CONTENIDO

Seguridad en sitios de Redes Sociales

Los sitios de redes sociales o simplemente redes sociales son grupos de personas que comparten información en Internet a través de un software que permite establecer relaciones de confianza entre los participantes, es Vdecir gracias a estos programas podemos compartir fotografías o comentarios, entre otras cosas, a las personas que se desea. Entre este tipo de redes encontramos a MySpace, Hi5, Orkut, Friendster, etcétera.

En los últimos años hemos podido observar un incremento considerable en el número de usuarios de éste tipo de servicios. Y es que este tipo de servicios permiten que las personas encuentren una nueva manera de conocer personas que tengan intereses en común y finalmente de hacer amigos, lo que combinado con ciertas funcionalidades, como el hecho de compartir archivos, imágenes y/o videos, generan una sensación de cercanía entre los integrantes de las redes sociales. Sin embargo esta tecnología ha sido víctima de usuarios malintencionados que buscan obtener algún beneficio personal de dichos servicios.

Algunos de los principales peligros en los sitios de redes sociales son:

- Robo de identidad. Usualmente los usuarios de redes sociales publican información personal, sin embargo si la información publicada no es protegida de manera adecuada estableciendo restricciones para que sólo las personas autorizadas puedan tener acceso es posible que usuarios malintencionados utilicen la información en situaciones de robo de identidad o para obtener mayor información acerca de los usuarios.

“La usurpación de identidad es un caso frecuente”

- SPAM en redes sociales. Debido a que en las redes sociales es posible enviar mensajes a los demás contactos de la red, estos servicios son susceptibles de ataques de spam que en ocasiones no sólo contienen publicidad sino también pueden contener enlaces a sitios con contenidos maliciosos (virus, spyware, etc.).

- Acoso. A través de las redes sociales, acosadores encuentran un lugar ideal para acechar a sus víctimas, pues a través de este medio pueden desde conocer las actividades que realizan sus víctimas hasta tener contacto con ellos.

- Difamación. Debido a que los sitios de redes sociales no comprueban la identidad de la persona que crea un perfil, un usuario malintencionado podría generar un perfil de una persona en particular y publicar información falsa con el objetivo de difamarla. Además de ello debido a que es posible enviar mensajes a otros contactos que sean visibles al público, usuarios malintencionados

podrían publicar información que sea vergonzosa para un usuario o grupo de usuarios.

- Códigos maliciosos. Los intrusos han encontrado maneras de propagar códigos maliciosos como virus o spyware a través de las redes sociales. El problema es que haciendo uso de estos servicios pueden elevar sus probabilidades de éxito pues explotan la confianza generada entre los usuarios de la misma red.

Pero, ¿es posible utilizar de manera segura las redes sociales?

Existen diferentes medidas para protegerse de los peligros de las redes sociales como las siguientes:

- Utilizar una contraseña robusta. De este modo es posible prevenir que algún atacante descubra fácilmente la contraseña utilizada. Es importante mencionar que la contraseña es la llave para acceder a nuestro perfil de redes sociales de modo que si un atacante lograra descubrirla podría realizar cambios al perfil o enviar mensajes basura a nuestros contactos.

- No aceptar contactos desconocidos. Aceptar contactos desconocidos incrementa las posibilidades de recibir mensajes SPAM o mensajes con ligas a sitios fraudulentos o con contenido malicioso.

- Ser precavido en la información publicada y permitir que sólo los contactos de nuestra red de amigos puedan ver esos datos. Al momento de publicar información se debe tener cuidado de no publicar información confidencial como números de cuenta o contraseñas. Así como teléfonos o direcciones tampoco deberían de ser compartidas por este medio pues si algún usuario que desconocido tuviera acceso a esta información podría terminar en casos de acoso o publicidad.

“ Los intrusos han encontrado maneras de propagar códigos maliciosos”

- Reportar cualquier caso de SPAM o abuso. Reportar los mensajes SPAM ayudará a prevenir que se sigan multiplicando estos ataques utilizando una misma cuenta.

- No almacenar contraseñas de acceso en equipos compartidos.

- Cerrar la sesión cuando se termine de utilizar el servicio.

- Mantener actualizado el explorador. Esto permitirá estar protegido contra ataques que exploten fallas en el navegador de internet.

