## Las redes sociales son indispensables

Las redes sociales están cambiando básicamente nuestra manera de interactuar, comunicarnos, organizarnos, formar opiniones e incluso hacer compras. Están derribando las barreras, incrementando la transparencia y creando fluidez en todo lo que hacemos. Las empresas, grandes y chicas, ya no pueden ignorar o tratar de bloquear las redes sociales en su entorno ya que actualmente estas vinculan la duodécima parte de la sociedad y están creciendo rápidamente. Son parte de la estructura en la que aprendemos, jugamos y trabajamos.

En realidad, usted debe ir hacia donde está el público objetivo, y es más probable que la gente participe en foros de medios sociales que en cualquier otro espacio. Tanto clientes como socios y empleados esperan relacionarse con usted a través de los medios sociales, que le permitirán mantenerse conectado, reunir comentarios, buscar personal y colaborar. Por ende, debe admitir los medios sociales en su entorno para posibilitar la innovación, el aumento de la productividad y el crecimiento acelerado que impulsarán su empresa.

## Los riesgos de las redes sociales

Todo lo que hace que los medios sociales sean atractivos para los usuarios: la personalización, la facilidad con la que se puede compartir información y el funcionamiento en tiempo real del medio representan riegos significativos para su empresa. Estos son los cuatro riesgos más importantes a los que se enfrenta al usar las redes sociales:

1. **Malware:** en el 2010, los medios sociales se convirtieron en el vehículo de comunicación preferido por los usuarios, quienes pasan más 700.000 millones de minutos por mes solamente en Facebook, lo que hace que los sitios de redes sociales y sus usuarios sean objetivos ideales del malware. Según Sophos, el 40 % de los usuarios fueron infectados por malware de los sitios de redes sociales. Los ataques típicos se aprovechan de la relación de confianza establecida entres los usuarios y sus contactos. Tratan de engañar a los usuarios para que proporcionen información y acceso que puedan ser utilizados para obtener ganancias económicas. Aquí le presentamos algunos ejemplos de malware particularmente exitosos en los medios sociales:

   *Phishing:* con técnicas cada vez más sofisticadas, los atacantes se hacen pasar por uno de sus contactos legítimos de redes sociales y tratan de engañarlo para que proporcione información confidencial, como sus credenciales de inicio de sesión. Se aprovechan de la tendencia de la mayoría de las personas a utilizar las mismas contraseñas para todas sus cuentas, con la esperanza de que al engañarlo para que proporcione un nombre de usuario y una contraseña, podrán obtener acceso a cuentas bancarias, financieras y otras cuentas on-line más rentables.

   La mayoría de los usuarios tienen sus radares ACTIVADOS en lo que respecta a sus cuentas financieras, pero sus inicios de sesión diarios en un sitio de red social son más vulnerables debido a la menor importancia que se les otorga. Este descuido deja el camino libre para que los delincuentes cibernéticos puedan robar activos on-line. Este es el motivo por el cual cada vez más ataques de phishing apuntan a cuentas on-line aparentemente "no relevantes".

   *Click-jacking:* los atacantes lo engañan para que haga clic en un enlace, quizás publicándolo en su muro y luego enviándolo masivamente a sus amigos con un mensaje del tipo "mira esto" o "mira mis fotos". Cuando alguien hace clic en el enlace, sin darse cuenta instala malware (código o script) que puede utilizarse para robar información o para obtener el control de la computadora. Click-jacking utiliza la naturaleza dinámica de las redes sociales y la disposición que se tiene para hacer clic en enlaces de sus conocidos (e incluso de desconocidos), para llegar rápidamente a una gran audiencia, persuadirlo para que revele información privada (por ejemplo, a través de encuestas), reunir clics para obtener ganancias con la publicidad y, en última instancia, que usted permita el acceso a toda su red social.

2. **Pérdida de datos:** las redes sociales consisten en establecer relaciones y compartir experiencias e información, aunque a veces no se pretende que esa información se haga pública. Es común que, sin querer se publique información confidencial, que proporciona "conocimiento privilegiado, por ejemplo: "Recién me encontré con xxx y creo que voy a obtener una gran comisión" o "Me estoy volviendo loco, si no podemos arreglar este error de software pronto, no sé si volveré a dormir". También hubo casos de empleados que publicaron involuntariamente códigos de software patentados en sitios de redes sociales, revelando así propiedad intelectual confidencial. Estas acciones, aunque no sean intencionales, pueden potencialmente violar las reglamentaciones específicas de la industria, afectar su reputación o ponerlo en una posición de desventaja competitiva.

