ENJOY SAFER TECHNOLOGY™

GUÍA DE

Privacidad en Internet

Lucas Paus
Security Reasearcher

Introducción

En los últimos años fuimos testigos de la migración hacia la Web 2.0 que, junto con el avance vertiginoso de la tecnología, permitió a los usuarios subir y compartir todo tipo de contenidos. Esta actividad ganó cada vez más popularidad, principalmente con la aparición de las Redes Sociales que posibilitan subir información a Internet tales como ubicaciones, fotos o datos personales, desde una computadora o un dispositivo móvil. De la misma manera, es posible manejar cuentas bancarias e, incluso, realizar transacciones comerciales.

En este sentido, la gran concentración de información sensible que se encuentra disponible en Internet puede convertir a un usuario en una potencial victima si no se toman los recaudos necesarios. **En esta línea, realizamos esta guía que ayudará a prevenir distintos tipos de incidentes relacionados con la privacidad, la Ingeniería Social y el robo de información.**

Índice

Qué es la privacidad

“

La privacidad es aquello que se lleva a cabo en un ámbito reservado; en Internet podría entenderse como el control que ejercemos sobre nuestra información para limitar la cantidad de personas autorizadas a verla. Esto incluye datos personales, fotografías, documentos, etc.”

Internet y la privacidad

Internet es una herramienta que permite, en conjunto con otras, la interacción entre dos o más personas. Dicha característica se ve reflejada en sitios como Facebook y Twitter, Redes Sociales en donde las personas suelen compartir públicamente sentimientos, ideas, opiniones, noticias, fotografías, videos, etc. Si bien esto forma parte de la interacción social normal que se da en la actualidad, es necesario considerar que Internet es un espacio abierto al mundo, por lo tanto, cualquier acción que se haga puede tener un impacto global y permanente. Por ejemplo, alguna publicación de la cual una persona pueda arrepentirse (como una fotografía u opinión) no solo podrá ser vista por millones de usuarios, sino que también será prácticamente imposible de borrar completamente de la red.

También puede resultar peligroso publicar datos que puedan identificar a una persona como dirección, teléfonos, lugar de estudio o trabajo, días de vacaciones, etc. Esto puede resultar todavía más complicado si se posee una gran lista de amigos que no son conocidos personalmente. Por todo lo que se ha mencionado, es de suma importancia que antes de publicar algo, cada persona piense en las consecuencias que puede conllevar divulgar información sensible en sitios públicos y de los cuales no siempre se tiene un control directo.

Producto del gran alcance, masividad, y otras características de Internet, es necesario comprender qué es la privacidad y cómo poder aplicarla correctamente.

Amenazas

I - Oversharing

II - Protocolos inseguros

III - Códigos Maliciosos

Amenazas que afectan a la privacidad

Podemos reconocer tres tipos de situaciones que amenazan o ponen en riesgo directo a la privacidad de la información. A continuación, mencionamos cada uno y a lo largo de toda la guía los detallaremos con mayor profundidad:

I

Oversharing: se da al compartir de manera desmedida la información. Se ve comunmente en Redes Sociales, y con la ayuda de los smartphones cada dia se hace mas notorio. A la hora de planificar un ataque, un ciberdelincuente se puede nutrir de múltiples datos, desde una ubicacion- como lugares donde se es habitué o la oficina donde se trabaja- hasta detalles de los contactos y amigos. Por esta razón, cuanto más se comparta, más expuesto se estará.

II

Protocolos inseguros: se relaciona con la seguridad en la comunicación de las aplicaciones. En muchas ocaciones utilizamos protocolos que realmente no ponen el foco en mantener la seguridad y privacidad de los usuarios, sino que prevalecen otras cuestiones como la funcionalidad y simplicidad en su uso, dejando muchas veces expuesta informacion sensible a manos de posibles atacantes.

