CNN.com.

PRINT THIS

Powered by Clickability

Click to Print

Facebook, Twitter users beware: Crooks are a mouse click away

- Story Highlights
- The FBI reports nearly 3,200 account hijacking cases since 2006
- Online scam losses amounting to $264.6 million reported in 2008
- Facebook has automated systems that detect compromised accounts
- MySpace.com creates blacklists of phony accounts

By Stephanie Chen
CNN

(CNN) -- If you're on Facebook, Twitter or any other social networking site, you could be the next victim.

That's because more cyberthieves are targeting increasingly popular social networking sites that provide a gold mine of personal information, according to the FBI. Since 2006, nearly 3,200 account hijacking cases have been reported to the Internet Crime Complaint Center, a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance.

It starts with a friend updating his or her status or sending you a message with an innocent link or video. Maybe your friend is in distress abroad and needs some help.

All you have to do is click.

When the message or link is opened, social network users are lured to fake Web sites that trick them into divulging personal details and passwords. The process, known as a phishing attack or malware, can infiltrate users' accounts without their consent.

Once the account is compromised, the thieves can infiltrate the list of friends or contacts and repeat the attack on subsequent victims. Social networking sites show there is ample opportunity to find more victims; the average Facebook user has 120 friends on the site.

"Security is a constant arms race," said Simon Axten, an associate for privacy and public policy at Facebook. "Malicious actors are constantly attacking the site, and what you see is actually a very small percentage of what's attempted."

As some social networking sites experience monstrous growth, they are becoming a new -- and extremely lucrative -- frontier for cybercrime. Facebook says it has 300 million users, nearly the size of the U.S. population, and it continues to attract users outside the college student niche. From February 2008 to February 2009, Twitter, a micro-blogging site where users post 140-character messages known as tweets, grew 1,382 percent to more than 7 million users.

"They [cybercriminals] are very adept to using social engineering," said Donald DeBold, director of threat research for CA, an Internet security company. "Your friend is in trouble traveling in another country, 'I lost my wallet. I need help.' They exploit the curiosity aspect out of human nature."

A few decades ago, malicious software and viruses were usually the result of a prank, but Internet security experts say today's attacks are profit-driven. A study from the Indiana University in 2005 discovered that phishing attacks on social networks operated with a 70 percent success rate. These users had fallen for the scam, opened the foreign link and released personal

information.

Cybercriminals are employing phishing and malware attacks for a number of reasons, including trying to redirect users to sites where profit is fueled by the number of visitors. They also try to elicit private information like passwords and bank account numbers to perform scams.

Early this year, Twitter experienced several phishing attacks in which a Web page that looked identical to the widely recognized light blue Twitter page was a hoax. The company warned users to double-check the URL to ensure they were visiting the correct site.

The Internet Crime Complaint Center received more than 72,000 complaints about Internet fraud in 2008 that were referred to law enforcement agencies for further investigation. These cases involved financial losses amounting to $264.6 million, an increase from 2007. Each person lost an average of $931.

"Most of us would want to help a friend in need, but if it's an online friend, and they want you to wire money, you should double-check," FBI spokesman Jason Pack said.

Security experts said it makes sense that cybercriminals are turning to social networking sites. Personal information is abundant on sites like Facebook and MySpace. Each time users give out valuable information like birth dates or addresses, they could be providing hints about their password, security experts say.

The American Civil Liberties Union has expressed concern about the information visible through Facebook quizzes and applications.

"They'll have access to all that information, so they can sell it, they can share it, they can do an awful lot with it," Chris Calabrese, legislative counsel for privacy-related issues with the ACLU, told CNN.com in September.

Many Internet security experts consider the first virus attack on the PC to have occurred in 1986. By the early 1990s, viruses transmitted on floppy disks became ubiquitous. When the World Wide Web became widely available that same decade, viruses, worms and malware became problems in e-mail accounts, frustrating users who clicked on messages thought to be legitimate.

In the new millennium, the most common form of malware attack has become known as drive-by downloads. While surfing on Google or Yahoo, spyware or a computer virus is automatically and invisibly downloaded on a computer, requiring no user interaction for the computer to be infected.

"We are on the verge from shifting from the Web being the No. 1 victim of infecting to social network," said Mikko H. Hypponen, chief of research technology at F-Secure Corp. His company sells anti-virus software and malware protection programs. "It's going to get a lot worse before it gets better."

Social networks are fighting the aggressive attacks from cybercriminals. Most sites have information pages dedicated to educating users about the risks of Internet scams. Users can become a fan of "Facebook Security" and receive updates on how to protect their accounts. One of the most common pieces of advice given by security experts is to change passwords frequently.

Facebook has also developed complex automated systems that detect compromised accounts. They spot and freeze accounts that are sending an unusually high number of messages to their friends. Company security officials said Facebook is a closed system, which can be helpful in erasing phony messages from all accounts.
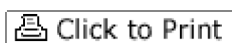
At News Corporation's MySpace.com, the company creates blacklists of phony accounts to prevent people from clicking on a faulty link. Hemanshu Nigam, first chief security officer for MySpace, said the firm warns about suspicious links and educates users about the harm phishing and malware attacks can bring.

"We are prepared for them," he said.

All About**Facebook Inc.** • **Twitter Inc.** • **MySpace Inc.** • **Computer Crime**

Find this article at:
http://www.cnn.com/2009/CRIME/10/19/social.networking.crimes/index.html

Click to Print

☐ Check the box to include the list of links referenced in the article.

SAVE THIS | EMAIL THIS | Close