3. **Consumo del ancho de banda:** prácticamente un 40 % de los empleados informan que ingresan a sitios de redes sociales en el trabajo, lo cual crea una sobrecarga potencial en el ancho de banda en detrimento de otras aplicaciones de negocios. El año pasado, cuando el gobierno de EE. UU. reglamentó el acceso abierto a las redes sociales, el tráfico de la red aumentó un 25 %. Solamente los videos (piense en todos los videos que sus amigos comparten y que usted enlaza a través de Facebook o Twitter) pueden sobrecargar muchas redes. Una única transmisión de video generalmente consume entre 500 k y 1,2 Mbps (y ni siquiera en HD, que pueden consumir de 4 a 7 Mbps), y cuando hay decenas o cientos de personas accediendo a videos es fácil ver cómo puede degradarse el rendimiento general.
4. **Pérdida de la productividad:** los sitios de redes sociales se están convirtiendo en destinos on-line, que le permiten publicar y leer mensajes, tener citas, hacer compras, cargar o ver videos y jugar. Todo esto los hace cada vez más convenientes y atractivos para los usuarios, que pasen cada vez más tiempo allí, y a su vez, cada vez más desafiantes para las empresas a la hora de controlarlos de manera apropiada. Cuando no se controla, el tiempo que se pasa en los sitios de redes sociales puede afectar la productividad, ya que los empleados pasan cada vez más tiempo (piense en los 700.000 millones de minutos en Facebook) jugando a Farmville durante el horario comercial.

## Requisitos

Aunque se vea obligado a permitir los medios sociales para competir y prosperar en la economía mundial de la actualidad, no es necesario que exponga su empresa a un riesgo excesivo. Existen maneras de atenuar y protegerse de los riesgos que representan las redes sociales. Específicamente, su solución debe proporcionar:

-> **Una defensa web en tiempo real:** las redes sociales cambian continuamente, así como también las tácticas que utilizan los atacantes para utilizarlas. Por consiguiente, su solución debe analizar el tráfico web sobre la marcha y detectar amenazas ocultas. El análisis en tiempo real de enlaces dinámicamente cambiantes proporciona análisis de riesgos y protección oportuna para mantener la seguridad de los medios sociales. Por lo tanto, cuando vea un mensaje del tipo "Deberías ver esto", puede aceptarlo o rechazarlo en base al riesgo potencial que represente.

-> **Controles selectivos de redes sociales:** para protegerse contra la pérdida de datos y cumplir con las reglamentaciones específicas de la industria, usted debe poder controlar las actividades de sus empleados dentro de los sitios de redes sociales. Por ejemplo, tal vez desee impedir que los empleados carguen adjuntos, fotos o videos a los sitios de medios sociales para así evitar los riesgos de la pérdida de datos involuntaria o los riesgos para la reputación de la empresa. La clave está en tener un control granular de lo que se puede hacer dentro de las redes sociales. Esto requiere una solución que no solo examine de dónde proviene el tráfico inicial (por ejemplo, Facebook, YouTube, etc.), sino que también examine lo que se hace dentro de esa aplicación (correo electrónico, publicación de mensajes, descarga de adjuntos).

-> **Almacenamiento en caché:** no puede permitir que los medios sociales invadan su red y afecten negativamente las aplicaciones fundamentales de la empresa; sin embargo, como las redes sociales se están convirtiendo en una parte integral de la empresa, no puede bloquearlas. Lo que puede hacer es contrarrestar cualquier degradación potencial del rendimiento con el almacenamiento en caché, lo cual le permite almacenar datos y archivos de video localmente luego de una descarga inicial y ponerlos a disposición de los usuarios que quieran acceder a ellos posteriormente. De esta manera, puede permitir el acceso a redes sociales sin perjudicar el rendimiento de otro tráfico en la red.

-> **Flexibilidad para las políticas:** a fin de controlar la productividad, usted debe poder establecer políticas de uso aceptable dentro de los medios sociales. Por ejemplo, puede optar por bloquear el acceso a Farmville durante el horario de trabajo; o si lo permite, quizás desee darle una menor prioridad, de manera que no afecte las aplicaciones fundamentales de la empresa. Con un modelo de políticas flexible, puede controlar y dar prioridad a las actividades que están permitidas o no permitidas, y cuándo. La capacidad de distinguir sitios de redes sociales de aplicaciones o contenido específicos dentro de esos sitios es crucial para establecer una política de uso aceptable eficaz. Entonces, si opta por bloquear los juegos, puede bloquear tanto los juegos independientes como los juegos dentro de los sitios de medios sociales.

Las soluciones de seguridad web de Blue Coat lo ayudan a alcanzar el nivel de protección, rendimiento y control que necesita en los medios sociales para poder aprovechar sus beneficios. Para obtener más información detallada sobre las soluciones de seguridad web de Blue Coat, visítenos en www.bluecoat.com/products.

Blue Coat Systems, Inc.
www.bluecoat.com

Sede Corporativa
Sunnyvale, CA USA // +1.408.220.2200

Blue Coat Brasil
São Paulo // +55 11 3443 6879

Blue Coat México
México D.F. //+52 55 3300 5825

Blue Coat Argentina
Buenos Aires //+54 (11) 4850 1215