III

Códigos maliciosos y phishing: desde hace ya bastante tiempo, los cibercriminales generan códigos maliciosos con el fin de robar información financiera y credenciales de Redes Sociales para propagar campañas maliciosas en nombre de las víctimas. Asimismo, espían el comportamiento de navegacion de las personas, de modo que pueden generar spam personalizado teniendo en cuenta los sitios y ofertas que más se visitan.

Por otra parte, se encuentran los sitios apócrifos conocidos como phishing, que roban las credenciales de usuarios distraídos que las ingresan pensando que se encuentran en un sitio real. Sin embargo, estos datos viajan al atacante quien gana acceso a las cuentas de las víctimas atentando contra su privacidad y muchas veces realizando actos fraudulentos.

Oversharing

I

Conceptos generales en Redes Sociales

Las configuraciones en las Redes Sociales no tienen, por defecto, los niveles más elevados en cuanto a la protección y a la seguridad. Por lo tanto, es recomendable dedicar un tiempo prudencial a cambiarlas y, además, revisar de forma periódica cuáles son las posibles fugas de información ante una mala o incorrecta configuración de la privacidad en la plataforma.

Revisemos cómo hacerlo en las principales Facebook, YouTube y Twitter:

Facebook

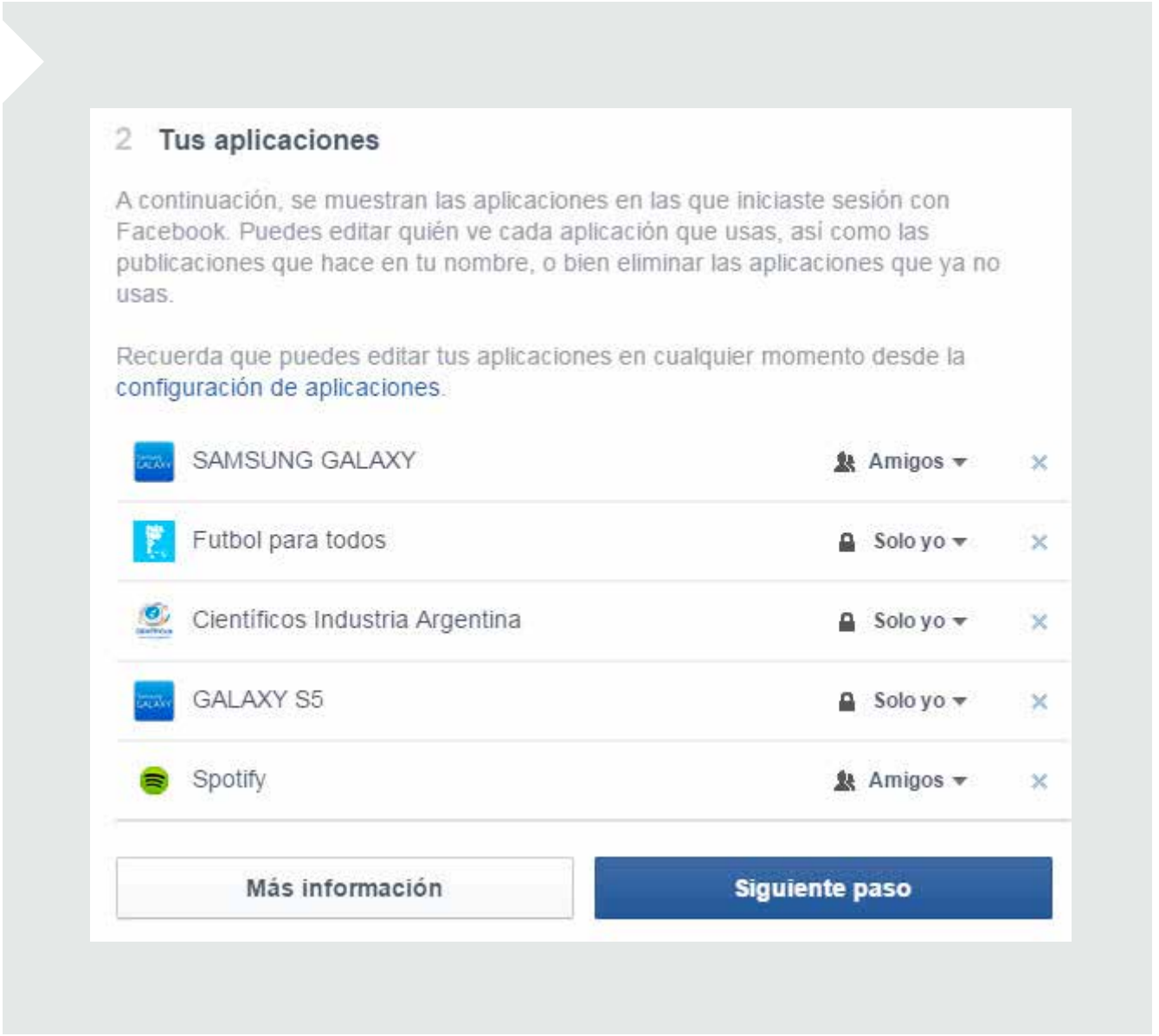
① En el margen superior derecho de la aplicación podremos encontrar el icono en forma de candado, el cual nos servirá para revisar de forma sencilla la privacidad del perfil, tal como se ve en la siguiente imagen:

