

Ataques y timos en redes sociales

El éxito de las redes sociales atrae también el interés de ciberdelincuentes, por lo que conviene que los usuarios adquieran unas sencillas pautas de prevención

Los carteristas y amigos de lo ajeno abundan de manera particular en los lugares más concurridos. Lo mismo sucede en Internet. El éxito de las redes sociales ha traído consigo un incremento de los ataques de ciberdelincuentes y mafias organizadas. Su objetivo es engañar al usuario con falsos mensajes, encuestas o donaciones para hacerse con sus datos personales, sus identidades digitales y, sobre todo, con su dinero. Por ello, también han aumentado las demandas para que se refuerce la seguridad de estos servicios.

Facebook, la red social más popular y principal destinataria de estas exigencias, cuenta con un nuevo Centro de Seguridad (<http://es-es.facebook.com/help/?safety=general>) en el que pone a disposición de sus usuarios gran cantidad de material informativo para padres, educadores, adolescentes y fuerzas de seguridad.

Ojo con "la nube". Los servicios que permiten al usuario almacenar información en el web (fenómeno que se conoce como "la nube") también son objeto de ataques. Entre ellos sobresalen las cuentas web de correo electrónico (Yahoo!, Gmail, Hotmail), álbumes de fotos (Flickr y Picasa en especial) o servicios de vídeos como Youtube o Vimeo. En estos casos, cuando se sale del entorno protegido del ordenador, si los servicios de almacenamiento no tienen la adecuada seguridad, se pueden sufrir ataques que supongan el robo o la pérdida de los datos.

Aunque los servicios más importantes son incluso más seguros que el propio ordenador, otros no tan conocidos pueden tener elementos vulnerables en su código y en sus niveles de seguridad. Es recomendable, en consecuencia, saber en todo momento cuál es la información de la cuenta del usuario que es pública, así como las diferentes opciones de configuración de privacidad y seguridad existentes en estas plataformas. Estos datos deben estar visibles y a disposición de todos los usuarios del servicio.

Ataques desde las aplicaciones de escritorio. Otra de las formas más comunes de infección es mediante la explotación de un agujero de seguridad en la aplicación de escritorio desde la que se accede a la red social, como es el caso del navegador de Internet. Así lo hicieron quienes trataron de acceder a cuentas de correo de numerosos disidentes chinos y a la información corporativa de Google en China. El uso de programas (conocidos como troyanos o gusanos) que roban contraseñas de cuentas o que se propagan por redes locales y dispositivos de almacenamiento externo ha sido otra de las amenazas habituales durante 2009. Estas tácticas suelen utilizar como disfraz algún motivo temporal (una felicitación navideña con un archivo malicioso adjunto), o bien noticias de actualidad (como fotografías relativas a la muerte de Michael Jackson en verano, o vídeos con el ataque a Berlusconi), para conseguir un mayor número de infecciones.

Desde páginas de terceros. El uso de páginas web y aplicaciones de terceros que permiten sincronizar datos, o el empleo de la API (una parte del código de un servicio que se libera para que los usuarios puedan crear otros servicios complementarios a partir de ella) de una red social también son estrategias para conseguir de forma fraudulenta el perfil de los usuarios. Redes sociales como Facebook y Twitter disponen de sistemas para validar las cuentas

de sus usuarios, sin necesidad de que éstos tengan que dar su nombre de miembro y su contraseña, en una página externa a estas plataformas, con el consiguiente peligro en la seguridad. Por lo tanto es recomendable no utilizar páginas y servicios que requieran contraseñas de sitios externos. Lo más habitual es el envío de mensajes no solicitados al resto de contactos del usuario, aunque también puede darse una pérdida de la identidad digital del usuario y un acceso no autorizado a sus datos personales.

Suplantación de identidades.

Se han dado casos de delincuentes ("crackers") que se han adueñado de la cuenta de Twitter del usuario para emitir mensajes falsos, e incluso insultantes para otros miembros de la popular red de 'microblogging', sin que el propietario de la cuenta pudiera recuperar su control hasta que el servicio decidió intervenir. Por otra parte, hay redes sociales, entre ellas Facebook, que permiten la creación e intercambio de aplicaciones de terceros dentro de la propia plataforma. Desde pequeños juegos on line a votaciones y encuestas sobre perfiles. En determinadas ocasiones, estas aplicaciones se han convertido en una vía para distribuir programas ejecutables con código malicioso. Es decir, mientras la aplicación realiza una acción concreta, de forma oculta para los usuarios podría realizar cualquier otra acción, como enviar datos personales a un servidor externo.

CONSEJOS para evitar problemas en las redes sociales

- **Leer siempre las condiciones de uso y las cláusulas de privacidad** para estar seguros de que el servicio tiene la calidad suficiente.
- **Buscar las especificaciones de seguridad y los protocolos de cifrado de datos: si no están visibles, no conviene confiar en el servicio.**
- **Ser parcios en la información que se ofrezca de manera pública: no hay que hacer ostentación ni mostrarse demasiado dispuesto a intercambiar contactos y datos con desconocidos.**
- **Ser selectivo con los nuevos contactos: no aceptar por norma a personas de las que no tengamos ningún conocimiento o referencia.**
- **Nadie regala nada ni ofrece nada gratuitamente: cortar de inmediato la comunicación ante sugerencias y ofrecimientos de tipo económico o sexual. Seguro que detrás hay una estafa.**
- **No abrir mensajes que despierten sospechas: las empresas de redes sociales envían mensajes para aceptar contactos, usar nuevas aplicaciones o informar, pero nunca piden que les ofrezcamos los datos personales por correo electrónico.**
- **En el caso de querer modificar algún dato, no hacerlo nunca desde la dirección que nos ofrece el servicio por correo electrónico, sino ir al buscador y desde allí a la página de inicio del servicio. Las direcciones que ofrecen en sus correos los delincuentes son tapaderas.**
- **Evitar verificar contraseñas con terceros servicios: es decir, no entrar a Twitter ni Facebook desde las contraseñas de Gmail o Yahoo! Mail.**
- **Diversificar nombres de usuario y contraseña: aunque resulte incómodo tener que guardar un registro de contraseñas, si usamos la misma en todos los sitios, es mucho más fácil que nos entren en todos nuestros servicios.**