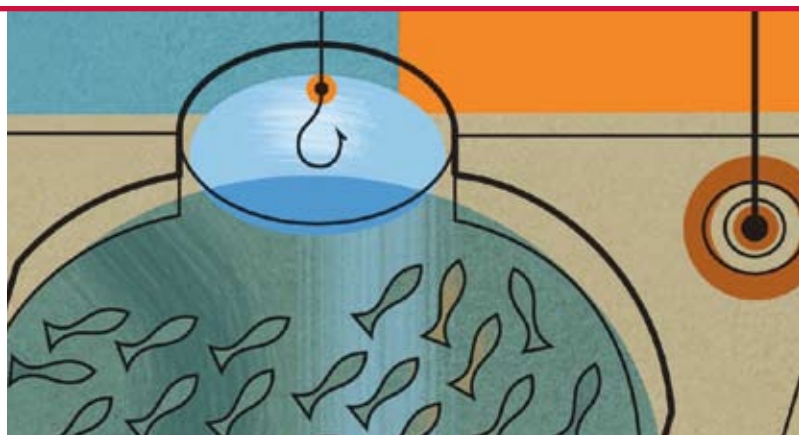


# The Future of Social Networking Sites

By Craig Schmugar



In recent years social networking sites—MySpace, Facebook, and others—have become household terms. Many people think of social networking on the Internet as a relatively new phenomenon

when, in fact, sites such as Classmates.com and SixDegrees.com have been around for more than a decade. Still, the growth explosion has occurred only during the past few years. So what exactly makes a site a “social networking” venue? At the core, social networking sites are those that comprise an online community which allows users to share information, discover new contacts, and reconnect with old ones.

Social networking sites are significant for two main reasons. First, they are the epitome of Web 2.0, in which the network of users is the platform and the community drives the content. The platform grows through user contributions, enabled by applications provided for community use. Second, social networking sites combine elements of communication channels—such as email, message boards, instant messaging, and chat—with media vehicles—such as audio, video, and print. In these communities, like-minded individuals can share information and interests and provide feedback and reviews. Such sites can act as collaborative platforms, allowing entire networks to grow in value as the user base increases. Furthermore, these platforms allow for the most direct and targeted media outlets ever seen; businesses can focus their marketing efforts on those who are truly interested. Social networking sites contain a warehouse of information that can be mined and analyzed to expand user profiles and to build complex diagrams and maps of user-to-user and user-to-interest relationships.

Key to the success of any social networking site is a strong and loyal user base. Friendster.com knows this all too well.

Friendster was the precursor to MySpace and by far the number-one social networking site during its prime. What happened to it? Friendster was a sort of success catastrophe. As the user base

grew more massive and the content evolved (including the addition of games), the back end failed to keep up with the growth. Site administrators were forced to restrict high-bandwidth content, but even still performance was unsatisfactory and the user base jumped ship. Furthermore, Friendster attempted to fit the user base into their predetermined model of how the network should be used and by whom.

MySpace provided a more robust platform, not only because of its greater bandwidth, but also in the level of freedom users enjoyed to create, modify, and view a wider variety of content. Once the word got out that MySpace was the new Friendster, it didn't take long for a majority of users to make the switch.

A few takeaways from this early battle in social networking are that the platform needs to be flexible, it needs to expand and evolve, and user retention is key. These principles are paving the way for the future of social networking sites.

## Social Insecurity

MySpace was able to overtake Friendster in part by allowing users to highly customize their profiles. But this opened the door for attackers to insert malicious code as well as launch convincing phishing attacks directly from their MySpace profiles.

Unfortunately such user flexibility lends itself to exploitable conditions, which the bad guys use and abuse. In a race for market share and in an effort to avoid being the next Friendster, security has taken a back seat for many social networking sites. Consequently, social networking sites have been hosts to worms, phishing attacks, vulnerabilities, data harvesting and leakage, rogue ad distribution, defamation, and last, but not least, spam.

## Where Are We Now?

Two and a half years after Samy, the first widespread social networking worm released on October 4, 2005, hit the scene, most old security vulnerabilities had been patched. But the problem has not gone away. Until security flaws result in fewer subscribers, vulnerabilities will be common, and cross-site scripting vulnerabilities, such as that exploited by Samy, are one of the most widely reported types of vulnerabilities in the Common Vulnerabilities and Exposures database.<sup>1</sup> And the situation is likely to get worse before it gets better.

In May 2007, Facebook launched the Facebook platform, which allowed third-party developers to author and market applications to Facebook's 20 million active users. One year and 50 million additional users later, more than 20,000 Facebook applications have been developed, with 95 percent of the user base having run at least one application.<sup>2</sup> These applications pose additional risks—as users may have a false sense of security because of the applications' association with a site they trust, Facebook.com. Yet the vast majority of these applications are released by developers without prior review by the site.

In January 2008, Facebook banned the application Secret Crush after it was reported to have led users to install Zango adware.<sup>3</sup> (See Figure 1 for other examples of widespread threats.) The significance is that Facebook doesn't review applications, and things can (and have) "slipped" by. Although this reported case was more of an annoyance (adware), the next could be much worse.

### Profiled social networking threats

THREAT	TYPE	SITE
Grey Goo	worm	Second Life
JS/QSpace	worm	MySpace
JS/SpaceFlash	worm	MySpace
JS/SpaceTalk	info stealer	MySpace
Kut Wormer	worm	orkut
Mass leak of private photos	data loss	MySpace
PWS-Banker! 1d23	password stealer	orkut
Samy	worm	MySpace
Scrapkut	worm	orkut
Secret Crush	unwanted program	FaceBook
Xanga Worm	worm	Xanga

Figure 1: Worms and other threats have plagued social networking sites. Users often trust their community sites too much.