②

Es importante revisar con quién se comparten las publicaciones, es decir, **qué público tendrá acceso a la información**. Esto es vital, por lo que recomendamos compartir la información siempre con los amigos y, en lo posible, tenerlos clasificados por grupos, como colegio o club. En la siguiente imagen podremos identificar cómo cambiar la configuración por defecto y compartir contenidos solo entre amigos.

3

La siguiente operación es decidir **qué aplicaciones tienen acceso al perfil**, ya que muchas podrían publicar información en nombre del usuario, por lo que es vital que se lean y asignen detenidamente los controles de permisos. En la pantalla siguiente observamos cómo podemos restringir los grupos de usuarios que verán los mensajes de las aplicaciones desde el perfil:



④

Este paso está relacionado con **la información personal que se comparte directamente en el perfil**. En este punto, es importante considerar el fin específico de compartir datos como la dirección, el teléfono o el correo electrónico. Como dijimos anteriormente, **se debe tener en cuenta que a mayor información personal compartida, mayor será el riesgo a sufrir ataques**, como por ejemplo de Ingeniera Social.

5

De este modo, **hemos finalizado el proceso de comprobación rápida de la privacidad en un perfil de Facebook.**

Ya vimos cómo en **5 pasos un usuario podrá revisar los parámetros y niveles de privacidad**, sin embargo, si se quiere realizar un análisis más profundo, debemos tener en cuenta las siguientes opciones desde el menú de configuración:

Desde este punto, Facebook permite elegir las siguientes opciones, tal como se ve en la imagen posterior:

- Quién puede ver las publicaciones por defecto
- Revisión de las publicaciones que puedan etiquetar a un usuario.
- Quién puede ponerse en contacto con el usuario, específicamente sobre solicitudes de amistad y mensajes privados.
- Quién puede buscar a un usuario, precisamente configurando parámetros como direcciones de correos, números de teléfonos o motores de búsqueda que puedan relacionarse con el perfil.

Recomendamos usar la opción "solo amigos"

Por otra parte, desde la pestaña "Biografía" y "Etiquetado" se podrán configurar cuestiones que también están vinculadas con la Privacidad. Algunas de ellas son: poder etiquetar a un usuario, quién verá las etiquetas, la opción de que otros usuarios puedan escribir sobre el muro propio e, inclusive, recibir sugerencias sobre etiquetas. Si bien cada configuración puede ser personalizada para cada perfil, recomendamos que se utilice la imagen siguiente como guía:

