

SEGURIDAD DE LA INFORMACIÓN Y REDES SOCIALES

Cuando se habla de redes sociales se hace referencia a aquellos servicios en los que los usuarios pueden crear un perfil personal e interactuar con otros usuarios. Estas plataformas permiten interactuar mediante mensajes, compartir información, imágenes o vídeos, de forma que estas publicaciones sean accesibles de forma inmediata por todos los usuarios que formen su grupo de contactos.

Concentran todo tipo de servicios para que la persona registrada pueda comunicarse y establecer relación con otros usuarios.

Para formar parte de ellas hay que registrarse rellenando una serie de formularios con datos personales, fotografías, etc. Normalmente basta con crear un perfil básico, y a partir de ahí aportar toda la información sobre sí mismo que se desee para aumentar los datos ofrecidos a la red social.

Las redes sociales se apoyan en las llamadas 3Cs de la Web 2.0:

- Comunicación (ayudan a la puesta en común de conocimientos).
- Comunidad (ayudan a encontrar e integrar comunidades).
- Cooperación (ayudan a realizar actividades conjuntamente).

El éxito que están alcanzando muchas de las redes sociales en los últimos años da una idea del interés del usuario medio en este tipo de relación con Internet y el acierto de estos modelos de comunicación. Las redes sociales van más allá del éxito de otros sistemas de comunicación entre usuarios de la Red.

El tiempo de permanencia en redes sociales como Facebook y Twitter aumentó un 82% durante el 2009. Facebook fue la red social número uno con 206,9 millones de visitantes únicos en diciembre de 2009, lo que equivale al 67% de los usuarios de las redes sociales en todo el mundo¹.

Pero también existen varios riesgos derivados del uso de las redes sociales. Por ello, a continuación se presentan algunas de las vulnerabilidades a las que el usuario de redes sociales está expuesto así como recomendaciones y consejos que debe seguir para asegurar la seguridad y la privacidad de su perfil en estas plataformas.

¹ http://digitalmedia.strategyeye.com/article/brzAEXrgBos/2010/01/25/social_network_use_soars_82_in_a_year/

I Riesgos de seguridad de las redes sociales

Es precisamente el bien compartido en las redes sociales, la información personal, donde radica la base del riesgo más habitual en ellas. Veamos algunas de las vulnerabilidades a las que se enfrentan los usuarios de este tipo de redes.

Uso indebido de la información del usuario para suplantar su identidad

El peligro directo y más evidente de las redes sociales es la divulgación sin consentimiento del usuario de la información personal que se expone en su perfil. El valor intrínseco de estas redes está en el hecho de publicar información personal para poder relacionarse con otras personas.

Datos que en principio pueden parecer intrascendentes, como fecha de nacimiento, nombres completos, fotografías aparentemente inocentes, lugar de trabajo, etc., pueden ser de gran utilidad para atacantes.

Con estos datos, se puede llegar a suplantar la identidad de una persona, por ejemplo a la hora de contratar servicios que no necesitan la presencia física de la persona que va a llevarlos a cabo.

Los datos personales también pueden ayudar a ciertos atacantes a tener acceso a cuentas de correo. Normalmente muchos sitios de Internet que ofrecen contenidos protegidos por contraseña, como por ejemplo los sistemas de correo, disponen de un sistema de recuperación de contraseña basado en una pregunta secreta, que suele consistir en un dato personal que pocas personas conocen.

Si esa información es divulgada, o se ofrece alguna pista que permita deducir las respuestas a estas preguntas, se pueden ver comprometidos otros servicios usados por el usuario. El atacante solo tiene que simular que es la víctima que ha perdido la contraseña y proporcionar la respuesta correcta como “garantía” de que es el legítimo dueño quien reclama el cambio.

Si los datos que introdujo la víctima son correctos, por ejemplo “nombre del colegio en el que estudiaste”, o “segundo apellido de tu madre”, el atacante podría tener acceso a la web protegida por contraseña sin necesidad de conocerla.