- Procura no visitar estos sitios en equipos de acceso público como los Café Internet. Muchas veces los equipo compartidos pueden contener herramientas maliciosas capaces de capturar todo lo que escribes, incluyendo usuarios y contraseñas, de este modo podrían posteriormente entrar a tu cuenta y realizar los cambios que deseen.

Otro punto que se deber considerar es que no todo lo que se recibe proviene de la persona que supuestamente lo envió. Como se comentó anteriormente la usurpación de identidad es un caso frecuente en las redes sociales, por ello es importante corroborar con la fuente si en verdad ellos publicaron el mensaje recibido

Redes Sociales en la escuela

Los problemas de acoso, acecho y difamación, así como las distracciones ocasionadas en los alumnos y maestros por el uso de las redes sociales han provocadto que algunas instituciones educativas implementen políticas que restrinjan su uso. Pero, ¿es esta la medida correcta para prevenir estos problemas?

Para responder esta pregunta es necesario explicar por qué existen estos problemas en las redes sociales. Los sitios de redes sociales basan su funcionamiento en la creación de un perfil personal y el establecimiento de relaciones de confianza entre los integrantes lo que permite establecer grupos donde es posible compartir información. Entre la información compartida encontramos datos personales como nombres, país, intereses, fotografías y, en ciertos casos, es posible obtener la dirección o teléfono de una persona.

Y desafortunadamente no todos los usuarios de estos servicios tienen buenas intenciones. Los casos de acoso y acecho en ocasiones ocurren como consecuencia de la información publicada yal hecho de que los usuarios no siempre son restrictivos con las personas que pueden acceder su red de amigos, de esta manera es posible obtener la información necesaria para acosar a una persona o un medio más para realizarlo.

Los casos de difamación podemos visualizarlos de dos maneras distintas, el primero cuando los contactos de un cierto usuario publican mensajes que podrían avergonzarlo y el segundo cuando un usuario adopta la personalidad de otro y crea un perfil para posteriormente publicar información que podría afectar la imagen de la otra persona, por ejemplo pensemos en un artista famoso y en un fan molesto, el fan podría crear un perfil de redes sociales a nombre del artista y posteriormente publicar mensajes falsos acerca de su vida personal.

Sin embargo, los sitios de redes sociales pueden proveer un espacio de interacción entre estudiantes quienes pueden crear verdaderas comunidades de intercambio académico, imaginemos una comunidad creada por estudiantes universitarios interesados en biología, al conformar un grupo de redes sociales podrían intercambiar información acerca de sus intereses, aclararse dudas, recomendarse artículos o métodos de estudio.

Es por ello que es importante encontrar un equilibrio. La restricción total de los sitios de redes sociales en las escuelas no protege a los estudiantes u otras personas de los peligros existentes, sin embargo las instituciones educativas podrían capacitar a su personal para que esté preparado para brindar asesoría cuando ocurran estos casos. Además de ello es posible que las universidades establezcan acciones que permitan concientizar a los usuarios de los peligros existentes y de los métodos de protección disponibles.

5 consejos prácticos para mejorar la privacidad en los sitios de Redes sociales

Garantizar la privacidad en los sitios de redes sociales es uno de los principales retos de seguridad y aunque los proveedores pueden proporcionar de herramientas que protejan nuestra información, nosotros como usuarios podemos llevar a cabo algunas acciones a favor de nuestra privacidad.

¿Qué hacer cuando tenemos múltiples servicios de redes sociales?

Como usuarios podemos utilizar más de un sitio de redes sociales pues a través de diferentes redes podemos encontrar más amigos o personas en común. El problema de esto es que en cada sitio de redes sociales se proporciona información distinta acerca de nosotros, de manera que si un usuario malintencionado tuviera acceso a nuestros múltiples perfiles podría complementar la información y crear un expediente completo acerca de nuestra persona. Así que la recomendación es ser precavido de la información publicada en cada servicio.

Sitios como Orkut, facebook, friendster, MySpace y hi5 son sólo algunos ejemplos de sitios de Redes Sociales

¿Debo permitir que cualquiera sea mi "amigo"?