Configuración de biografía y etiquetado

¿Quién puede agregar contenido a mi biografía?	¿Quién puede publicar en tu biografía?	**Solo yo**	Editar
	¿Quieres revisar las publicaciones en las que tus amigos te etiquetan antes de que aparezcan en tu biografía?	**Activado**	Editar
¿Quién puede ver contenido en mi biografía?	Comprueba lo que ven otras personas en tu biografía		Ver como
	¿Quién puede ver las publicaciones en las que te etiquetaron en tu biografía?	**Solo yo**	Editar
	¿Quién puede ver lo que otros publican en tu biografía?	**Solo yo**	Editar
¿Cómo puedo administrar las etiquetas que otros agregan y las sugerencias de etiquetas?	¿Quieres revisar las etiquetas que otros agregan a tus publicaciones antes de que aparezcan en Facebook?	**Activado**	Editar
	Cuando se te etiqueta en una publicación, ¿a quién quieres agregar en el público que la ve, si aún no está incluido?	**Solo yo**	Editar
	¿Quién recibe sugerencias para etiquetarte en fotos en las que parece que estás presente?	**Nadie**	Editar

Twitter

Twitter es otra Red Social muy utilizada, vinculada a los smartphones desde su nacimiento, que permite mejorar la privacidad de los usuarios mediante algunos paneles que veremos a continuación:

