

**THINK THERE'S NO CLEAR
ANSWER TO COSTLY SECURITY?**



[Print This Article](#)

[<< Return to Social network security: Social anxiety](#)

Social network security: Social anxiety

Dan Kaplan

August 07 2009

Users of social networking sites are feeling the stress of cybercrooks, says Virginia Tech's Randy Marchany.

After a deranged student's shooting rampage killed 32 classmates on a spring morning two years ago at Virginia Tech University, one of Randy Marchany's first priorities was accounting for the seven students who worked in the school's information security office.

Marchany, director of the Virginia Tech IT Security Testing Lab, was able to confirm that six of them were unharmed. But one remained unaccounted for – and it was known that this student took classes in the engineering building, where most of the shootings occurred. With phone lines jammed, the university's website overloaded with traffic and the campus in lockdown mode, a classmate turned to Facebook to track down the missing man.

“One of the other students saw that he was signed on to Facebook and was able to get in touch with him to find out where he was,” Marchany recalls. “After the shooting, sites like Facebook and MySpace provided a way for people to get in touch with their friends and family outside of the traditional channels.”

Social networking sites proved an invaluable outlet for Virginia Tech's 29,000 students and 6,500 faculty and staff to not only ensure the safety of one another, but also to send condolences, share memories and gain closure in the wake of the nation's deadliest ever peacetime shooting. The true value of Web 2.0 – with its raw power to connect and unite – was on clear display that day in April.

But Marchany, 55, knows that with the good on the internet often comes the evil. He says community-oriented sites that rely on user-generated content – Facebook, Twitter, YouTube and LinkedIn, just to name a few – have replaced emails and shady corners of the internet as the preferred means of phishing users to steal their credentials and other personal information, pummeling them with spam and infecting them with pernicious malware.

“These methods have always been around,” Marchany says. “It's sort of a rinse-lather-repeat cycle. What's different is the delivery mechanism. Most people trust a Facebook or a MySpace because they assume they're going to offer at least some protection for you. But they don't.”

A friend in need

By and large, users have been conditioned to avoid surfing to the pornographic site loaded with spyware, or clicking on the email link or attachment that claims to contain a funny video of the recipient, but actually is a trojan, experts say. But they haven't quite adapted to the next generation of the internet. And the malware writers have taken notice, preying on the implicit trust members place in social networking sites. Businesses, too, must be on guard, especially considering that more than 50 percent of IT professionals queried for a recent FaceTime survey said employees use these sites for more than an hour per day while at work.



“The ways to reach people inside a company have become more prevalent,” says Jonathan Cran (*left*), a security consultant at Rapid7. “The real risk is if you use these sites at work. If employees click on a malicious link and it executes code, it's going to execute inside the company.”

According to Kaspersky Lab, a Moscow-based anti-virus provider, the number of malicious software samples spreading through social networks more than doubled from 2007 to 2008, rising from more than 10,000 to more than 25,000. This year alone, analysts expect to see more than 100,000 malicious files.

Perhaps the most prolific attack occurring specifically within social networking sites is Koobface, a data-stealing worm that first struck MySpace and now mostly propagates on Facebook, according to Kaspersky. The number of variants skyrocketed from 109 at the start of the year to around 930 at the end of June. The malware spreads through messages in which users receive a link to a video claiming to come from a friend. However, if victims follow the link, they are asked to download a fake Adobe Flash update, which installs the worm.

Gary Warner, director of research in computer forensics at the University of Alabama at Birmingham, has analyzed trojans that, instead of being designed to steal banking credentials, have been customized to siphon login details for social networking sites. The malware authors then use these to hijack legitimate accounts to send spam links to friends, resulting in a higher click-through rate than one might achieve through junk mail.

“Compromising these accounts is now a new path to money,” Warner says. “It all goes down to targeting your message for a higher rate of return by creating an assumption that there is a relationship with the advertiser. If it's from your friend, you'll always answer it.”

Meanwhile, the number of phishing attacks targeting social networking sites increased 241 percent from the first quarter of 2008 to the first quarter of this year, according to MarkMonitor, which provides enterprise brand protection.

