YOU'RE ON FACEBOOK? WATCH OUT!

Facebook is the world's largest online social network, and increasingly, the destination of choice for messaging friends, sharing photos and videos, and collecting "eyeballs" for business advertising and market research. But, watch out! It's also a great place for losing your identity or being attacked by malicious software.

How could that be? Facebook has a security team that works hard to counter threats on that site. It uses up-to-date security technology to protect its Web site. But with 500 million users, it can't police everyone and everything. And Facebook makes an extraordinarily tempting target for both mischief-makers and criminals.

Facebook has a huge worldwide user base, an easy-to-use Web site, and a community of users linked to their friends. Its members are more likely to trust messages they receive from friends, even if this communication is not legitimate. Perhaps for these reasons, research from the Kaspersky Labs security firm shows malicious software on social networking sites such as Facebook and MySpace is 10 times more successful at infecting users than e-mail-based attacks. Moreover, IT security firm Sophos reported on February 1, 2010, that Facebook poses the greatest security risk of all the social networking sites.

Here are some examples of what can go wrong:

According to a February 2010 report from Internet security company NetWitness, Facebook served as the primary delivery method for an 18-month-long hacker attack in which Facebook users were tricked into revealing their passwords and downloading a rogue program that steals financial data. A legitimate-looking Facebook e-mail notice asked users to provide information to help the social network update its login system. When the user clicked the "update" button in the e-mail, that person was directed to a bogus Facebook login screen where the user's name was filled in and that person was prompted to provide his or her password. Once the user supplied that information, an "Update Tool," installed the Zeus "Trojan horse" rogue software program designed to steal financial and personal data by surreptitiously tracking users' keystrokes as they enter information into their computers. The hackers, most likely an Eastern European criminal group, stole as many as 68,000 login credentials from 2,400 companies and government agencies for online banking, social networking sites, and e-mail.

The Koobface worm targets Microsoft Windows users of Facebook, Twitter, and other social networking Web sites in order to gather sensitive information from the victims such as credit card numbers. Koobface was first detected in December 2008. It spreads by delivering bogus Facebook messages to people who are "friends" of a Facebook user whose computer has already been infected. Upon receipt, the message directs the recipients to a third-party Web site, where they are prompted to download what is purported to be an update of the Adobe Flash player. If they download and execute the file, Koobface is able to infect their system and use the computer for more malicious work.

For much of May 2010, Facebook members and their

friends were victims of a spam campaign that tries to e-mail unsolicited advertisements and steal Facebook users' login credentials. The attack starts with a message containing a link to a bogus Web page sent by infected users to all of their friends. The message addresses each friend by name and invites that person to click on a link to "the most hilarious video ever." The link transports the user to a rogue Web site mimicking the Facebook login form. When users try to log in, the page redirects back to a Facebook application page that installs illicit adware software, which bombards their computers with all sorts of unwanted ads.

Recovering from these attacks is time-consuming and costly, especially for business firms. A September 2010 study by Panda Security found that one-third of small and medium businesses it surveyed had been hit by malicious software from social networks, and more than a third of these suffered more than $5,000 in losses. Of course, for large businesses, losses from Facebook are much greater.

Sources: Lance Whitney, "Social-Media Malware Hurting Small Businesses," CNET News, September 15, 2010; Raj Dash, "Report: Facebook Served as Primary Distribution Channel for Botnet Army," allfacebook.com, February 18, 2010; Sam Diaz, "Report: Bad Guys Go Social: Facebook Tops Security Risk List," *ZDNet*, February 1, 2010; Lucian Constantin, "Weekend Adware Scam Returns to Facebook," Softpedia, May 29, 2010; Brad Stone, "Viruses that Leave Victims Red in the Facebook," *The New York Times*, December 14, 2009; and Brian Prince, "Social Networks 10 Times as Effective for Hackers, Malware," *eWeek*, May 13, 2009.

The problems created by malicious software on Facebook illustrate some of the reasons why businesses need to pay special attention to information system security. Facebook provides a plethora of benefits to both individuals and businesses. But from a security standpoint, using Facebook is one of the easiest ways to expose a computer system to malicious software—your computer, your friends' computers, and even the computers of Facebook-participating businesses.

The chapter-opening diagram calls attention to important points raised by this case and this chapter. Although Facebook's management has a security policy and security team in place, Facebook has been plagued with many security problems that affect both individuals and businesses. The "social" nature of this site and large number of users make it unusually attractive for criminals and hackers intent on stealing valuable personal and financial information and propagating malicious software. Even though Facebook and its users deploy security technology, they are still vulnerable to new kinds of malicious software attacks and criminal scams. In addition to losses from theft of financial data, the difficulties of eradicating the malicious software or repairing damage caused by identity theft add to operational costs and make both individuals and businesses less effective.