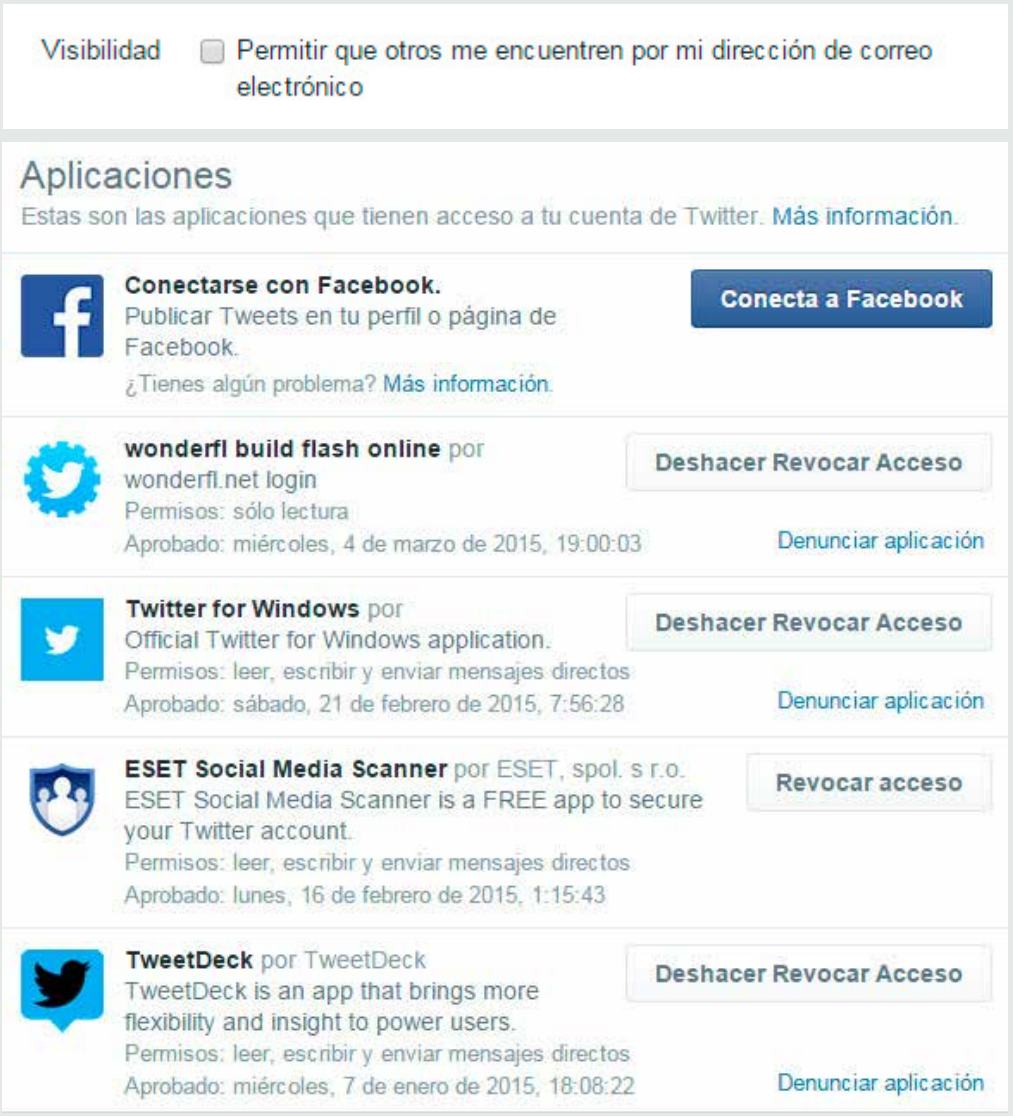
①

Dentro de la pestaña "Privacidad", se podrá seleccionar la opción de no permitir que lo etiqueten a uno en su cuenta, de dejar visibles los tuits solo para personas que se encuentren en la lista de contactos e inclusive no develar la ubicación geográfica desde donde se tuiteó. A continuación, se ven los menús de cada opción:

2

Además, podremos personalizar la opción de no permitir que el usuario sea encontrando por su dirección de e-mail, tal como se ve a continuación:

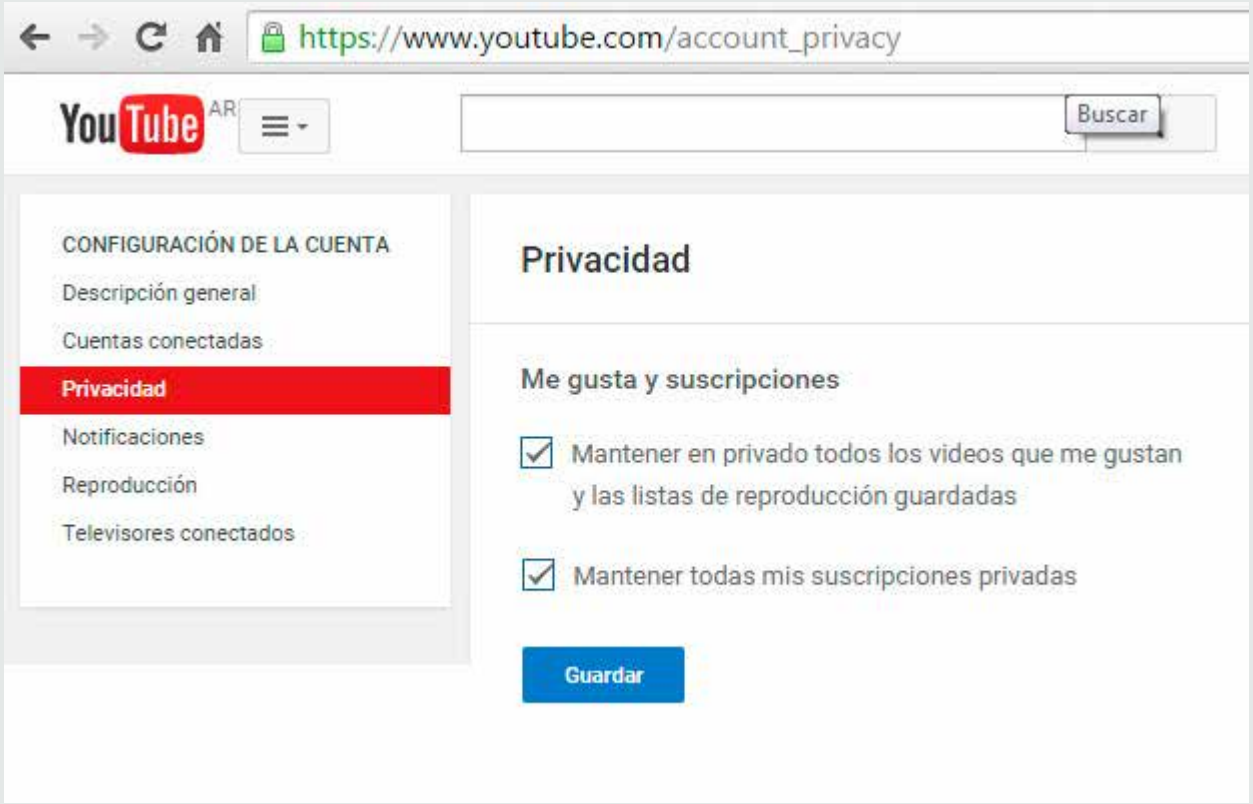
Como en el caso de Facebook, en Twitter tambien es recomendable verificar qué aplicaciones tienen acesso a el perfil de usuario. Es aconsejable revocar o desaher acceso a las aplicaciones que se vean sospechosas o sean directamente desconocidas.



YouTube

Para finalizar, veamos el último ejemplo con YouTube, una Red Social que nos permite subir videos y compartirlos. Como se pueden ver en la siguiente imagen, el usuario tiene la opción de mantener en privado los videos, las listas de reproducción e, inclusive, las suscripciones a otros canales:

Además, **si se realizan videos propios, siempre es importante tener cuidado con la información personal que se puede llegar a revelar en los mismos** y que ello no sea una puerta abierta para se contactado a través de otra red social con el objetivo de recabar más información por parte de un atacante. Asimismo, t**ambién hay que ser cuidadoso con los comentarios que se incluyen en los videos en los que se invita a visitar sitios webs de dudosa reputación** y que podrían valerse de los intereses del usuario que crea el video.



Metadatos

Comúnmente, se define a los metadatos como un conjunto de datos sobre datos. Si lo llevamos a la vida diaria, un ejemplo podría ser el siguiente: si el dato en cuestión es un libro, la ficha que podríamos tener sobre ese libro en una biblioteca serían los metadatos, es decir, su autor, fecha de publicación, editorial y demás especificaciones del libro (dato).

Para el caso de **archivos como fotos, musica y documentos de ofimática, estos archivos también traen consigo metadatos que, en muchas ocasiones, servirán para buscar un archivo creado en una fecha específica, de un autor preciso e inclusive saber con qué calidad se encuentra un archivo de audio.**

Sin embargo, hay veces en las cuales a través de imágenes se puede conocer una posición geográfica (mediante coordenadas GPS) en el caso de los smartphones, o subiendo algún archivo de ofimática a la nube se puede ver el nombre de usuario de un equipo. Es por esto que se debe tener un cuidado especial entendiendo que la información que se sube a Internet puede contener (o brindar) más datos que meramente lo que se ve en una foto o se muestra en un archivo.

Si bien en la actualidad la mayoría de las Redes Sociales elimina los metadatos, no se puede saber a ciencia cierta si futuras redes también lo harán, por lo cual nos parece importante resaltar su existencia y los posibles peligros que traen aparejados.
Para mayor información se pueden consultar los siguientes posts de WeLiveSecurity:
"Metadatos: tus fotos podrían mostrar más de lo que ves"
"¿Qué información ocultan los documentos que imprimes?"

Protocolos inseguros

II

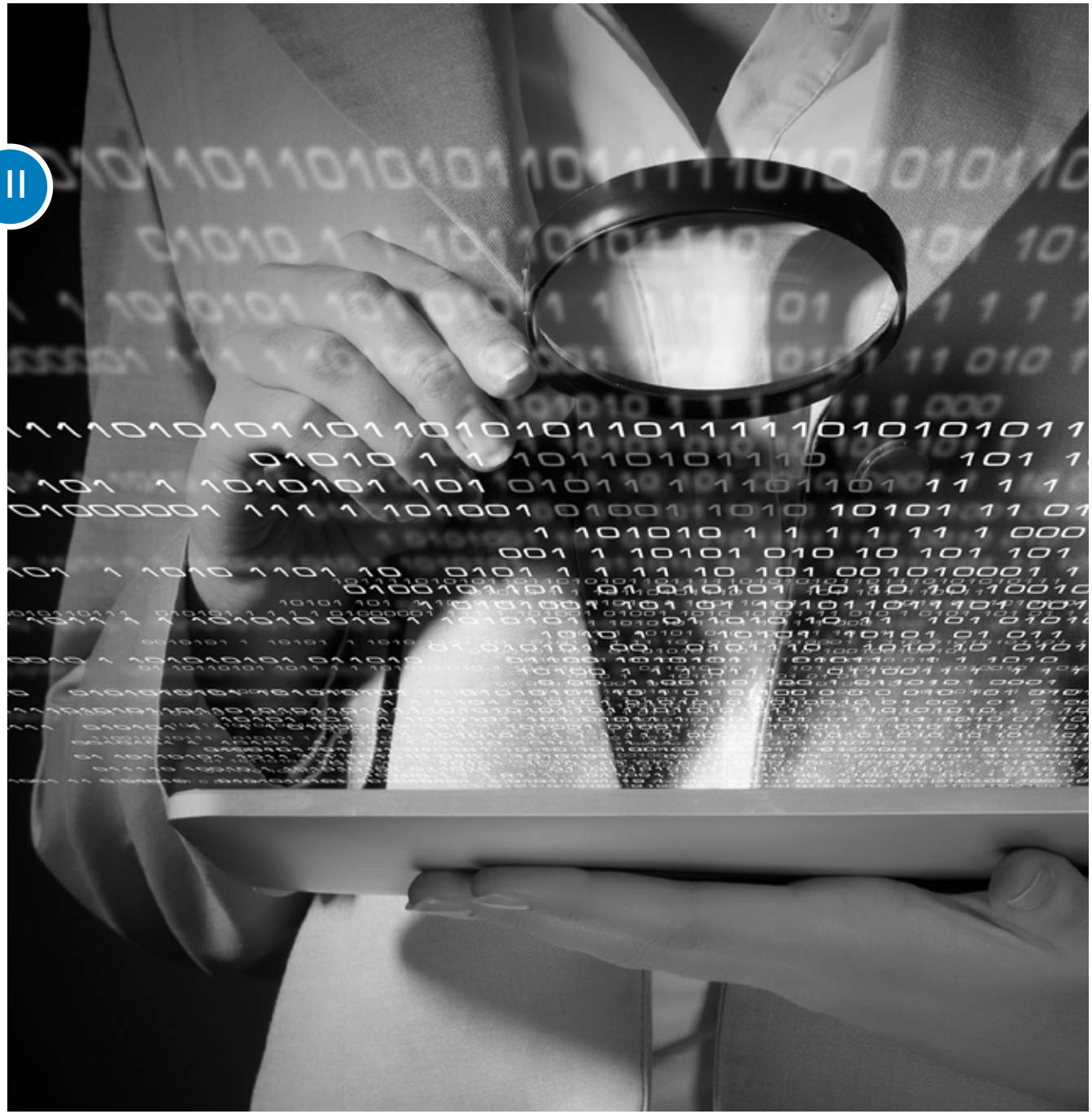
Precaución al conectarse en redes públicas

Cada vez que el usuario se conecta a una red inalámbrica Wi-Fi, Windows o algunos firewalls preguntan si se trata de una red hogareña, corporativa o pública. Es importante, como primera medida, seleccionar siempre "red pública", para que se adopten configuraciones más restrictivas de seguridad, especialmente en lo que respecta a archivos compartidos y acceso al sistema. Si no se tienen en cuenta los controles de seguridad pertinentes, es recomendable evitar el uso de servicios que requieran de información sensible en conexiones inalámbricas compartidas o públicas.

Además, se debe tener en cuenta que al conectarse a redes de terceros, no se conocen a las otras personas que estén conectadas a la misma red ni sus intenciones, por lo tanto, se deben tomar los mismo recaudos que se tomarían en redes públicas.