Uno de los puntos más importantes en sitios de redes sociales es la popularidad y ésta se adquiere en función del número de usuarios que pertenecen a nuestra red, así como de la cantidad de información que publiquemos y de la cantidad de comentarios que realicemos o que nuestros amigos nos envíen. La existencia de los niveles de popularidad puede provocar que los usuarios no tomen en cuenta a quien dejan entrar a su red de amigos, por ello te recomendamos que sólo a las personas que les tengas confianza permitas el acceso a tu información personal.

Es frecuente aceptar personas de las cuales sabemos poco.

¿Es recomendable compartir información de mis amigos con terceros?

Debido a que en las redes sociales se conforman grupos de intereses comunes, es posible que algunos usuarios puedan obtener información acerca de nosotros mediante nuestros contactos, por ejemplo un desconocido podría preguntar a uno de nuestros amigos nuestro correo electrónico argumentando que nos conoce. Si nosotros proporcionamos información de nuestros amigos podríamos exponerlos a ataques de acoso o acecho, aún cuando no sea nuestra intención. Por ello es mejor sólo compartir información con personas que hemos conocido previamente y siempre que nuestros contactos lo autoricen.

¿Existe algún riesgo si publico fotografías?

No existe un riesgo directo por hacerlo, sin embargo las fotografías aportan mayores detalles acerca de nuestra persona, como lugares que nos gusta visitar, a quienes frecuentamos, cómo nos gusta vestir, etcétera. Pero también es tuna manera de mejorar la interacción con nuestros amigos, así que la recomendación en este caso es solamente compartir fotografías a nuestra red de amigos y restringir su exposición al público en general. No olvides que al publicarla en internet podría ser vista por millones de personas.

¿Qué hacer si uno de mis contactos envía mensajes ofensivos?

Algunos sitios de redes sociales cuentan con un botón de Reporte de Abuso que al dar clic nos permite notificar si algún usuario hace un uso inadecuado de la red, como por ejemplo publicar pornografía o enviar mensajes ofensivos a los demás. Así que notificar estas actividades ayudará a eliminar usuarios malintencionados.

Buenas prácticas de seguridad

Seguridad en Mensajeros Instantáneos

Los Mensajeros Instantáneos son los programas que comúnmente utilizamos para comunicarnos con otra persona en internet en tiempo real por ejemplo MSN Messenger, AOL Messenger, Yahoo Messenger, entre otros. Estos programas tienen grandes ventajas ya que no sólo los utilizamos para comunicarnos, sino también nos permiten intercambiar archivos de trabajo, videos, fotografías, etcétera.

Desafortunadamente los intrusos han desarrollado diversas técnicas para transmitir virus o malware utilizando a los mensajeros, estas técnicas van desde aprovechar alguna vulnerabilidad en el mensajero hasta enviar mensajes para que el usuario descargue algún archivo infectado haciéndolo creer que proviene de alguno de sus amigos. Además existen algunas técnicas con las cuales los intrusos pueden ver las conversaciones o también capturar todo lo que se escribe en el teclado haciendo uso de algunos programas denominados keyloggers.

De manera que dejar de utilizar los mensajeros para no ser atacado parecería la mejor opción, pero ¿acaso no existen otras alternativas? Por supuesto que sí, a continuación proporcionamos algunas recomendaciones para protegerse de posibles ataques:

- Utilice la última versión del mensajero de su preferencia, así disminuirá los huecos de seguridad existentes en versiones anteriores y evitará que el atacante tenga éxito si intenta aprovechar alguno de estos huecos.

- Verifique si existe alguna actualización para su mensajero, esto se puede realizar a través del sitio web del distribuidor, pero en la mayoría de las ocasiones los mensajeros advertirán que una nueva versión o actualización ha sido liberada así que cuando suceda no olvide instalarla.

- No envíe mensajes que contengan contraseñas o información sensitiva como números de tarjetas de crédito, números de cuentas bancarias, NIPs, saldos, etcétera.

- No abra ninguna liga que invite a visitar cierta página o descargar algún archivo, a menos que el contacto, de quien recibe el mensaje, confirme que fue él quien lo envió.

- Evite almacenar su contraseña en equipos compartidos.

- Agregue o acepte solamente a contactos de confianza.

