UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

SEGURIDAD DIGITAL

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

Necesidad que tiene cualquier usuario (adulto o menor) de acceder a Internet con las garantías de que se respetan sus derechos.

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

Reglas de seguridad en Internet

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

No publiques algo de lo que te vas a arrepentir

Probablemente la regla más básica. **En Internet nada es efímero**. Si alguien quiere guardar para siempre lo que publicas, encontrará la manera de hacerlo.

Una foto publicada que de mala imagen puede suponer una oportunidad de trabajo pérdida, o burlas durante años.

Una captura de pantalla y esa foto que solo iba a estar en Internet “unos segundos” ha quedado guardada para siempre.

Por no mencionar todo lo que queda guardado en los servidores de las redes sociales.

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

FECYT FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

¿SABES QUE DATOS DAS?

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

Al instalar una app en Android, o cuando la usas por vez primera en iOS, dicha app te pide varios permisos para acceder a distintos datos privados de tu smartphone.

Hay permisos que son lógicos e imprescindibles.

La app de Llamadas necesita permiso para acceder a tu lista de contactos, el reproductor de vídeo necesita permiso para acceder a la tarjeta microSD en donde guardas las vídeos, etc.

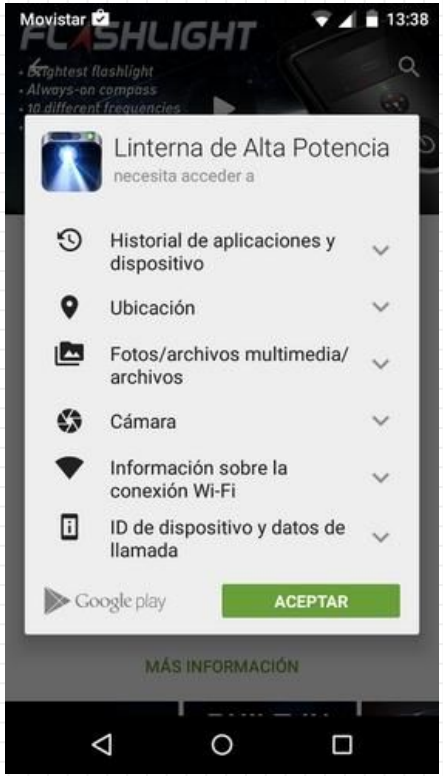
El problema surge cuando **una app pide más permisos** de los que necesita.

Por ejemplo, un app de Linterna sólo necesita acceder a la cámara para usar el Flash.

Sin embargo, esta app Linterna de Alta Potencia que puedes ver aquí, te pide permiso para acceder a tu historial de aplicaciones, ubicación, fotos, vídeos, lista completa de archivos, información sobre WiFi, ID del dispositivos y datos de llamada:

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA



UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

¿Para qué necesita una linterna, cuya función es iluminar, acceder a tus fotos, tus vídeos, tu ubicación, tu historial y tus datos de llamada?

Es la gran trampa de las apps gratuitas. Te ofrecen un caramelo gratis (la linterna) a cambio de extraer datos sobre tí.

No hacen nada ilegal, porque te están pidiendo permiso. Pero se aprovechan de que los usuarios tenemos la mala costumbre de aprobar permisos sin leerlos.

El problema es que **las apps piden permisos para robarnos nuestra privacidad**, pero no nos dicen qué harán con esos datos.

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

¿Podemos defendernos?

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

Instala sólo apps de confianza

En la medida de lo posible, instala apps únicamente de compañías conocidas y contrastadas. No quiere decir que no te espien, seguramente lo hacen, pero sus actividades se reducen al ámbito publicitario, descartando así actividades malignas como robar tus datos bancarios, instalar malware o apuntarte a un servicio Premium.

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

Si hay exceso de permisos, busca alternativas

Cuando instales una app o la uses por primera vez, revisa los permisos antes de aprobarlos. Sólo te llevará unos segundos. Si detectas que pide más permisos de los que necesita, busca una app alternativa que haga lo mismo. Todas las apps tienen alternartivas con la misma función, pero más respetuosas con tu privacidad.

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

Revisa las apps instaladas

Echa un vistazo a los permisos que has dado a las apps que tengas instaladas y desinstala las que abusen. Para ello ve a Ajustes, Aplicaciones, y toca la solapa Instaladas. Entra en una app y desliza hasta abajo para ver los permisos.

UNIVERS
DE GRAN

FECYT FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

FECYT FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

CUIDADO con FREEMIUM y las compras integradas


PILAR Y SU CELULAR
¿Conoces qué son el FREEMIUM y las compras integradas en la app?

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

NO SIEMPRE TODO EL MUNDO ES QUIEN DICE SER

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA

USA DE MANERA RESPONSABLE TU WEBCAM

Una chica navega por Internet mientras chatea con sus amigos por Facebook Messenger. Llegado el momento de irse a dormir, cierra el navegador y los programas de su ordenador.

