Las mayores amenazas de seguridad en las redes sociales

Guillaume Lovet

Senior Manager

Equipo de Respuesta a Amenazas de EMEA
Fortinet Technologies

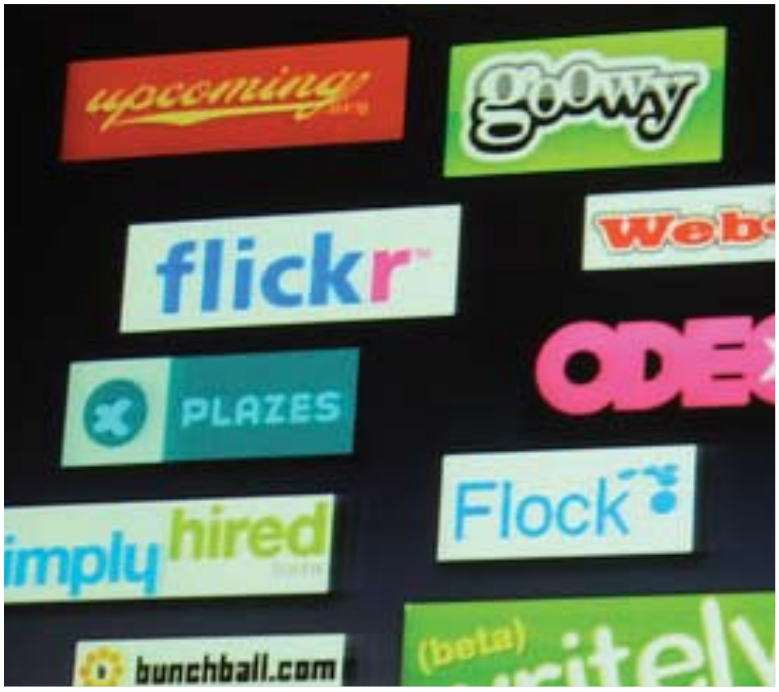
Hoy en día, las redes sociales como MySpace, Facebook y Twitter han superado su función fundamental como herramientas de comunicación para mantenerse conectados con familiares y amigos. El rápido desarrollo de estos sitios web también ha abierto nuevos canales para las empresas para comunicar y llegar a sus socios comerciales y clientes.

Cada vez más empresas están explorando y experimentando con el rentable uso de los canales de redes sociales para optimizar sus operaciones, aumentar la productividad e incluso mejorar la comunicación interna entre los empleados (aunque esto puede ser un arma de doble filo debido a la naturaleza pública de tales sitios). Sin embargo, y probablemente desconocido para muchos, las redes sociales también han introducido nuevos peligros y riesgos para las redes corporativas. De tal manera que, en general, muchas veces se aconseja a las

empresas no seguir esta tendencia de forma agresiva o no apresurarse en la adopción de redes sociales como herramientas de comunicación.

Sin embargo, las redes sociales se están convirtiendo cada vez más en una herramienta de marketing, por lo que todas las compañías con presencia online deben estar bien informadas sobre las amenazas de seguridad a las que pueden estar expuestas sus empresas al estar online y qué medidas deben tomar para protegerse.

1. Malware – El gusano Koobface ha estado recorriendo Facebook desde hace más de un año, y recientemente también ha sido visto en Twitter. La infección se consigue a través de la ingeniería social, ya que los usuarios son en su mayoría engañados para hacer clic en enlaces maliciosos integrados en mensajes personales haciéndose pasar por un amigo (que está probablemente infectado).



2. Privacidad – La gente tiende a revelar demasiada información personal online, por ejemplo, sus círculos sociales, comentarios, fotografías familiares, lugares de trabajo, etc. Dejando esto en manos de criminales cibernéticos, esta información puede ser utilizada de manera más eficaz para hackear las preguntas de seguridad online, lo que conduce inevitablemente al robo de identidad. Un hacker también puede utilizar la información para diseñar un ataque dirigido, por ejemplo, un hacker dispuesto a penetrar en la red corporativa de una empresa puede pasar semanas sin dormir, tratando de encontrar un agujero en el sistema de seguridad de la red. Por otro lado, puede encontrar el nombre del contable financiero, invertir cinco minutos para hojear su perfil social, y otros cinco minutos para elaborar un correo electrónico basado en sus intereses (por ejemplo, cría de perros, coches rápidos, lo que sea ...) que lleven un enlace o un documento malicioso.

3. Estafas de *phishing* – Las redes sociales alojan una gran cantidad de información, desde datos personales y perfiles hasta mensajes archivados que pueden ayudar a los cibercriminales en la personalización de mensajes fraudulentos de correo electrónico o sitios web falsos (o mejor conocidos como sitios de *phishing*), diseñados para persuadir a las víctimas a revelar información confidencial, como su nombre de usuario y contraseña o números de tarjetas de crédito.

4. Defectos en sitios web – A principios de junio, se encontró un agujero en Facebook que permitía a los usuarios ver la "información básica" de cualquier otra cuenta, sin importar el nivel de confidencialidad que se había establecido. Esta información puede incluir el nombre de soltera de la madre, a menudo utilizado como una pregunta en los controles de seguridad online. El agujero se resolvió el 23 de junio, pero al igual que el 100% de los elementos de programación, todos los sitios de redes sociales tienen defectos (defectos del servidor, XSS, CSRF...), hasta la fecha, algunas de estas vulnerabilidades se han resuelto, mientras que otros aún están por descubrir, por lo que los usuarios deben actuar con cautela.

5. Spam 2.0 - Una posible razón de por qué los ciberdelincuentes “pescan” (phish) cuentas de redes sociales (o las comprometen con gusanos como Koobface) es con la intención de usar la información para enviar publicidad y spam.

¿qué debe hacer la gente para estar protegida?

Ser precavidos cuando un mensaje suene raro, incluso cuando sea de un amigo, sobre todo si incita a ver un vídeo. Nunca instale los codecs cuando un sitio se lo pide: los populares sitios de “online streaming video” (sitios de transmisión de vídeo online), como YouTube utilizan Flash, por lo que no se necesitan codecs de vídeo. Y si le piden la actualización de Macromedia Flash, no lo instale desde el sitio de redes sociales, es probable que sea un malware troyano. En cambio, visite el sitio web del proveedor de Flash (http://www.adobe.com) y actualice su reproductor Flash directamente desde allí.

En cuanto a la protección de datos: considere toda la información que pone en los sitios públicos de redes sociales, por ejemplo, ya que un potencial reclutador o delincuente cibernético puede mirarlo.