Ilustración 1: Pregunta secreta necesaria para poder restablecer una contraseña del correo de Yahoo



Fuente: YAHOO

Otro riesgo al que se exponen los usuarios de redes sociales es la utilización fraudulenta de otro tipo de material que los usuarios comparten en estas plataformas, como por ejemplo fotografías, y que pueden ser usadas para desprestigiar, o directamente chantajear o extorsionar.

Phishing

El phishing² se concibió en principio como una amenaza contra bancos y entidades de pagos a través de Internet, que trabajasen directamente con movimientos de dinero. Poco

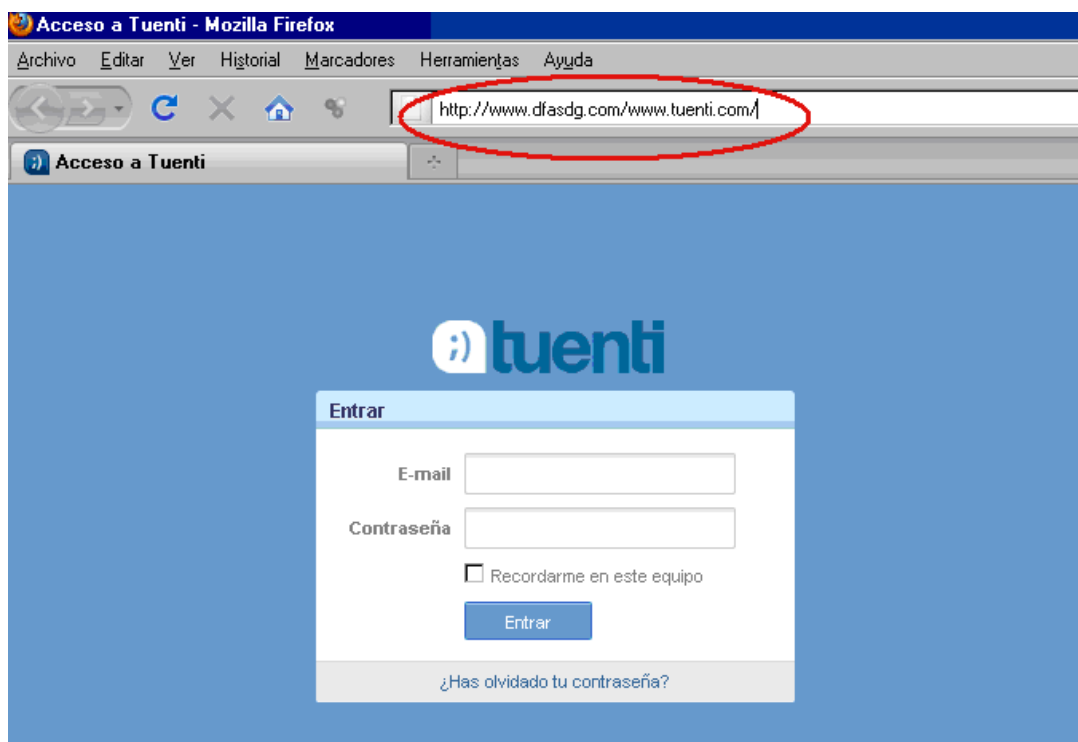
² Según el AWPG (Anti-Phishing Working Group) se puede definir como: “Los ataques de phishing recurren a formas de ingeniería social y subterfugios técnicos para robar los datos de identificación personal de consumidores y las credenciales de cuentas financieras.

Los ardidés de ingeniería social se basan en correos electrónicos engañosos que conducen a los consumidores a sitios web falsos diseñados para estafar a los destinatarios para que divulguen datos financieros tales como números de tarjetas de crédito, nombres de usuario de cuentas, contraseñas y números de la seguridad social.

