Spammers target Facebook

April 4 2011, By Pete Carey

Interested in a free iPad like the one your Facebook friend got by filling out a survey?

Curious about that "friend" request from someone you don't know?

Want to see that video a friend recommended on your Facebook news feed that shows a whale hitting a building in Japan's tsunami?

Don't bite - or click. They're spam, or worse.

Such attacks have long been common with email. Now social media are the new targets, and Facebook - with 500 million users - is the biggest target of them all.

"It's a spammer's dream," said Kurt Roemer, chief security strategist for Citrix Systems. "You have all your friends, business connections, who you do banking with, who you travel with - all kinds of aspects of your life. Facebook has a great reputation, but this one thing's dragging them down."

Facebook says fighting spam is "a top priority" and has a large team of investigators working on it. The company has sued spammers successfully, winning $2 billion in judgments, and has added new security features, along with advice for users on how to protect against spam.

"It's an arms race," said Pedram Keyani, leader of a Facebook Site

Integrity team. "We are constantly adapting our strategy to handle changes in their tactics."

The spammers make money by driving people to sites that pay them for clicks. "Ninety-nine percent of this is financially driven," Keyani said.

The assaults on Facebook users have a common denominator, said Kevin Haley of Symantec, a major Internet security company. "It really begins with tricking a user into helping. The relationships are what they're counting on to help spread things. If I can get you, then I can get all your friends, and then I can get all their friends."

Phishing uses fake messages to direct users to sites for knockoff products, or to pages that can capture your computer and turn it into a automaton that floods your friends with spam. Users can also be tricked into downloading malware onto their computer. The malware is activated when a user innocently clicks on a button on a scam Web page. Then it sends friends of the user messages, directing them to a website that infects their computer.

A technique called "likejacking" tricks users into "liking" a page when they visit it. The "Like" button on Facebook lets a user share content with friends. When users click the button, the content shows up on their home page and can show up on friends' news feeds.

"Fill out the survey to win the iPad, and you end up subscribing to the joke of the day for $5 a joke, charged to your cell phone," said Chester Wisniewski of Sophos.com, an online security company.

If you click on the alleged video of the whale hitting the building, you instantly spam all your friends, said Jeremy Gin, chief executive officer of SiteJabber.com, a San Francisco online consumer protection site.

One Internet worm hijacks your Facebook account, sends messages to your friends and harvests their accounts and passwords.

Carol Hoover, executive director of the Eyak Preservation Council in Alaska, may have been a victim.

"Somehow they became a friend of mine, stole my profile, my picture, emailed a lot of my friends in waves," she said. The fake Carol Hoover would chat with her friends, saying things like - 'Did you win your $50,000 dollars yet?' 'Have you heard from the Obama administration?' Their English is bad, they drop words," Hoover said.

She complained, and the imposter was removed. "There's an aspect of it that's frightening," she said. "But I really enjoy Facebook. It's a huge social networking tool."

While the amount of spam has grown, Facebook's Keyani said the number of actual attacks in which a Facebook account or computer is taken over by spammers is less than one percent of the social network's 500 million users. That's still a lot of users - 1 percent would be five million of them.

Keyani said he's "really proud" of the fact that there is far less spam and danger of malicious attack on Facebook than on Internet email. "Our response time to a threat is very fast, within minutes," he said.

Facebook has developed a couple of spam and malware detection systems to protect users. One, called "linkshim," evaluates websites associated with spam attacks. A user who is about to click on one is directed to a warning page. Another, called "roadblock," looks for unusual activity from users, like massive email blasts. If a malware infection is detected, McAfee security software cleans up their account and logs them back on.

Julien Sobrier, senior security researcher for Zscaler, a Web 2.0 security provider, said he would like to see more protection against unapproved widgets that can be downloaded from the Internet and used with Facebook. Facebook might limit the number of people who can click on one until it is proven to be a trusted item, similar to what Facebook does with approved applications, he said.

But the best anti-spam tool is user awareness.

"First review privacy settings," said Roemer of Citrix. "If you let anybody find you, anybody's going to find you. When it gets into friends of friends, anything can happen."

Beyond that, be careful what you download, and check out Facebook's security pages.

"Education on what you should and shouldn't install on your machine solves 99 percent of this," Keyani said.

FACEBOOK SECURITY TIPS

Review your security settings and consider enabling login notifications. They're in the drop-down box under Account on the upper right hand corner of your Facebook home page.

Don't click on strange links, even if they're from friends, and notify the person if you see something suspicious.

If you come across a scam, report it so that it can be taken down.

Don't download any applications you aren't certain about.

For using Facebook from places like hotels and airports, send the text

message "otp" to 32665 for a one-time password to your account.

Visit Facebook's security page, www.facebook.com/security, read the items "Take Action" and "Threats."