AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación

Riesgos de seguridad derivados del uso de redes sociales

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-2036-120515*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*15/05/2012*
N° de Páginas	*1 de 11*

1 TABLA DE CONTENIDOS

2 OBJETO

El objeto de este documento es proporcionar al personal de la Junta de Andalucía recomendaciones para un uso seguro de las redes sociales. Llevar a la práctica los puntos que en este documento se citan evitará en gran medida que nos veamos afectados por las múltiples amenazas a las que estamos expuestos cuando hacemos uso de las redes sociales.

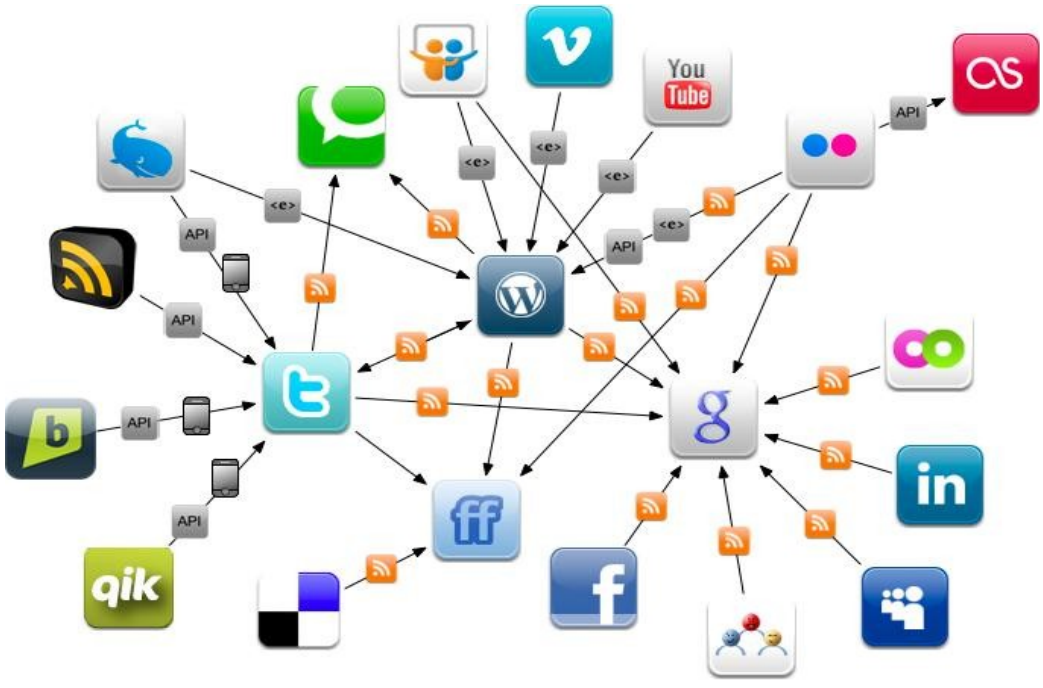
3 ALCANCE

El documento va destinado al personal de la Junta de Andalucía y público en general.

4 INTRODUCCIÓN

Las redes sociales, a día de hoy, forman parte de los hábitos cotidianos de navegación de los usuarios. Cualquier usuario de Internet hace uso de, al menos, una red social y muchos de ellos participan activamente en varias de ellas. Para muchos usuarios (especialmente los más jóvenes), las redes sociales son el principal motivo para conectarse a Internet.

Sin embargo, a partir de su uso, los usuarios se ven expuestos a un conjunto de amenazas informáticas, que pueden atentar contra su información, la propia integridad del usuario o incluso su dinero. Ante la creciente tendencia de los ataques informáticos a utilizar las redes sociales como medio para su desarrollo, se vuelve de vital importancia para el usuario estar protegido y contar con un entorno seguro al momento de utilizarlas.



- ¿Cuáles son las principales amenazas?
- ¿Qué podemos hacer para que no nos veamos amenazados mientras las usamos?

El presente informe les ayudará a conocer mejor algunas de las principales amenazas a las que estamos expuestos cuando hacemos uso de redes sociales, y les proporcionará consejos y recomendaciones para evitar que nos veamos afectados por ellas.

4.1 Redes sociales mas populares

4.1.1 Facebook

Es la red social mas popular del mundo. Según los datos publicados, en Abril de 2012 cuenta con más de 900 millones de usuarios. Originariamente estaba orientada a los jóvenes, pero actualmente su uso se expande por todas las generaciones, e incluso por el mundo empresarial.

4.1.2 Twitter

Se trata de una red social de microblogging. Con 200 millones de usuarios, es la red social que actualmente está experimentando un mayor crecimiento.

4.1.3 Tuenti

Tuenti es una red social española, orientada principalmente al público adolescente. A fecha de febrero de 2012, Tuenti tiene más de 13 millones de usuarios, obteniendo un crecimiento del 33% en el último año.

4.1.4 MySpace

Es una de las primeras redes sociales, lanzada en 2003, siendo en sus comienzos una de las más populares. Está principalmente orientada a la música. A finales de 2011 contaba con 30 millones de usuarios.

4.1.5 Google+

Es una de las últimas redes sociales incorporadas al mercado. Fue lanzada en Junio de 2011 por Google y actualmente cuenta con mas de 170 millones de usuarios. Google+ intenta seguirle los pasos a Facebook, aunque actualmente sigue estando por detrás de ésta.

4.1.6 LinkedIn

Red social orientada a las relaciones laborales y los negocios. Cuenta con mas de 100 millones de usuarios. En LinkedIn podemos crearnos un perfil con nuestro currículum y comenzar conectarnos con gente de nuestro entorno laboral. Conectarnos y hacer lazos, amistades en el entorno empresarial o buscar nuevas ideas o proyectos.

5 PRINCIPALES AMENAZAS EN REDES SOCIALES

5.1 Amenazas clásicas: Phishing, spam y malware

Las redes sociales se suman a los medios de comunicación ya existentes en Internet (e-mail, chat, foros, ...), y por tanto son igualmente vulnerables a las amenazas que afectan a éstos.

A través de las redes sociales se puede enviar SPAM, en formato de publicaciones basura que llenan nuestro espacio personal (muro, timeline, ...) de información no solicitada. De la misma forma, se puede distribuir malware a través de enlaces y se puede realizar phishing suplantando identidades con el fin de engañar a los usuarios y obtener información u obligarle a que realice una cierta acción.

5.2 Robo de información

A diario, los usuarios suben información a las redes sociales. En muchos casos esta información es de carácter personal (fotos, situación laboral, domicilio, creencias religiosas, políticas, etc).

Compartir demasiada información sobre ti mismo (bien seas tu el que la comparta o tus amigos) puede convertirse en un problema si permitimos que toda esta información pueda ser accedida por cualquier persona del mundo ya que podría ser aprovechada para involucrarnos en situaciones no deseadas o usada por terceros para fines no deseados. Algunos peligros de exponer demasiada información sobre ti son:

- **Daño a tu carrera**: Publicar información embarazosa puede dañar tu futuro profesional. Muchas organizaciones (organismo públicos, empresas, universidades, etc), como parte de la revisión de antecedentes de un nuevo candidato a una plaza, consultan en las redes sociales todo lo que haya sido publicado por esa persona. Cualquier publicación embarazosa, sin importar su antigüedad, podría evitar que obtuvieses la plaza buscada.
- **Ataques en tu contra**: Los ciberdelincuentes pueden recolectar tu información con el fin de que un ataque contra ti sea mas sencillo. Por ejemplo, la información recolectada podría ayudarles a adivinar la respuesta de una "pregunta secreta" usada por un sitio web para restablecer la contraseña.
- **Ataques contra la adminsitración**: Cuando un atacante prepara una ataque contra algún organismo de la administración pública, y necesita información previa, puede obtenerla a través de lo que sus empleados publican en las redes sociales. Por otra parte, una actividad en línea irresponsable por tu parte puede dar lugar a una mala imagen de tu organismo.

El robo de información en redes sociales es considerado como robo de identidad, uno de los delitos informáticos mas creciente de los últimos años. Los vectores de ataque mas usados para el robo de información en redes sociales son:

- **Ingeniería Social**: El contacto directo con el usuario víctima para obtener información es uno de los métodos mas comunes. Una conversación "amistosa" a través de los canales que ofrece una red social puede convertirse en una fuente de información sensible para un atacante.

- **Información pública**: Una mala configuración de las redes sociales puede permitir que información de índole personal esté accesible más allá de lo que el usuario desearía, o le sería conveniente para su seguridad.

5.3 Acoso

Humillaciones, insultos, extorsiones, sobornos...El maltrato psicológico en general constituye un serio y creciente problema presente en las redes sociales.

Los perfiles, tanto del acosador como del acosado son muy variados. Este amenaza gana en seriedad cuando se trata de niños.

Algunas variantes de acoso en redes sociales son:

- **Ciberbullying**

Es el acoso realizado entre menores de edad. Tanto el acosador como la víctima son menores de edad. Si existe la intervención de un adulto no es ciberbullying, sino ciberacoso.

Al igual que el bullying, el ciberbullying se produce cuando un menor atormenta, amenaza, hostiga, humilla o molesta a otro, normalmente compañeros de colegio, mediante el uso de las nuevas tecnologías y de forma prolongada.

Las redes sociales (principalmente Tuenti), son un escenario típico donde se producen estos acosos entre menores.

http://www.ciberbullying.com

- **Grooming**

Tiene lugar cuando un adulto intenta contactar con un menor a través de Internet, y con el objetivo de obtener satisfacción sexual intenta convencer al menor para que le envíe imágenes eróticas o pornográficas. El adulto puede además intentar concertar un encuentro con el menor convenciéndolo de buenas maneras o bien amenazándolo.

5.4 Likejacking

Esta técnica deriva del clickjacking y es usada en la red social Facebook. El término se crea a partir del nombre del botón "Me gusta" o "Like" de Facebook que aparece bajo cada comentario o elemento compartido, y el término "hijacking" que significa secuestro.

Existen varias formas de utilizar esta técnica según el objetivo que desea alcanzar.

- **Campañas de spam, phishing y malware**

  El escenario es el siguiente. Un usuario hace clic en un enlace distribuido a través de la red social y va a parar a una web. Una vez que ve el contenido que hay en la misma, la abandona. Sin embargo, sin su consentimiento se ha publicado en su muro de Facebook un enlace a esa web. El comentario aparece como si lo hubiera publicado él y como si hubiera pulsado al botón de "Me gusta".

  El riesgo de este tipo de ataques es que los amigos de ese usuario verán ese link y pensarán que es algo interesante, por lo que a su vez pincharán también en el enlace y serán víctimas de ese mismo ataque, poniendo en peligro así a toda su lista de contactos. Se trata, pues, de un ataque viral.

  En un momento dado, los ciberdelincuentes pueden cambiar el contenido de la web y colocar en ella una página de phishing o malware. Por ejemplo, en éstas pueden aparecen anuncios que nos indican que tenemos desactualizado el navegador o que necesitamos cierto complemento para poder ver el contenido de la web. Evidentemente esto suele ser falso y el programa que nos decargamos o instalamos en el navegador es un malware.

  De esta manera, los usuarios que lleguen a la misma no verán sólo como se publica un comentario en su nombre en su muro de Facebook sin su consentimiento, sino que además terminarán con su ordenador infectado por malware.

- **Obtener seguidores / Marketing viral**

  Las personas somos curiosas por naturaleza. Bajo esta premisa se crea esta forma de likejacking. El proceso consiste en publicar algo que genere cierta atracción y curiosidad a todo aquel que lo vea (por ejemplo, "Mira al presidente del gobierno desnudo"). A esto se le añade el condicionante de que para poder ver el contenido anunciado, es obligatorio darle a "Me gusta". En algunos casos aparece el contenido prometido, y en otros no.

  Sea como sea, el objetivo es que el usuario haga click en "Me Gusta" y por tanto ganar seguidores. Esto es usado en campañas de marketing viral principalmente.

6 RECOMENDACIONES PARA UN USO SEGURO Y RESPONSABLE

6.1 Configura la PRIVACIDAD de tu perfil

A la hora de crear una cuenta de usuario en una red social, las opciones sobre la privacidad del perfil que vienen configuradas por defecto no siempre son las mas adecuadas para nuestra seguridad. De hecho, en la mayoría de las redes sociales las opciones de privacidad por defecto suelen ser poco restrictivas. Por ello es recomendable dedicar un mínimo de tiempo a configurar las opciones de privacidad de nuestro perfil de usuario y evitar fugas de información no deseadas.

También es conveniente revisar estas opciones de forma periódica ya que las redes sociales cambian y se actualizan continuamente, se añaden nuevas funcionalidades y éstas suelen venir con las opciones de privacidad configurada por defecto (la cual no suele ser la que mas nos convenga).

Como ejemplo de una configuración adecuada de las opciones de privacidad, veamos el caso de Facebook:

- Evitar que ninguna configuración de perfil esté disponible de forma pública, sin limitaciones. Preferentemente, mostrar la información **sólo a los amigos** y, de ser posible, solo a un grupo de estos en caso de contar con un número elevado.
- Limitar el público que observa las fotos donde el usuario fue etiquetado, especialmente si se trata de un niño.
- Evitar que las aplicaciones puedan acceder a información personal, o publicar en el muro por si solas.
- **Usar un seudónimo** en vez de nuestro nombre real. Bien es cierto que en ciertas redes sociales, como Linkedin, esto no es muy habitual ya que está orientada a las relaciones laborales.

Estos pasos suelen ser aplicables a el resto de redes sociales, con algunas diferencias de terminología.

6.2 Limita la información personal y laboral contenida en tus publicaciones

No realizar publicaciones con información sensible como direcciones, número de teléfono o datos sobre compromisos de agenda o rutinas. Tampoco es conveniente publicar información relacionada con tu trabajo y tu entorno laboral como reuniones, noticias internas, sucesos cercanos, viajes de empresa, etc. En ocasiones realizar publicaciones relacionadas con tu trabajo y tu organismo puede ser ilegal e ir en contra de las políticas y normas de conducta dictadas.

A veces limitar la cantidad de información que fluye por una red social sobre nosotros no es tarea fácil debido a que nuestros contactos pueden decidir hacer una publicación que contenga información personal nuestra. Si tienes amigos publicando información, fotografías u otros datos sobre nosotros que no deseamos que ser hagan públicos, pídeles que los borren.

Es conveniente asegurarse que todos los datos combinados, los publicados por nuestros contactos, más los que publicamos nosotros, en conjunto no constituyan una cantidad de información sobre nosotros mayor de lo que estamos dispuestos a compartir con un extraño.

6.3 Escoge a tus amigos

Las redes sociales facilitan a las personas hacer nuevos amigos o contactos, e intercambiar sus identidades.

Considerar limitar las personas a quienes se les permite contactarnos y ver nuestros datos publicados en las redes sociales. Si interactúa con personas desconocidas, debe ser cauteloso acerca de la cantidad de información que le revela o si queda en citarse con esta persona.

6.4 Se un poco escéptico

No hay que creer todo lo que se lee online. Las personas podrían publicar información falsa o engañosa sobre varios tópicos, incluyendo sus identidades.

No necesariamente esto se hace siempre con malas intenciones, podría ser sin intención, una exageración o incluso una broma. Aun así, tomar las precauciones apropiadas y verificar la autenticidad de cualquier información antes de realizar alguna acción.

6.5 Usa una contraseña FUERTE

Se un poco creativo con la contraseña que usamos para entrar en nuestro perfil. No escojas nombres del diccionario, ni nombres propios, ni combinaciones típicas como “qwerty”, “abc123”, series de números, etc.

Como ayuda pueda usar un programa como KeePassX que nos permite generar y guardar contraseñas para diferentes aplicaciones en un archivo cifrado.

6.6 No uses la misma contraseña para todo

No use una misma contraseña para diferentes propósitos. Supongamos que uso una misma contraseña para varias aplicaciones, por ejemplo, correo, Facebook, Twitter, eBay y la cuenta de esa tienda que tanto nos gusta. Si un intruso consigue vulnerar solo una de estas páginas, por ejemplo la tienda, y consigue nuestra contraseña, tendrá total acceso al resto de aplicaciones.

6.7 Conoce las condiciones y políticas del servicio

Leer con atención y de principio a fin la política de privacidad y las condiciones y términos de uso de la red social que escojamos.

Leer las políticas del sitio nos permitirá detectar si existen puntos expuestos con los que no estemos conformes, como por ejemplo, el envío de correos a nuestros amigos para que se unan a la red

social en cuestión. Algunos sitios podrían compartir datos tales como direcciones de correo o preferencias de los usuarios con otras compañías. Esto podría ocasionar un incremento del spam.

6.8 Accede de forma segura (HTTPS)

Algunas redes sociales te permiten acceder usando conexiones cifradas por medio de HTTPS, pero no te obligan a ello. Por ejemplo, si accedemos a Facebook con www.facebook.com lo hacemos sin cifrar las conexiones. Para acceder usando HTTPS tenemos que escribir en nuestro navegador https://www.facebook.com.

La mayoría de las redes sociales nos permiten configurar opciones para obligar el acceso mediante HTTPS. Por otro lado podemos hacer uso de complementos en los navegadores para que, siempre que esté disponible el acceso por HTTPS a un sitio web, lo use. Uno de estos complementos es HTTPS Everywhere.

6.9 Cuidado donde haces click

Se cuidadoso al hacer click sobre enlaces publicados, incluso por tus contactos. Muchos virus y gusanos se propagan a través de enlaces. Si un enlace te parece extraño, sospechoso o que muestra demasiado interés por ser accedido, no pulses sobre él. No importa que el enlace esté en el muro de tu mejor amigo. La cuenta de tu amigo puede haber sido infectada o secuestrada y estar distribuyendo malware o publicando enlaces maliciosos sin darse cuenta.

Aunque son muy útiles, los acortadores de URL pueden convertirse en una peligrosa arma para los atacantes a la hora de publicar enlaces maliciosos. Ten cuidado pues en las URLs cortas, a priori, accedemos a ciegas al enlace que hay detrás. Existe una extensión de Firefox llamada LongURLPlease cuya funcionalidad consiste en localizar las url de cerca de 80 servicios que se encargan de realizar la reducción de longitud y convertir en el navegador del usuario el enlace mostrado por su correspondiente enlace destino.

6.10 Aplicaciones

Algunas redes sociales te permiten ejecutar o instalar aplicaciones de terceros, como juegos. Ten en cuenta que estas aplicaciones tienen un bajo o nulo control de calidad y pueden tener acceso total a tu cuenta y a tus datos. Las aplicaciones maliciosas usan estos privilegios de acceso a tu cuenta para interactuar con tus amigos en tu nombre, robar y hacer un mal uso de tu información personal.

Procura solo instalar aplicaciones de confianza de sitios reconocidos, y mantenerlas actualizadas. Cuando dejes de usar alguna de estas aplicaciones, bórrala.

7 CONCLUSIONES

No cabe la menor duda de que las redes sociales constituyen un gran avance en las relaciones y comunicación de las personas. En este informe se han mostrado algunas amenazas a las que estamos expuestos como usuarios durante su uso. Que seamos o no víctimas de éstas depende en gran medida de que las usemos de una forma responsable. Solo basta con preocuparnos un mínimo de evitar que nuestra información personal pueda acabar en manos de indeseables, y en definitiva, actuar con sentido común, no dejándonos llevar siempre por la curiosidad.

8 REFERENCIAS

- ONTSI, 2011: Las redes sociales en Internet
- ESET, 2011: Guía de seguridad en redes sociales
- SANS, Septiembre 2011: OUCH! Boletín mensual de consejos de seguridad para usuarios de computadoras.
- CYBSEC, 2009: Seguridad en redes sociales
- Ministerio de educación, cultura y deporte. Observatorio tecnológico, 2011: Privacidad y seguridad en redes sociales
- Ciberbullyng