Apropiándose de nombres comerciales de bancos, distribuidores y compañías de tarjetas de crédito, los phishers a menudo convencen a los destinatarios para que respondan. Los subterfugios técnicos implican la instalación de crimeware en ordenadores personales para robar las credenciales directamente, habitualmente utilizando troyanos que captan las pulsaciones de teclado”.

después los atacantes percibieron que se podía realizar phishing de cualquier página que requiriese una contraseña.

Ilustración 2: Phishing contra la red social Tuenti



Fuente: INTECO

Esto reporta beneficios a los atacantes ya que muchos usuarios utilizan la misma contraseña para varios servicios en la Red. También, el obtener contraseñas de perfiles privados les permite acceso a información sensible de usuarios (fecha y lugar de nacimiento, por ejemplo).

Ingeniería social

Una vez que los atacantes consiguen acceso a los perfiles, pueden usarlos para aplicar ingeniería social. Se trata de técnicas "psicológicas" que permiten a los atacantes que los usuarios con los que tiene relación el usuario al que se ha suplantado la identidad, se encuentren más confiados, y puedan aprovechar esa circunstancia en beneficio propio.

Por ejemplo, es mucho más fácil que un usuario pulse sobre un enlace que parece provenir de una persona que considera "amigo" en su red social, o con la que ya ha establecido contacto previamente. También es más sencillo convencer a usuarios de que ofrezcan información sensible a los atacantes si estos, por ejemplo, en el caso particular de que los suplantadores, se hagan pasar por personas del sexo opuesto, que señalan que quieren establecer una relación personal. Esto también se considera un tipo de

ingeniería social. Los atacantes utilizan fotografías de usuarios reales de la red social que dan credibilidad al engaño.

Vulnerabilidades

En las redes sociales, muchas páginas de creación o muestra de perfil han contenido en algún momento vulnerabilidades que han permitido a atacantes manipular el perfil propio o ajeno de otros usuarios, o redirigirlos a otras páginas donde son infectados por código malicioso. Este fallo se volvió común en la red social Myspace.

Otra de las vulnerabilidades de la mencionada red social, permitía a un atacante incrustar publicidad en forma de anuncio emergente en las cuentas de ciertos usuarios. En muchos perfiles se observó durante un tiempo una *popup* o ventana emergente que simulaba ser la ventana de administración de actualizaciones de Windows. Si el usuario aceptaba la supuesta actualización, se descargaba un programa que infectaba al sistema operativo.

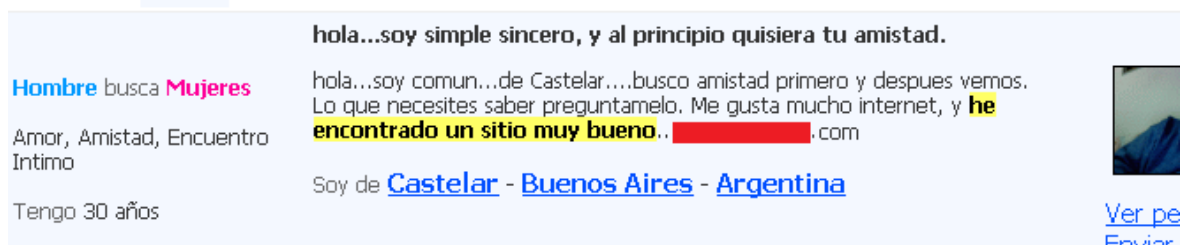
Publicidad

Los atacantes, una vez poseen un perfil propio o ajeno en una red social, pueden utilizar sus recursos para promocionar páginas o productos ilegales con publicidad no deseada.

Los atacantes programan “robots” u ordenadores zombies³ que realizan comentarios genéricos o intrascendentes en foros o en cualquier otro método que permita comunicarse con otros usuarios. En estos comentarios, se insertan direcciones web de las páginas que quieren promocionar o hablan del producto que desean. En ocasiones son personas reales las que están detrás de estos comentarios, lo que les proporciona mayor realismo.