- Utilice algún antivirus y manténgalo actualizado, así incrementará la seguridad de su equipo.

- Si tiene conocimientos intermedio/avanzados podría utilizar alguna herramienta de cifrado para la comunicación de los mensajeros.

Seguridad en Reproductores de Audio y Video

Los reproductores de Audio y Video son programas que utilizamos para reproducir música y/o videos en diferentes formatos (mp3, avi, wma, etc.), entre ellos encontramos a Windows Media Player, Winamp, iTunes y otros muchos. Algunos integran funcionalidades extras como cambiar su apariencia (skins) o convertir música a otro formato (por ejemplo convertir la música de un CD a mp3).

Y a pesar de todas las ventajas que tiene utilizar estos programas existen algunos riesgos que podrían dañar a nuestra computadora, algunos de ellos consisten en manipular un archivo de música o video para que al momento de ser reproducido ejecute instrucciones que permitan instalar programas o virus; otro de los riesgos es que al descargar skins de páginas no confiables podríamos descargar e instalar algún virus, spyware o publicidad no deseada.

Como medidas de protección recomendamos:

- Mantener actualizado su Reproductor. Las actualizaciones se pueden conseguir del sitio oficial del distribuidor y en algunos casos el reproductor alertará sobre nuevas actualizaciones.

- Mantener su antivirus actualizado y cuando desee reproducir un archivo nuevo, primero solicite al antivirus que lo analice en busca de actividad maliciosa (virus o malware).

Seguridad en Juegos

La computadora no es solamente un instrumento de trabajo y por ello se han desarrollado algunas aplicaciones para nuestro entretenimiento, entre ellas encontramos los juegos. De ellos existe una gran variedad como juegos de estrategia, de rol, azar, educativos, etcétera y los riesgos a los que nos enfrentamos dependerán del modo de adquisición:

Juegos descargados de Internet

En Internet podemos encontrar algunos juegos que podemos descargar e instalar en nuestras computadoras. En este caso debemos tener mucho cuidado ya que aquellos que proceden de páginas no confiables y normalmente gratuitas podrían contener algún tipo de virus o spyware; así que si descarga este tipo de archivos no olvide analizarlos con su antivirus antes de instalarlos.

Juegos en línea

Existen algunos juegos en los que para utilizarlos necesitamos estar conectados a Internet y su modo de juego puede ser individual o con otras personas en la red. Existe peligro en estos juegos ya que algunos usuarios podrían enviar algún virus o malware sin que el usuario se dé cuenta. También podría al momento de abrir la página del juego podría instalarse algún programa dañino, pero es posible protegerse si el antivirus y antispywarfe se encuentran en modo de autoprotección para que verifique que estos archivos no serán instalados ni ejecutados en el equipo.

Juegos en CD

Los juegos que adquirimos en lugares autorizados y que por lo tanto son originales no representan un riesgo directo a nuestra computadora, sin embargo si son adquiridos de manera ilegal (piratería) existe el riesgo de que el software venga contaminado con virus. En este caso recomendamos adquirir juegos originales y en caso de que se desconozca la procedencia del juego cuide que el antivirus este actualizado y en modo de autoprotección. Además mantener actualizados los juegos instalando los parches que proporcione el distribuidor.

Seguridad Para Niños

HISTORIETAS
USUARIOCASERO
www.seguridad.unam.mx/usuario-casero

No muy lejos de ahí, Wormnia observaba a las PC's de los usuarios.

No te preocupes te voy a actualizar, así estarás protegido contra ataques del Equipo Malicioso.

Muchas gracias Mr. Update.

Es mi oportunidad de multiplicarme en todas las PC's que no hayan instalado la actualización de seguridad.

¡Debo encontrar cuales PC's están vulnerables!