“On social networking sites, you already have that ring of trust,” says Derek Manky, a threat researcher with security firm Fortinet. “Any message coming from that known person seems legitimate and has a higher rate of effectiveness.”

Neither Facebook nor Twitter representatives returned messages asking to be interviewed for this story. In the past, though, spokespeople for the companies said the sites try to block known malicious links from being shared across their platforms, in addition to resetting the passwords of phishing victims and working with ISPs to get offending domains taken down. But, ultimately, security rests with the user: “We do our best to keep Facebook safe, but we cannot guarantee it,” Facebook states in its Terms of Use.

Experts, though, say these sites could do a better job by initiating measures, such as URL scanning, to deter the spread of malware and designing better code to prevent vulnerabilities.

A change in thinking

Despite the risks on social networking sites, businesses are finding less reason to restrict connections to them. At first, the cries for access came from employees, particularly the younger generation. Now many company

executives are finding that these sites provide effective forums to publicize business offerings and to collaborate with partners and customers. After all, it is not uncommon for an organization to tweet about a new product or set up a Facebook page to keep “fans” updated on its latest news.

“It's not just about selling a product,” says Michael Argast, a security analyst at security firm Sophos. “It's about forming a relationship, and sometimes these relationships are taken into these platforms.”

At Virginia Tech, prohibiting access to social media sites is not an option due to the openness of the university experience.

“It's supposed to be that way,” Marchany says. “But it presents a unique set of challenges from a security standpoint.”

Marchany's office can help protect pupils from cybercrooks lurking on the web. For example, the security office hosts a site that offers comprehensive resources for protecting oneself online. A more personable attempt at reaching students is made during freshman orientation, when the security office addresses online risks, including those that can be found on social networking sites.

Particularly, the students are warned about phishing attacks and third-party widgets that sites like Facebook make available to them. Users must be mindful that when running these applications and games, they are not installing malware or divulging private data that could be used later in a targeted social engineering ploy. And when they arrive for their freshmen year, students at Virginia Tech are given a CD-ROM that they must install before plugging their machines into the network. The disk contains the latest AV and spyware updates and firewall configurations and blocks known malware sites.

Students also are regularly reminded to watch what they post to these sites, as it could come back to bite them when they go hunting for a job after college. “We tell students that these sites are not your personal diary,” Marchany says.

Providing too much information takes on a different meaning in the corporate world, where the spilled beans there might take the shape of intellectual property or other proprietary data, says David Etue, vice president of product management at Fidelis Security Systems.

“The biggest risk we see is the casual conversation about things that shouldn't be disclosed, whether that's sensitive company layoffs, mergers or financial activity,” says Etue, whose company makes a solution to detect these communications.

The potential consequences of a tweet are undeniable. In Guatemala, a man faces five years in prison for posting a 96-character message that urged customers to pull their money from a national bank. In Michigan, the mayor of Battle Creek recently was forced to apologize when he tweeted a link to a city check registry document that, unbeknownst to him, contained Social Security numbers of six municipal workers.

Compliance requirements that specifically address social networking sites could soon be coming, says Kailash Ambwani, CEO of application control solutions provider FaceTime.

Gotham embraces Web 2.0

Dan Srebnick (*right*), associate commissioner of IT security in the New York City Department of Information Technology and Telecommunications (DoITT), says he has long stopped eschewing legitimate sites that could invite productivity declines, data loss and malware.



In fact, Mayor Michael Bloomberg recently unveiled an effort to establish a city Twitter account, where employees can notify residents about such things as parking rules and street cleaning.

Srebnick decided the best way to control social networking across the city's 50 agencies and 25,000 computer users is through education and technology – the DoITT has deployed a FaceTime appliance as a gateway anti-malware solution.

“As a security guy, your gut feeling is you ought to block anything that could possibly be a threat,” Srebnick says. “Of course, that doesn't go over so well with business. City government has a responsibility to be accessible and transparent, and we are going to be making use of the technologies people use in their daily lives in order to facilitate that.”

He says social networking is just another threat vector. The criminal element always will be present in the digital world. One cannot shy away from it.

“You can as much block access to all social networking sites as you can prevent your kids from going to a shopping mall on a Saturday afternoon,” he says. “It's not realistic. You have to find a way to let people do what they're used to doing.”