La mayoría de la publicidad que inunda las redes sociales de esta forma se corresponde con estafas o productos ilegales, al igual que el correo basura o no solicitado.

Ilustración 3: Publicidad encubierta en red social contactos



Fuente: INTECO

³ Artículo: [Amenazas silenciosas en la Red: rootkits y botnets](#), del Observatorio de la Seguridad de la Información.

También es posible que se publiquen enlaces que incitan a la descarga de código malicioso que aparentemente es software legítimo.

Aprovechamiento de los recursos

En el caso de la red social Twitter, se observó un fenómeno extraño. Su plataforma fue utilizada como un canal para controlar botnets. Las botnets⁴ son redes de ordenadores infectados que están a las órdenes de otro sistema central, el cual puede controlarlos a distancia mediante el atacante, y para los fines que él considere oportunos.

Normalmente se utilizan para aprovechar la capacidad de cómputo o el ancho de banda de esos ordenadores infectados y usarlos para enviar spam, atacar una web legítima inundándola de visitas hasta que no puede mantener el servicio en línea (lo que se conocen como ataques de “denegación de servicio distribuido”), o para distribuir malware y robar contraseñas.

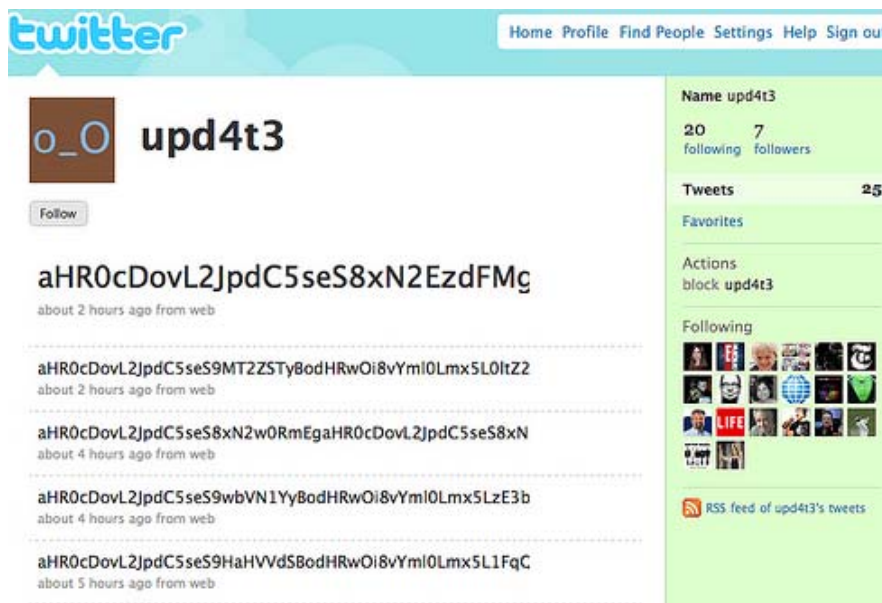
Las botnets necesitan un panel de control, gestionado por el atacante, que le permita enviar los comandos a los ordenadores infectados. Así puede administrarlos desde un solo punto. El panel de control puede consistir en cualquier método.

Normalmente se trata de un programa que se gestiona desde una página web que permite de forma anónima y deslocalizada organizar la botnet. Otro método común es el uso del protocolo IRC (*Internet Relay Chat*). Muchos troyanos que hacen que los sistemas formen parte de una botnet, usan el modelo de chat para controlar a sus infectados.

Este modelo de ataque se llevó a cabo en agosto de 2009 en Twitter. Se utilizó su infraestructura como panel de control de una botnet. Un usuario registrado, el atacante, cada vez que publicaba una nota, estaba en realidad enviando mensajes a las máquinas comprometidas, que formaban parte de la botnet. Los mensajes se hallaban codificados de forma que resultaban incomprensibles, pero pudieron ser detectados y descifrados.