Sin embargo, justo cuando se está preparando para meterse en la cama, se enciende una pequeña luz verde situada al lado de la webcam.

La chica se da cuenta de ello y se queda mirando a su ordenador con cierta confusión. Al poco tiempo, cae en la cuenta de que alguien ha activado su cámara de forma remota para vigilar lo que hace.

Si te suena esta historia seguramente sea porque eres consciente de que este tipo de cosas suceden en la vida real.

En 2014, algunos hackers rusos crearon una página web que violaba la privacidad de miles de personas de todo el mundo. Se trataba de una plataforma en la que se mostraba las webcams hackeadas de personas que no eran conscientes de que estaban siendo vigiladas.

Periodistas de The Telegraph entraron en esta web y grabaron lo que vieron a través de las cámaras webs de los dispositivos infectados. Se trataba de escenas cotidianas, como por ejemplo, la de una mujer mayor que dormía en su salón mientras los niños veían la televisión. Afortunadamente, la web fue cerrada a finales de 2014.

¿Por qué querrían hackear tu webcam?

Hay muchos motivos por los cuales los hackers accederían a un ordenador para poner en marcha la webcam del usuario sin su permiso.

Sin embargo, en la mayoría de casos que han llamado la atención de los medios, los hackers buscan lucrarse ilegalmente y usar ese contenido de forma malintencionada.

Cómo hackean tu ordenador

Una Herramienta de Administrador en Remoto (RAT) es un programa que permite operar con el sistema de un ordenador como si el usuario estuviera sentado frente a él.

Generalmente, este tipo de herramientas es utilizado por criminales o personas con malas intenciones, ya que un RAT es instalado en un dispositivo sin el consentimiento del usuario, de ahí que también se conozcan los RATs como Troyanos de Acceso Remoto.

Se pueden descargar de forma muy sencilla haciendo una simple búsqueda en Internet. También se encuentran en programas de intercambio de archivos P2P (Peer-to-Peer) como LimeWire, o en protocolos P2P como BitTorrent y Freenet.

Botnets

En los últimos años, el término botnet también se ha utilizado para referirse a una red privada de ordenadores que han sido infectados con un virus y pueden ser controlados en grupo. El artífice del botnet puede controlar esta red a través de la infraestructura mando y control (C&C en inglés).

El creador del botnet es el que toma el control de los ordenadores una vez la seguridad de estos ha sido comprometida a través de un malware.

El ataque DDoS que tuvo lugar en 2016 fue llevado a cabo por el botnet Mirai, un malware que convertía a los dispositivos que tenían versiones desactualizadas de Linux en un bot controlado en remoto. Dyn, proveedor de servicios de sistema de nombres de dominio, calificó el botnet Mirai como la fuente principal de este malicioso ataque.

Código malicioso

Si utilizas un ordenador cuyo antivirus o sistema operativo no están actualizados, entonces cualquiera podría hackearlo fácilmente mediante código malicioso.

Este puede tratarse de un script o un programa del sistema que tratará de causar brechas de seguridad y con ello, resultados no deseados.

Si tu ordenador opera con aplicaciones que no han sido actualizadas y accedes a una aplicación web que contiene código malicioso, entonces un hacker podría incrustar este código y tomar el control de tu ordenador, así como de la webcam.

Cómo evitar que tu cámara web sea hackeada

Mantén tus aplicaciones actualizadas

Tal y como se ha visto a través del método de la infección de código malicioso, actualizar los programas que tienes instalados en tus dispositivos es una manera de minimizar los riesgos de que tu webcam termine siendo hackeada.

Tener un buen antivirus o un cortafuegos es clave para que tu ordenador no sea infectado por un RAT, un malware, o cualquier tipo de programa que comprometa el control de tu webcam.

Cubre tu cámara web o desconéctala

Una de las maneras definitivas de evitar que los hackers tomen imágenes de ti a través de tu webcam es cubriéndola con cinta o desconectándola de tu ordenador en caso de que sea externa.

Si tu cámara web está integrada a tu ordenador y la luz LED comienza a encenderse sin ninguna razón, cúbrela inmediatamente o desconecta tu ordenador de Internet.

Modifica la configuración de tu webcam

Con algunas habilidades técnicas, puedes modificar la configuración de tu cámara web a través de su aplicación y restringir que, direcciones IP ajenas a ti, accedan a tu webcam sin tu autorización.

Trabajar con una VPN, o con un proxy más seguro que una VPN, también puede minimizar los riesgos de que tu cámara web sea hackeada. Además, tener una contraseña segura en cada aplicación, protocolo o/y proxy implementado son detalles que aumentarán tu protección.

SENTIDO COMÚN

- NO ENTRAR EN PÁGINAS WEB “SOSPECHOSAS”

- DESCONFIAR DE PROGRAMAS “SOSPECHOSOS”

UNIVERSIDAD DE GRANADA

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · FECYT · FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA