

Guía de Seguridad en Redes Sociales



INTRODUCCION

Las redes sociales son 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 los principales ataques? ¿Cuáles son las principales medidas de seguridad? A partir de responder estas dos preguntas, el presente informe guiará al usuario para una mayor protección en el uso de redes sociales.

REDES SOCIALES



Facebook

- Es la red social más popular del mundo.
- Durante el 2011 ha superado los 600 millones de usuarios en todo el planeta.
- Es la predilecta entre los más jóvenes; utilizada para armar redes de contactos entre amigos, entre otros usos.
- También es utilizada por empresas y organizaciones para comunicarse con el público.



MySpace

- Otra plataforma basada en las relaciones sociales, permite compartir perfiles de usuarios, amigos, fotos, música, etc.
- Facebook le ha quitado usuarios, aunque mantiene su importancia, por ejemplo, para la difusión de bandas musicales.
- A marzo del 2011, posee 34 millones de usuarios.



Twitter

- Red social de microblogging.
- Los usuarios comparten contenidos en un máximo de 140 caracteres.
- Ha sido una de las redes sociales de mayor crecimiento durante 2010.
- Posee más de 200 millones de usuarios.



LinkedIn

- Red social para profesionales. Es la más utilizada en el ámbito corporativo.
- Permite a las personas tejer redes de contactos laborales, cargar sus curriculum vitae en la web, y disponer de ellos en formato público.
- A marzo del 2011, cuenta con 100 millones de usuarios registrados.



A close-up photograph of a computer keyboard. A single key is highlighted in a vibrant red color. On this red key, the word "Toxic" is printed in white, sans-serif font. To the right of the text is a white icon of a human skull with a glowing lightbulb inside, symbolizing a dangerous idea or malware. The surrounding keys are white with standard keyboard symbols like "command", "option", "alt", "shift", and "delete".

Toxic

¿Cuáles son los riesgos en las redes sociales?

La información y el dinero de los usuarios son el objetivo de los atacantes, por lo que a mayor cantidad de usuarios, más atrayente se vuelve un sitio web para el atacante. Por lo tanto, más allá de todas sus ventajas, la navegación por los sitios web de redes sociales, implica exponerse a una serie de amenazas informáticas.

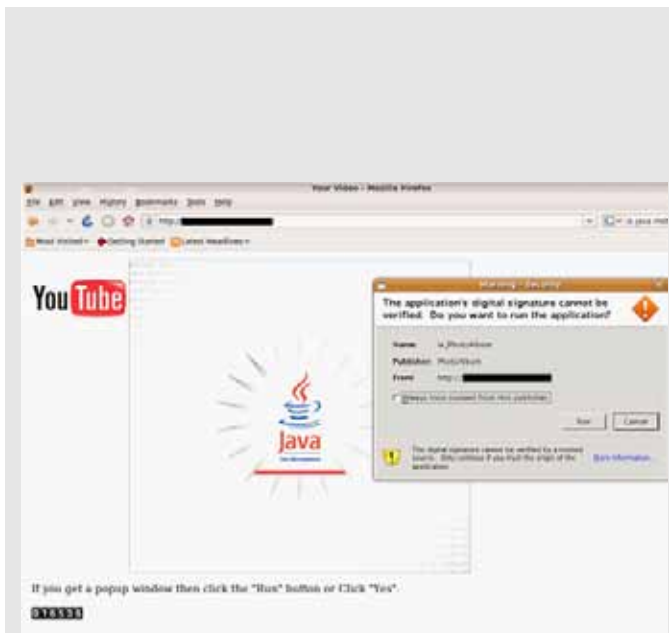


Imagen 1 – Sitio web de propagación de Boonana

- Acrónimo en inglés de las palabras malicious y software, es decir, código malicioso.
- Son archivos con fines dañinos que, al infectar una computadora, poseen diversas acciones, como el robo de información, el control del sistema o la captura de contraseñas.
- Virus, gusanos y troyanos; son las variantes más conocidas en este campo.

A partir de estrategias de Ingeniería Social, los desarrolladores de malware suelen utilizar las redes sociales para propagar los códigos maliciosos.

El troyano Koobface es el más conocido de este tipo. Con nombre de acrónimo de la red social más popular (Facebook), el troyano se caracterizó, en sus primeras campañas de propagación, por utilizar mensajes atractivos en redes sociales. La amenaza, conforma una botnet, una red de equipos zombies que pueden ser controlados remotamente por el atacante.

En octubre del 2010 (a casi dos años de su aparición), una nueva variante de Koobface (identificada como Boonana: Java/Boonana.A o Win32/Boonana.A) tenía la particularidad de propagarse a través de Java, una tecnología multi-plataforma, que permitía realizar la infección tanto en sistemas Windows, Linux y Mac OS. Al momento que la víctima visita la página maliciosa, la misma identifica qué sistema operativo está ejecutando el usuario, y descarga el archivo correspondiente a esa plataforma.

