

Week 1

Hackers want to be your (malicious) friend

Cybercrooks break into Facebook profiles

By Jon Swartz
USA TODAY

SAN FRANCISCO — Facebook isn't just popular with consumers and marketers. Hackers are finding flaws in computer-programming language JavaScript and planting malicious code in the profiles on the popular social-networking site and its rivals.

Once cybercrooks break into a profile, they can steal data and turn the compromised PCs of the victims into remote-controlled machines that spew more malicious software, spam and phishing attacks.

Last week, computer security firm Sophos detailed an attack in which messages posted on the walls of users' Facebook pages urged them to view a video that claimed to be hosted on a Google website. But when the link was clicked, the victim was diverted to a website containing malware.

"It seemed like a regular message from my friend," says Gil Demeter, 23, an analyst at an investment bank in San Francisco who is one of Facebook's more than 80million users.

The malicious code entered his e-mail box and spread the same message to 200 of his Facebook friends. The same message was sent from the e-mail boxes of those 200 people to their friends, and so on, Demeter says.

"If you don't have the proper virus protection, it

could be a problem," says Demeter, who contacted Facebook, which quickly changed his password.

Though Facebook promptly resolved the issue, millions of social-networking users who post and share personal information should take note. Instances of so-called malware on social-networking sites has increased sharply during the past year, based on anecdotal data, says Jeremiah Grossman, chief technology officer of WhiteHat Security.

As millions of people post and share personal information on Facebook, MySpace and other social-networking sites, computer intruders have steadily expanded their attacks from operating systems, such as Microsoft Windows, and software applications, such as Apple's iTunes.

Last week's attack, which spread quickly, could be a harbinger of more to come, experts say.

"Cybercrooks want a foothold on your machine," Grossman says. "Gaining entry to your personal profile is another way."

The changing dynamic of computer intruders has prompted security specialists at Facebook, MySpace and elsewhere to act quickly. Facebook fixed the video-inspired worm as soon as it was alerted. Max Kelly, Facebook's security head, says less than 0.002% of people on Facebook were affected — and all were notified and advised on how to remove the malware.

"If a user sees something that doesn't seem right, report it to us," Kelly says.

Security researchers inform Facebook of about seven potential problems a month. Once alerted, Facebook uses high-tech tools to rid its system of bogus messages and the profiles they come from, Kelly says.

Facebook routinely posts blog items on how to avoid spam and phishing. MySpace, which was the victim of a fast-spreading worm in 2005, employs a phalanx of security technology, warning systems, educational outreach and safety tips to protect its 117million monthly active users, says Hemanshu Nigam, chief security officer.

"What is important is collaboration between tech companies, law enforcement and researchers to address the problem," Nigam says.

That should come as some relief for frazzled corporate network administrators, many of whom say they're concerned about security risks among workers who use social networks, according to a Symantec report to be released later this week.

Still, only about 1 in 4 administrators block social networks. Two out of three acknowledged they have no company policy on social networks, and most are not working on one.

"It's a problem, but the solution is not straightforward," says Kevin Haley, a director at Symantec Security Response.

"Corporations can block people from using their social networks at work, but not at home," Haley says. "They can conceivably download malware at home, and then bring it to the office later."

Discussion

1. Why are cybercrooks breaking into Facebook profiles?
2. What's the difference between spam, malicious software and phishing?
3. In your opinion, what kind of personal information, if any, is it safe to post on a social networking site?
4. What should Facebook users do if they see something suspicious on the site? Have you ever encountered someone or something that concerned you on a social networking site?
5. Do you think MySpace's safety methods are sufficient? Why or why not.
6. After reading the article, has your attitude about the safety of social networking sites changed?
7. What is anecdotal data? Why is it useful? How reliable is it?

Activity

Jeremiah Grossman, chief technology officer of WhiteHat Security, says that, based on anecdotal data, instances of malware on social networking sites have increased in the last year. Talk to at least five teens about the cybersecurity breaches that they have observed. Write down each person's comments. Next, consider the kinds of security problems that you have encountered online. Then, write an informal assessment, based on your anecdotal evidence, that describes the most pressing cybersecurity issues facing people your age.

Lesson objectives:

In this lesson, students will:

- ▶ identify security threats posed by social networking sites.
- ▶ reflect on the safety of giving out personal information online.
- ▶ interview peers about the cybersecurity threats that they have personally observed.

Time requirements:

Step 1: Read the article (10 minutes).

Step 2: Discuss the articles using the questions provided (15 minutes).

Step 3: Use anecdotal evidence to write an informal assessment of the cyber-security threats teens face (Homework).

Total: 25 minutes in class + homework

Notes:

- ▶ **Question 2:** *Spam* is unsolicited “junk” e-mail. *Malicious software* or “malware” is designed to take control of and/or damage an individual’s computer without her or his knowledge. *Phishing* is the attempt to acquire a person’s passwords, account numbers, etc. by posing as a legitimate source (e.g., the individual’s bank) in an electronic communication.
- ▶ **Question 7:** Explain how teachers use anecdotal data to assess students. What kind of anecdotal data do students think Jeremiah Grossman, chief technology officer of WhiteHat Security, used to determine that Malware on social networking sites is increasing?

Links:

- ▶ National Cyber Security Alliance: www.staysafeonline.org
- ▶ United States Computer Emergency Readiness Team: www.us-cert.gov
- ▶ i-SAFE: www.i-safe.org
- ▶ Wired Safety Organization: www.wiredsafety.org
- ▶ Federal Trade Commission: www.onguardonline.gov
- ▶ Multi-State Information Sharing and Analysis Center: www.msisac.org/awareness