La sociedad debe ser parte de la solución para combatir la ciberdelincuencia

Con motivo de la celebración, este martes 8 de febrero, del Día Internacional de la Internet Segura, la empresa especializada en ciberseguridad S2 Grupo ha destacado que, actualmente, "nos encontramos en un momento complicado en relación a la ciberdelincuencia" y "es muy importante que la sociedad contribuya" a combatirla concienciándose sobre el uso de la tecnología de una forma segura

En un comunicado, S2 Grupo ha resaltado que, en el que un dispositivo está conectado Internet y se descargan apps, es clave tener en cuenta algunas cuestiones críticas de ciberseguridad para evitar caer en las redes de la ciberdelincuencia. “El problema es que la tecnología ha avanzado muy rápido. Ha habido generaciones enteras que no han podido sumarse al cambio. Muchas veces, no tenemos en cuenta o no entendemos cómo se puede abusar de la tecnología y esto es lo que nos puede poner en jaque a la sociedad”, ha declarado José Rosell, socio-director de S2 Grupo.

“Desde el ámbito de la ciberseguridad trabajamos a diario para crear nuevas herramientas que impidan a los ciberdelincuentes acceder a los sistemas conectados online, ya sean de uso doméstico, del sector industrial, sanitario o transportes, por ejemplo. La tecnología se ha metido prácticamente en todos los procesos, desde una cafetera, hasta en un hospital, en los trenes o en los coches. Por ello, necesitamos la ayuda de la sociedad para ganar la batalla a los ciberdelincuentes”, ha afirmado Miguel A. Juan, socio-director de S2 Grupo.

8 consejos para utilizar las apps de una forma segura

Una de las acciones cada vez más comunes es descargar aplicaciones en los dispositivos online para acceder a nuevas funciones, juegos, tiendas de ropa, redes sociales, el banco, etc. En este contexto, S2 Grupo ha señalado algunas pautas que se deben "tener en cuenta para descargarlas de forma segura y evitar ser víctimas del malware":

Ajustar los dispositivos en su configuración para no permitir la instalación de aplicaciones de origen desconocido.- Esta medida sólo permitirá la instalación de apps provenientes de la tienda oficial, lo que otorga mayor seguridad debido a que aquéllas que no son oficiales pueden contener funciones ocultas, como virus.

Actualización de las aplicaciones.- Las actualizaciones de las apps habitualmente responden a mejoras en su sistema de seguridad, por este motivo los expertos de la compañía recomiendan ajustar el dispositivo para que éstas se realicen de forma automática. Para que no se produzca un consumo exagerado de datos, se puede indicar que estas actualizaciones se realicen únicamente cuando el móvil se encuentre conectado a una red wifi.

Revisar periódicamente los permisos concedidos a las redes sociales.- Pueden hacer concesiones para necesidades puntuales y olvidarlo. Esto puede permitir que sus desarrolladores estén leyendo información en silencio durante años.

Preservar la intimidad.- Los permisos más comunes que se da a las apps son leer los archivos (fotos y vídeos), conocer la ubicación del móvil, acceder a los mensajes y correo electrónico, leer los

contactos y escribir y publicar en nombre de su dueño en una red social. Para preservar la intimidad, es recomendable acceder al área de ajustes del teléfono y eliminar aquéllas apps y permisos que sean inadecuados.

Permisos coherentes con la función que la aplicación va a realizar.- Por ejemplo, es normal permitir que Whatsapp acceda a la cámara de fotos o a la tarjeta SD porque es una herramienta de mensajería. Sin embargo, si se instala, una aplicación linterna no es “normal” que solicite el permiso para enviar SMS o realizar llamadas, ya que éstos podrían ser realizados de forma oculta y elevar considerablemente la factura telefónica.

Antes de instalar la app, leer la lista de permisos solicitados.

Una vez instalada revisar en “ajustes” los permisos que realmente se han otorgado.- Es interesante realizar esta comprobación para asegurarse de que coincide con la información facilitada antes de la descarga.

Instalar un antivirus.- Cada año aparecen nuevas variantes de virus destinados a atacar directamente a los teléfonos móviles, por este motivo es esencial tener un antivirus que analice la idoneidad de las apps cada vez que se descarguen.

Datos de contacto:
lununcan Núñez
666666666

Nota de prensa publicada en: Madrid

Categorías: Nacional Sociedad E-Commerce Ciberseguridad