Phishing

- Consiste en el robo de información personal y/o financiera del usuario, a través de la falsificación de un ente de confianza.
- Es frecuentemente realizado a través del correo electrónico y sitios web duplicados, aunque puede realizarse por otros medios.

¿Cómo identificar un sitio de phishing?

No siempre es sencillo identificar un sitio web duplicado, aunque por lo general, para llegar allí; el usuario ya debe haber sido víctima de alguna técnica de Ingeniería Social, o infección de malware que lo enlazó al sitio malicioso.

Para el primer caso, es recomendable evitar hacer clic en enlaces sospechosos y, en caso que alguna entidad solicite información sensible, acceder manualmente al sitio web; sin utilizar ningún tipo de enlace, y verificar si en el mismo existe dicha solicitud.

Además, es recomendable verificar tanto el dominio en el sitio web, como así también que se utilice cifrado para transmitir los datos (protocolo HTTPS). Esto último, aunque no es garantía de la legitimidad de un sitio, sí es requisito indispensable y, por lo general, los sitios de phishing no lo poseen.

(P) Phishing


Ejemplo II: phishing a través de correo electrónico

Asunto: Facebook Password Reset Confirmation. Customer Support.
Fecha: Tue, 8 Dec 2009 10:13:58 +0800
De: Facebook Service <customer@facebook.com>
A: customer@facebook.com

Hey [username](#),

Because of the measures taken to provide safety to our clients, your password has been changed.
You can find your new password in attached document.

Thanks,
Your Facebook.

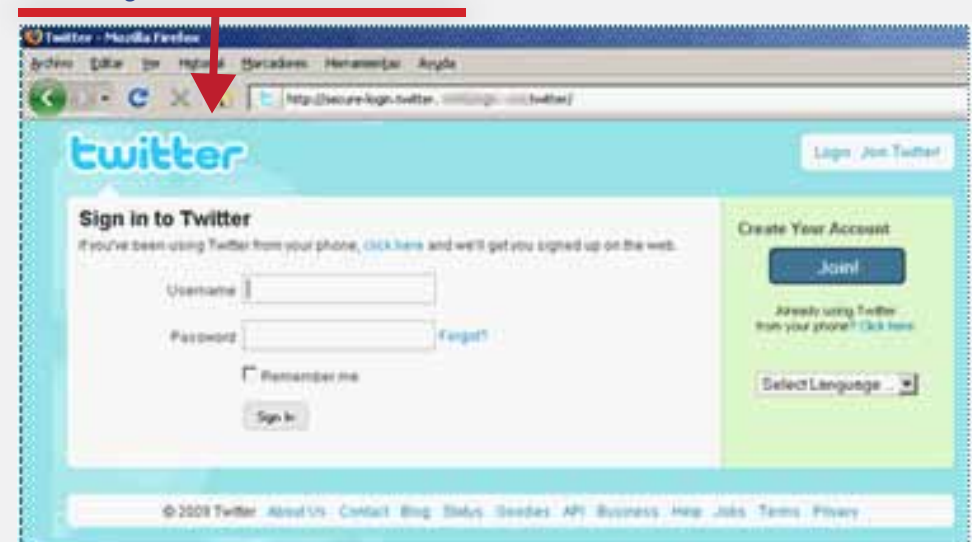
 Facebook_Password_833fd.zip
22 K [Descargar](#)

Ejemplo I: phishing a Twitter

El sitio original utiliza el protocolo seguro HTTPS:



El sitio original tiene el dominio correcto:



(R) Robo de información



- En el uso diario de las redes sociales, los usuarios suben a la web diversos datos de índole personal, que pueden ser de utilidad para los atacantes.
- El robo de información en redes sociales, se relaciona directamente con el robo de identidad; uno de los delitos informáticos que más ha crecido en los últimos años.
- Los dos vectores de ataque más importantes para el robo de información son:
 - ✓ **Ingeniería Social:** el contacto directo con el usuario víctima, extrayendo información a través de la comunicación, la “amistad” o cualquier comunicación que permita la red social.
 - ✓ **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. Personas malintencionadas podrían acceder a dicha información.

A) Acoso y menores de edad



- Los niños utilizan las redes sociales desde muy temprana edad, incluso más allá de lo que las propias redes sociales indican como conveniente (Facebook, por ejemplo, fue concebida para mayores de 18 años).
- Existen una serie de amenazas, que están enfocadas específicamente en los jóvenes que utilizan estos servicios: acoso (cyberbullying), grooming, sexting; son algunos de los riesgos a los que se ven expuestos al navegar por redes sociales.
- El rol de los adultos es fundamental para la protección de los niños: estos no deberían utilizar las redes sociales, sin contar con el apoyo, el diálogo y la educación; de sus padres o cualquier otro adulto de referencia, incluso los propios maestros.



Formas de protección

Ante este escenario de amenazas, el uso de redes sociales puede parecer peligroso. No obstante, si se siguen los consejos brindados a continuación, es posible utilizarlas y contar con niveles de protección adecuados para un uso correcto, y seguro, de las redes sociales.

Se destacan como principales medidas, utilizar tecnologías de seguridad, configurar correctamente los usuarios en las redes sociales y utilizar el protocolo HTTPS para la navegación. No obstante, la constante educación del usuario y un uso cuidadoso al momento de la navegación, siempre permitirán minimizar de forma importante los riesgos a los que se ve expuesto.

UTILIZAR TECNOLOGÍAS DE SEGURIDAD



Siendo los códigos maliciosos la amenaza masiva más importante, la utilización de un software antivirus con capacidades proactivas de detección, y la base de firmas actualizadas; es un componente fundamental para prevenir el malware que se propaga por redes sociales.

Las herramientas antispam y firewall, también permiten optimizar la seguridad del sistema ante estos riesgos.

También es fundamental no utilizar un usuario administrador al momento de navegar por estas redes, y contar con perfiles en las computadoras para cada usuario de la misma; de forma tal de minimizar el impacto en caso que ocurriera un incidente.

Finalmente, para los menores de edad, herramientas de control parental permiten bloquear sitios web indeseados, así como también restringir el horario o cantidad de horas en que el niño utiliza las redes sociales.



CONFIGURAR LA PRIVACIDAD EN LAS REDES SOCIALES

Por defecto, no siempre las configuraciones en las redes sociales son las más óptimas para la seguridad del usuario. Por lo tanto, es recomendable dedicar un tiempo prudencial al momento de crear el usuario (y periódicamente), para revisar cuáles son las posibles fugas de información ante una mala configuración del sistema.

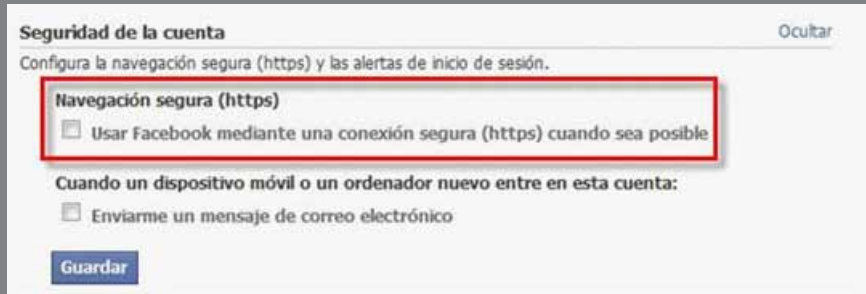
Configuraciones de privacidad en Facebook

- 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 publica ren el muro.

Más información: <http://blog.eset.com/2011/05/25/facebook-privacy>

En Facebook

Elegir la opción “Configuración de cuenta” en el menú “Cuenta” de la esquina superior derecha. Luego, dirigirse hacia la pestaña de “Seguridad de la cuenta” y se encontrará la posibilidad de optar por la navegación segura:



En Twitter

Ir a la configuración de la cuenta y marcar la casilla “usar siempre HTTPS”, como se indica en la siguiente imagen:



CÓMO CONFIGURAR HTTPS EN FACEBOOK Y TWITTER



Configurar la navegación por el protocolo HTTPS, permite que todos los ataques relacionados a la interceptación de información que viaja en texto claro (legible) a través de redes de computadoras, sean controlados. Con el protocolo HTTPS, todos los datos – no solo el usuario y la contraseña – viajarán cifrados y serán ilegibles para cualquier atacante en la red.

Es recomendable aplicar estas configuraciones, especialmente útiles cuando se conecta a estas redes sociales desde redes inalámbricas públicas.

DECÁLOGO DE SEGURIDAD EN EL CIBER ESPACIO

1

Evitar los enlaces sospechosos

2

No acceder a sitios web de dudosa reputación

3

Actualizar el sistema operativo y aplicaciones

4

Descargar aplicaciones desde sitios web oficiales

5

Utilizar tecnologías de seguridad

6

Evitar el ingreso de información personal en formularios dudosos

7

Tener precaución con los resultados arrojados por buscadores web

8

Aceptar sólo contactos conocidos

9

Evitar la ejecución de archivos sospechosos

10

Utilizar contraseñas fuertes



CONCLUSIÓN

Sin lugar a dudas las redes sociales son un valioso recurso para los internautas. No obstante, como se presentó en la presente guía, existen una serie de amenazas que pueden exponer al usuario durante su uso. Es por ello que es recomendable no subestimar a los delincuentes informáticos, y haciendo un uso correcto de herramientas tecnológicas, configuraciones correctas, y una conducta adecuada durante la navegación; **será posible utilizar las redes sociales de forma segura.**