⁴ http://www.inteco.es/Seguridad/Observatorio/Multimedia/botnet_multimedia

Ilustración 4: Usuario ficticio manejando una botnet desde Twitter



Fuente: INTECO

Suplantación de la imagen de personajes famosos para recabar datos de otros usuarios

La popularidad de las redes sociales ha llegado a todos los niveles y escalas sociales. Son muchas las personas conocidas que han creado su propio espacio en ellas de forma que pueden mantener un contacto directo con sus seguidores, además de constituir un medio más de promoción.

Actores, deportistas, cantantes, etc., utilizan una o varias redes sociales, además de páginas web, donde interactúan de forma más directa con sus fans.

Aprovechando esta circunstancia, no son pocos los casos que se han dado de suplantación de identidad en redes sociales. Usuarios que se hacen pasar por personas famosas, deportistas, marcas, etc. y aprovechan esta circunstancia para establecer contactos con la intención de recabar toda la información personal posible de los seguidores del personaje famoso, habitualmente con fines fraudulentos.

Ilustración 5: Página de un perfil falso de Bill Gates



Fuente: FACEBOOK

Rumorología

Relacionado con el punto anterior se han dado también casos de uso de las redes sociales para lanzar rumores, bulos o falsos testimonios que puedan dañar seriamente la credibilidad o el honor de las personas afectadas. La rumorología y técnicas *pump & dump* son viejas estafas en Internet relacionadas con los activos financieros.

Las técnicas *pump & dump* consisten en difundir un rumor financiero a través de cualquier método, con el fin de inflar artificialmente el precio de una acción. Los rumores se centran en ofrecer datos y consejos sobre inversiones en mercados alta volatilidad, presentando en los mensajes información supuestamente privilegiada, como por ejemplo, cotizaciones, expectativas, rentabilidades, etc. Normalmente exagerados, falsos u obtenidos directamente sobre servicios gratuitos de información financiera.

Los atacantes que se hacen pasar por operadores de bolsa, han comprado a un precio muy inferior los activos financieros, consiguen inflar las acciones a corto plazo gracias a los rumores, y venden rápidamente. Es una forma muy específica y estratégica de utilizar el spam, y todos los medios al alcance, para propagar rumores que pueden darles una gran rentabilidad a corto plazo. Las redes sociales no se libran de este tipo de mensajes.

Malware -códigos maliciosos-, y el caso particular de los gusanos

En la actualidad son varios los ejemplos de malware específicamente diseñado para una red social. En la mayoría de los casos aprovechan un fallo en la infraestructura de la plataforma para propagarse con eficacia entre los diferentes contactos, o se camuflan como una aplicación o complemento de la red en cuestión para pasar desapercibidos y que los usuarios lo ejecuten:

- Koobface es actualmente el gusano específico de redes sociales más versátil y que más “éxito” ha alcanzado. Ataca en principio a Facebook, pero sus últimas versiones están diseñadas para reproducirse por MySpace, Twitter, hi5, Bebo, Friendster, myYearbook, Tagged, Netlog y Fubar.

Apareció por primera vez a finales de 2008. El gusano deja mensajes a los contactos o amigos de las redes sociales del usuario cuyo ordenador ha sido infectado. Si un amigo de este usuario con el ordenador infectado por código malicioso pulsa sobre uno de los enlaces, será instado a descargar desde la página de un tercero algún tipo de software, o se descargará de forma automática con el navegador a través de alguna vulnerabilidad. Con lo que este usuario queda a su vez infectado.

El archivo que se intenta descargar se puede camuflar bajo diferentes formas y está destinado a su vez a robar información sensible de los usuarios, tales como contraseñas de entidades bancarias.

- MW.Orc, descubierto en junio de 2006, también se propagaba a través de la red Orkut. El funcionamiento es básicamente el mismo descrito para Koobface. El usuario infectado contamina la mensajería de usuarios asociados a su red, esperando que estos pulsen sobre un enlace y queden a su vez infectados.
- Un gusano brasileño llamado W32/KutWormer, consiguió 700.000 infecciones esparciéndose a través de Orkut.
- En abril de 2009 fue el turno de Twitter. StalkDaily es el gusano creado por un chico de 17 años que utilizaba la infraestructura de Twitter para enviar spam desde las cuentas de los usuarios infectados.

II Recomendaciones y Consejos de seguridad para el uso de las redes sociales

Lo principal al utilizar una red social es mantener la información privada fuera del alcance de desconocidos. Para ello lo primero, antes de darse de alta en la plataforma, es plantearse cuáles son los datos que realmente quieren hacerse públicos, o si son imprescindibles para establecer una relación con el resto de usuarios.

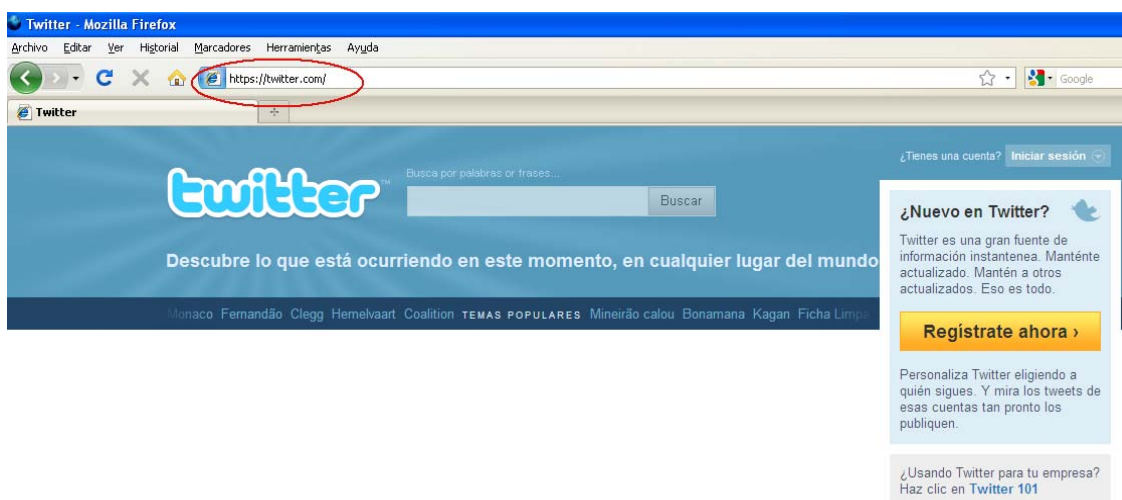
Por tanto, el sentido común debe ser la regla más importante a tener en cuenta al utilizar una red social. Evitar subir fotografías sin plantearse antes su verdadera utilidad, u ofrecer información que pueda resultar comprometedor en el futuro.

Comprobar que se trata de la página adecuada

Esta es una medida de seguridad extensible a cualquier lugar de Internet donde se introduce un usuario y una contraseña. Es imprescindible comprobar que el usuario se encuentra en el sitio adecuado en el que introducir sus datos, y que además si es posible, esta información se está transmitiendo de forma segura al servidor.

Para ello en la actualidad, los navegadores facilitan esta tarea verificando la identidad del servidor.

Ilustración 6: Ejemplo de validación de certificado en Twitter



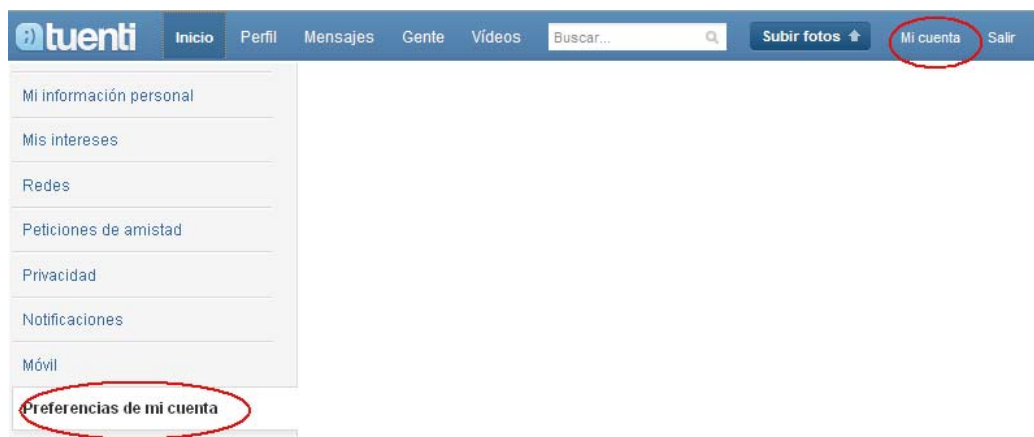
Fuente: TWITTER

Controlar quién tiene acceso la información personal

En las redes sociales existe el concepto de “amigo” que, normalmente, tiene acceso al perfil personal, de forma que puede visualizar la información publicada por el usuario. Es importante que este permiso se establezca previa autorización del interesado, que debe evaluar si realmente quiere que esa persona que solicita ser “amigo” tenga acceso a dicha información.

Algunas redes sociales permiten además, organizar a los amigos en listas tales como “familia”, “compañeros de trabajo”, etc. Con estas listas se puede controlar realmente qué tipo de personas tienen acceso a qué tipo de información de forma granular.

Ilustración 7: Opción de configuración de privacidad en Tuenti



Fuente: TUENTI

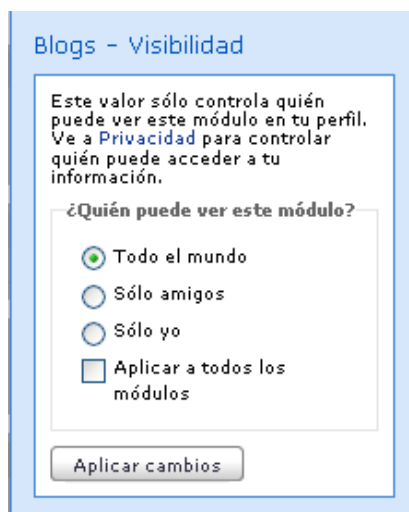
Por último, es aconsejable cerciorarse de si quien dice querer ser nuestro “amigo” es realmente quien dice ser, y no se trata de una suplantación de identidad.

Privacidad del perfil

Habitualmente, en las redes sociales, en la opción “Configuración de privacidad” se puede establecer quién puede tener acceso a los distintos módulos del perfil (fotografías, muro, etc.).

El centro de la seguridad de los datos se encuentra en esta zona de información del perfil, donde se le puede indicar al programa que sólo muestre la información a personas que, por ejemplo, se encuentren en las listas de amigos creadas.

Ilustración 8: Control de la seguridad de los blogs en MySpace



Fuente: MYSPACE

Búsqueda

En casi todas las redes sociales se pueden buscar amigos por nombre u otras opciones para localizar su perfil. Las redes también permiten elegir al usuario qué datos están disponibles a través de las búsquedas para que puedan ser localizados por terceros.

Ilustración 9: Control de la seguridad de las búsquedas en Facebook



Fuente: FACEBOOK

No seguir enlaces (links) sospechosos

Al igual que se recomienda en el uso del correo ordinario, no se deben seguir enlaces a otras páginas que el usuario no haya solicitado, incluso si provienen de contactos que conozca. Se debe evitar acceder a sitios ajenos a la propia red social por medio de enlaces, y por supuesto, evitar la ejecución de archivos que hayan sido enviados.

Eliminación del perfil

Por último, cabe recordar que si no se va a utilizar una red social temporalmente, es aconsejable deshabilitar el perfil. Y si definitivamente no se va a usar más, se debe borrar el perfil de usuario.