Wormia identifica las PC's vulnerables e inmediatamente utiliza sus poderes de HyperVelocidad y Clonación para poder copiarse rápidamente en ellas

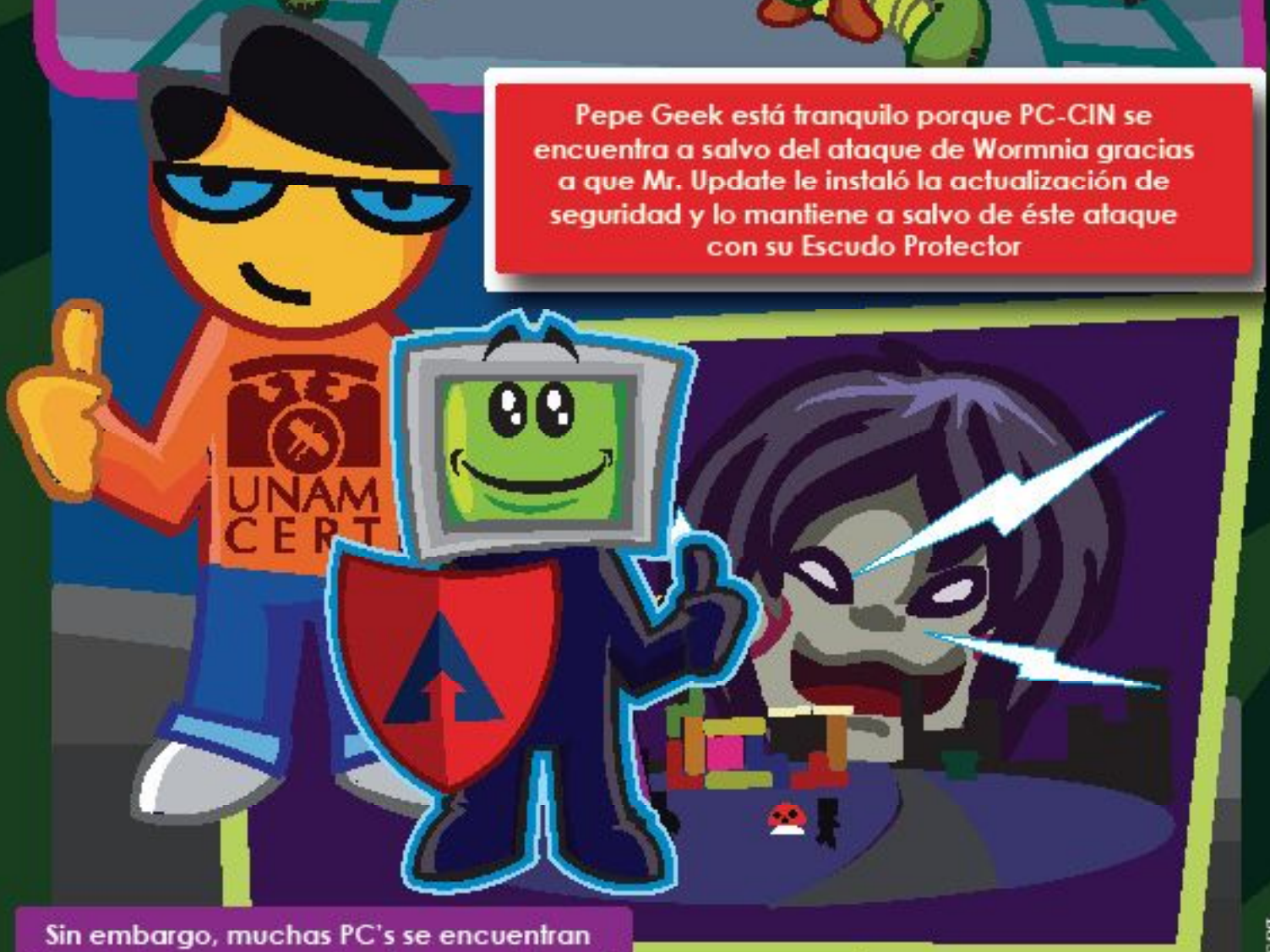
NOOO...!!

ff

HISTORIETAS
USUARIOCASERO
www.seguridad.unam.mx/usuario-casero

Finalmente, Wormnia ha infectado a los equipos vulnerables, los cuales disminuyen su rendimiento y pueden caer en manos de un intruso

Pepe Geek está tranquilo porque PC-CIN se encuentra a salvo del ataque de Wormnia gracias a que Mr. Update le instaló la actualización de seguridad y lo mantiene a salvo de éste ataque con su Escudo Protector



Sin embargo, muchas PC's se encuentran infectadas y las comunicaciones en Internet podrían comenzar a colapsarse

Continuará...