Códigos maliciosos

III



Códigos Maliciosos

Durante estos últimos meses hemos identificado diversos ataques que utilizan a las Redes Sociales como métodos de propagación; sin embargo, los métodos clásicos de infección, como el envío de correos maliciosos, todavía están a la orden del día y, en conjunto con técnicas de Ingeniería Social, siguen engañando a los usuarios para lograr infectarlo con malware.

La aparicion de codigos maliciosos en Smartphones ya no es una novedad, y de a poco se van convirtiendo en una de las plataformas con mayor crecimiento para el cibercrimen. Android encabeza el ranking de mayor amenazas encontradas vinculadas a codigos maliciosos, sin embargo, todas las plataformas mobile están en mayor o menor medida expuestas al malware que se propaga en Internet y en repositorios de aplicaciones no oficiales.

Ademas, la aparición de nuevos tipos de campañas de propopagacion de botnets, troyanos o keyloggers que pueden verse ligadas a noticias actuales o personajes populares son utilizados como señuelos para atraer la atencion de sus victimas.

Con este tipo de infecciones, los ciberdelincuentes adquieren acceso a las claves personales e información sensible contenida en los equipos de las víctimas. En este sentido, utilizando una solución completa de seguridad es posible prevenir proactivamente las infecciones contra distintos tipos de malware y, de este modo, cuidar la privacidad de los datos. Para que esta barrera sea eficaz, es de vital importancia mantener actualizado el sistema

operativo, las aplicaciones que se utilicen y, por supuesto, la solución de seguridad.

Consejos para cuidar la privacidad en Internet

En la seguridad no existe una sola regla de oro para protegerse contra todos los posibles incidentes que puedan afectar la privacidad, sin embargo, teniendo en cuenta los diez siguientes consejos es posible minizar en gran medida los riesgos de ser víctima de este tipo de ataques:

- Evitar ingresar en enlaces sospechosos o a sitios web de dudosa reputación.
- Evitar utilizar sitios que manejen informacion sensible sin el candado de seguridad (HTTPS).
- Evitar realizar operaciones financieras o manejar las redes sociales desde redes Wi-Fi abiertas.
- Evitar el ingreso de información personal en formularios de dudoso origen.
- Utilizar y mantener siempre actualizada la solución de seguridad.
- Actualizar el sistema operativo y las aplicaciones periodicamente.
- Tomarse el tiempo para configurar correctamente la privacidad de las cuentas en las Redes Sociales.
- Aceptar solo contactos conocidos y evitar el exceso de información en el perfil.
- Descargar aplicaciones desde sitios web y repositorios oficiales.
- Evitar la ejecución de archivos sospechosos provenientes de correos electrónicos.

Conclusiones

A lo largo de esta guía, se profundizó en **la importancia de contar con un manejo óptimo de la información que se comparte en las Redes Sociales**. Siendo conscientes de los peligros de no manejar correctamente la privacidad y modificando los perfiles por defecto, se contará con una capa más de protección en las plataformas contribuyendo, así, a la protección de la información.

Teniendo en cuenta que cada vez se maneja más información sensible en las cuentas, resulta lógico que los cibercriminales destinen mayores recursos a la investigación y generación de códigos maliciosos para robar las credenciales, conseguir acceso a la información del perfil y, finalmente, tener una base más robusta para sus ataques de Ingeniería Social.

Desde el punto de vista técnico, **es posible reducir este tipo de ataques, siempre y cuando se cuente con la participación y el compromiso de los usuarios en todo el proceso de protección, sobre todo para evitar incidentes ligados a temas de privacidad**. Para solucionar este inconveniente es necesario que todos comprendan la importancia del cuidado de la privacidad como método de protección. Aprendiendo a configurar distintos servicios y aplicaciones disponibles en Internet de manera correcta los datos no solo estarán más seguros, sino que también se podrá disfrutar más de la tecnología y todo lo que tiene para ofrecer.

www.eset-la.com

/esetla

@esetla

/company/eset-latinoamerica