Each time you click a link, rate a blog, or chat on a specific subject, the site can gain intelligence about you to enhance your social network.

Approximately nine months after Facebook launched its platform, MySpace followed suit, and recently Google released an application program interface (API) for orkut, Google's social networking site. Although these platforms have set the stage for the next generation of social networking sites, they have also created another vector for attackers to exploit.

## What Lies Ahead?

Future social networking sites will become more important because platforms will expand further. "Killer apps" will include mobility, presence, and location awareness, with the goal of making your physical life more convenient through your virtual network; you'll have a traveling social network in your back pocket. Not only will you be able to know which of the friends in your network is online, but you'll also be able to know which are nearby. Cell tower triangulation and global positioning systems will be able to pass along your location to whomever you allow. Location-aware services could match local businesses and entertainment to your interests based on your profile. Business travelers could more easily rendezvous with coworkers and clients at conferences and trade shows. The thrill of online dating could be heightened through the creation of location-specific communities, so you wouldn't only meet someone online, but you could also chat with a prospective mate in the same room.

Social sites will also be smarter, mining user information across the web. Social bookmarking site functionality such as Digg will be married with social networks and enhanced with self-learning technology such as Pandora or StumbleUpon and tagging functionality such as Flickr. The result is a more constant and refined stream of relevant information, which actually educates and informs the community in a much more efficient manner than occurs today.

From your iPhone, you'll be able to get movie recommendations from those in your network. You'll also be able to read reviews that your friends found helpful and find show times for the theaters in your vicinity, and then you'll be able to check the location of your friends to determine how quickly they can meet you.

Sites will understand your interests based on your behavior: web sites you visit, articles you read, music you listen to, friends you chat with and what their interests are, for example. This information will be used to keep you current on changing events and to filter the noise that bombards users today. You'll be left with a highly customized web experience that requires very little direct user input. Whereas Web 1.0 was driven by site administrators and Web 2.0 was driven by user-generated content, the future of social networking lies in user and content relationships augmented by user behavior to tailor content.

Early incarnations of next-generation sites, called Social Networking 3.0, may in fact be perceived as spooky in the level of accuracy of this "artificial intelligence." Profiling takes on a different meaning in this realm, where the site can actually bring together users of similar interests. In some respects, compatibility profiling used by online dating services could be considered an early incarnation of creating social connections through online profiling, bringing compatible people together; but in Social Networking 3.0 this concept is significantly expanded without the need to complete a lengthy questionnaire. Each time you click a link, rate a blog, or chat on a specific subject, the site can gain intelligence about you to enhance your social network.

Who will benefit from this explosion of information correlation? Of course, the user base is a driving factor, but others seek to benefit from this arrangement. Advertisers are drooling at the notion of higher conversion rates when marketing happens at the users' level based on their specific interests. More users will actually pay attention to the ads and take an interest in their content.

## Risks Increase

As user benefits increase, so will opportunities for attackers. Spammers and scammers will look to exploit this treasure trove of information and will more easily construct convincing social engineering attacks with all this data. Users will be taken off guard by the level of detail and personalization in attack messages. Social botnets will also have the potential to seriously disrupt the ecosystem, poisoning the network with solicitations and false testimonials. Site administrators will have their work cut out for them to keep the content quality high, while blocking the bad guys and still allowing everyone else to use the site as it is intended.

Securing future social networks will depend more heavily on server-side defenses. Back-end systems will need to scan large amounts of incoming and outgoing data, searching for evidence of mischief or malicious code. Site and content reputation services may help balance usability and security. The trust relationship between sites and users is key to the success of tomorrow's networks. Violation of that trust could lead to the failure of an entire community.

The increased use of open and portable profiles, mash-ups (web applications that combine content from various sources into a single tool), and open APIs will dramatically facilitate cross-site usage, but will also increase the complexity in defending against threats targeting these vectors. Multitiered attacks are difficult to pinpoint today and will be even more so tomorrow. Attacks may originate from one site only to be propagated through another before appearing on an affected social network. Host-based defenses will need to negotiate the relationships sites have with one another to piece together valid and invalid site interactions and weed out the good from the bad.

Many users will find the privacy concerns in this article—information harvesting and correlation, and location tracking—to be too great to ignore. Indeed, many people will not opt into such services. However, when users see that they can benefit from providing a little bit of data and they have established trust relationships, many of them will volunteer some details. Vendors are acutely aware of this and are encouraging users to take baby steps, such as allowing locations to be reported granularly only by state or city, for example. Unfortunately, online predators will be lurking, and security vulnerabilities can have dire consequences when such information falls into the hands of the bad guys.

This is an exciting time for social networking sites, which are rapidly expanding, adding functionality, and growing their user bases. These sites have multibillion-dollar valuations. Big changes lie ahead that are both compelling and threatening; in many ways the future of social networking sites defines the future of the Internet itself.



Threat Researcher **Craig Schmugar** has been researching and combating threats for McAfee Avert Labs since 2000. Since then he has discovered and classified thousands of new threats, including the Blaster, Mydoom, Mywife, and Sasser worms. He admits that during this time he is starting to feel more anti-social.

### ENDNOTES

- 1 <http://cwe.mitre.org/documents/vuln-trends/index.html>
- 2 <http://www.facebook.com/press/info.php?statistics>
- 3 <http://www.zdnet.com.au/news/security/soa/Spyware-claims-kill-off-Facebook-Secret-Crush/0,130061744,339284896,00.htm?omnRef=http://www.google.com/search?num=100>