



## Social Networking Threats

Social networking sites are an increasingly popular way for people to keep in contact with friends, family and business colleagues. These sites offer a rich set of features that enable users to share personal information as well as videos, music, and images with members of their network—all in the name of keeping their contacts updated on what goes on in their lives. Although the ability to share information and multimedia files are among social networking sites' greatest strengths, hackers see these assets as new vectors to attack unsuspecting users.

With the increased use of these sites in the workplace, businesses should examine and understand the risks social networking sites pose to the enterprise.



**Kevin Haley**  
Director, Product Management  
Symantec Security Response

Kevin Haley is Director of Product Management for Symantec Security Response where he is responsible for ensuring the security content gathered from Symantec's Global Intelligence Network is actionable for its customers. This includes educating customers on security issues and incorporating the security content into Symantec's enterprise and consumer product lines. The valuable security data provides the basis for protecting customers against complex Internet threats and other security risks.

During his nine years at Symantec, Haley has leveraged his security expertise in the development of

### **What kind of security threats do social networking sites pose to the enterprise?**

The threats posed by social networking sites are generally the same for consumers and enterprise users.

First, people often divulge considerable amounts of personal information on these sites, including details about their employment. Attackers use information gathered from social networking sites to carry out targeted social engineering attacks, tricking victims into downloading malware or into divulging sensitive company information.

Another threat to consider is the possibility that the site itself could get compromised. If an attacker is able to compromise the social networking site with malicious code, any visitor to the site would be susceptible to attack. Hackers have also found ways to insert malicious code into advertisements, which are often provided to social networking sites through third party vendors.

### **Aside from phishing and other targeted attacks, how are social networking sites used to propagate malicious code?**

Social networking sites provide users with a wide variety of customization options and third party applications. Users can customize details in their profile, include links to other sites, upload images, videos, and in some cases users are even allowed to embed code into their profile page.

The problem is that hackers can do all of these things as well and they see all of these features as potential attack vectors. For example, they can customize their own profile or hijack another user's profile to gain access to a social network and use information gathered from others to carry out a social engineering attack. Posing as a member of a social network, hackers can also post links, videos, and images to distribute malware.

### **How do hackers use social engineering and pretexting techniques to make the most effective use of social networking sites?**

Targeted attacks that use social networking and pretexting techniques have become more common. Attackers rely on users posting significant amounts of personal information to help them craft an attack. Sometimes they even hijack a user's profile and then propagate an attack throughout the victim's network of contacts, leveraging trust among friends.

the company's antivirus solutions for endpoints and mail servers, and in creating network and system management solutions. Most recently, Haley managed a global team of technical product managers who evangelized Endpoint Security Products and were responsible for field enable and technical training for SAV, SCS, SEP v11.0 and SNAC 11.0.

Before joining Symantec, Haley was part of the OpenView group at Hewlett-Packard, working on the company's software distribution tools. Prior to Hewlett-Packard, Haley was a product manager at Sun Microsystems, where he managed the development and delivery of network and server software for Solaris on Intel.

###

If you have a question for our expert, please contact:

Pamela Reese at Symantec  
(424) 750-7858  
or  
Connect Public Relations at  
(801) 373-7888

### **How do spammers exploit social networking sites?**

Any site that displays easily accessible, real-world email addresses would naturally give spammers a quick and easy way to bolster or update their address lists. Most sites have policies and technologies to address this and display full email information only when appropriate and only if the user has configured their account to make that permissible.

Spammers still find ways around security measures social networking sites put in place to limit the amount of in-network spam. For example, once an attacker has infiltrated a person's network of friends, they can send emails with malicious code or find other ways to install scripts on victims' machines to harvest email addresses from the social networking site itself or a victim's address book. Again, these attacks are more effective because the recipient 'knows' the sender. A social engineering attack increases the likelihood that the recipient will read the messages and click on the links included with the message.

### **How does the convergence of social networking sites and virtual worlds affect the threat landscape?**

Virtual worlds are similar to any social networking site and security threat trends often mirror those found elsewhere online. Also, virtual worlds involve increasingly complex client software in order to render graphics and interact with the world on the user's behalf. In general, increased complexity often leads to increased potential for vulnerabilities, thus creating more opportunities for attackers.

Furthermore, as people interact with each other and social networks form in virtual worlds, we will see various types of virtual world fraud that leverages the underlying social context in much the same way that real world fraud does. There are several reasons for this:

- Material gains in virtual worlds can have real-world impact. There are often secondary markets where goods inside of virtual worlds can be bought and sold for real currency. Attackers go where the money is.
- Virtual currencies and goods are not regulated. Therefore, the legal implications for performing theft are murky. That's good news for the attacker.
- Converting virtual currencies and goods can provide a money laundering mechanism. Because currencies and goods can be traded inside the virtual world and then subsequently sold into secondary markets for real money, it becomes difficult to trace a crime.
- Many people are willing to go to great lengths to acquire assets inside a virtual world, and might compromise their security in the process. For example, suppose that the virtual world takes the form of an online game. If a hacker posing as a player or game administrator offers you a tool that claims to improve your performance in the game, you might use that tool without thinking through the repercussions. The tool could really be a keystroke logger in disguise. Virtual worlds offer really interesting opportunities for attackers, and to the extent that attackers can use social context in these worlds, they will be that much more powerful.

**In the past few years, business-oriented social networking sites have increased in use, even by top-level executives. What security implications should enterprises consider regarding these sites?**

In general, business-oriented social networks can be safe as long as users take some precautions. First, be careful with information you put on your profile. Any information you disseminate to a social networking site is no longer in your control. Don't reveal anything that you wouldn't want to be made public.

Also, be selective of people you allow into your network. It is generally not a good idea to link to someone you do not know, even if they say they know you. One risk lies in the sometimes automatic nature in which users accept invitations from people claiming to be past business acquaintances. Once you allow them into your network, they can more easily gain access to all of your contacts and subsequently attempt to target them.

The human element presents enterprises with perhaps the greatest danger of social networking. In the case of phishing, users are often too trusting and open themselves and their employer up to attack. If a hacker wants to target company XYZ, it's not difficult to find an employee from that company on a social networking site. All an attacker would have to do is make friends with one or several employees, gather sensitive information about the company and its IT infrastructure, and launch an attack.

**What policies and technology solutions should enterprises put in place to protect themselves?**

Ensuring that IT infrastructure is running good and up-to-date security software is always important. Policy compliance software can also go a long way to ensure that unauthorized client software is not installed on corporate computers. Beyond that, unless the company requires it, consider disabling access to popular social networking sites at the perimeter for both security and productivity purposes. One must not assume they are entirely safe due to the software and tools they use. Users across the enterprise need to modify their behavior as well.

IT administrators should keep in mind that it is human nature to want to take the short and quick path. Companies should train employees and executives to question the validity of URLs they see or receive in emails, even if they come from friends and coworkers. Enterprise users should also be wary about opening and viewing emails sent from users they do not know. For example, social networking also extends beyond sites and reaches users through chain-letter emails and e-cards as well. These can be used to both infect user systems with malware or to harvest email addresses. Each time an email is read, a request can be sent to the server hosting the image divulging the user's email address.

**What can companies do to educate employees on how to protect themselves and the company from threats associated with social networking sites?**

Security awareness training can go a long way to protect the enterprise from Internet-based attacks. Employees and executives alike should be made aware of the threats that exist and how to guard against them. Corporate Internet security policies should be put in place and all users need to have a clear understanding of why and how to comply with these policies.

Still, network administrators need to keep in mind that while awareness campaigns address part of the problem, hackers are constantly adapting. Companies must keep current on security trends that target enterprise users. Because user behavior can be so unpredictable, it is wise to invest more heavily in security technologies, like high-quality endpoint security products. If your machine is protected, this forms a critical last line of defense.

**What best practices should be implemented to protect against malicious threats?**

Two of the most important best practices mentioned above are to be careful of who you allow to join your network and filter which information you publish on the site. Additionally, do not run programs sent to you by others, even your own friends or contacts, without first confirming via a side channel that it is legitimate. Also, when you browse to a social networking site, have the latest version of a reputable Internet security suite on your machine. For example, the software you use should have browser protection that is capable of blocking a wide class of web-based threats. Also, if the social networking site has privacy options, make sure that these are set as strictly as your normal usage of the site allows.

For social networking site administrators, user confirmation scripts such as captchas can be added to verify that postings are from actual users versus automated systems. Even though these systems can be successfully bypassed by bots, it will reduce the risk from less technically savvy hackers. A more successful approach would likely involve the utilization of a behavior-based antivirus solution to detect potentially malicious code in a virtual environment, prior to the site allowing data to be uploaded.