Security
April 30, 2009 9:55 AM PDT

Facebook hit by phishing attacks for a second day

by Elinor Mills

Facebook stopped a phishing attack on Thursday, its second day in a row of dealing with a worm on the site that lures people to a fake Facebook page and prompts them to log in.

Unsuspecting Facebook users get a message from a friend urging them to "check this out" and including a link to a Web page that appears to be a Facebook log-in page, but it is a fake site that steals their information when they type in their username and password. The worm also sends a copy of the message to the infected Facebook member's contacts.

In the latest attack, the Web address was "FBStarter.com." In Wednesday's attack, the address was "FBAction.net."

The attacks were stopped within a few hours in each case, said Facebook spokesman Barry Schnitt. He said it was too early to say whether the two phishing attacks are related. "We are investigating," Schnitt said.

Once Facebook learns of a phishing attack, either by members notifying the company or employees noticing that a URL is being distributed to a lot of people, the company deletes the URL from members' pages, blocks fresh postings, and removes the redirect to the URL that appears in e-mail messages, Schnitt said.

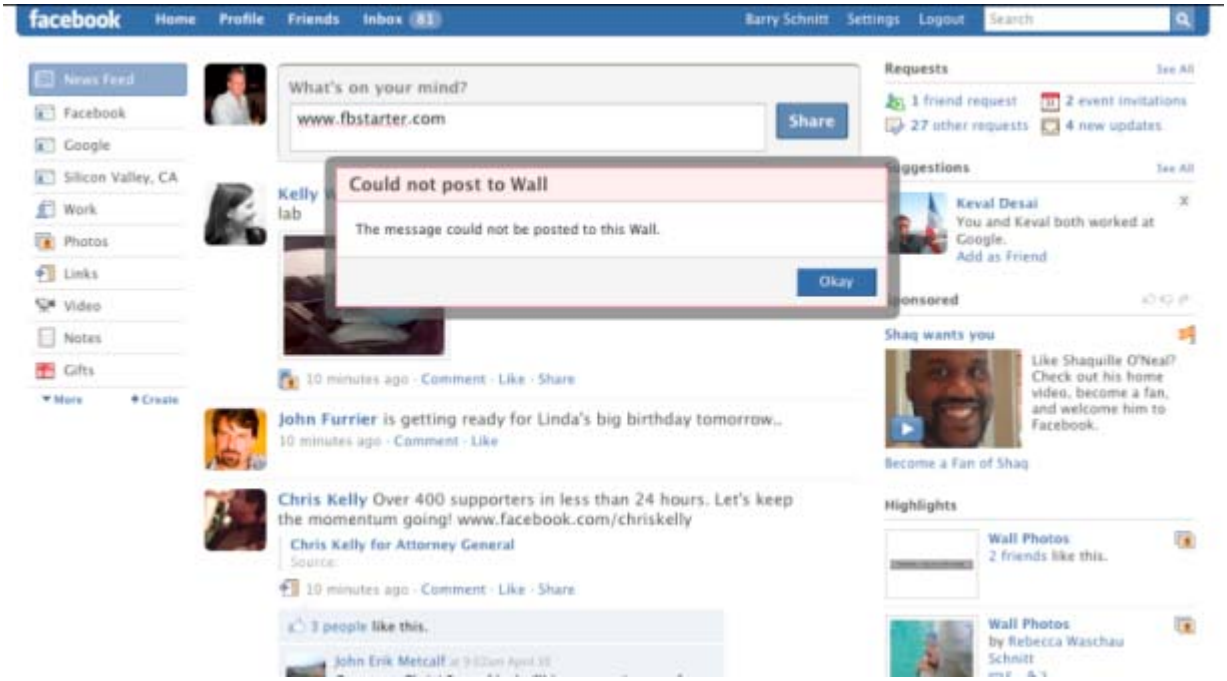
Facebook also goes in and resets the passwords of member accounts that had been used to distribute the spam, he said.

The company also alerts anti-fraud partner MarkMonitor, which passes the phishing URL on to the major browsers to block it and contacts ISPs to take the site down, according to Schnitt.

To protect against phishing scams, Facebook users should make sure that the URL they are visiting says "www.facebook.com." If it doesn't use that domain it's likely to be spam. Also, members that are already logged in to Facebook will not be asked to log in again.

"People should have a healthy dose of suspicion, and ask themselves 'why did I get logged out?'" Schnitt said. "If something looks a little strange you should check the address bar."

Facebook users who think they have been affected by the scam should change their passwords and review their Facebook stream for any unauthorized changes. If they use their Facebook password for other sites, they should change those passwords as well. And if they are using their Facebook authentication to log in to any other sites, they should check for any unauthorized changes on those sites. Information on safe password creation and use **is here**.



Facebook prevents accounts from re-distributing phishing URLs once a spam attack has been noticed.

(Credit: Facebook)

Elinor Mills covers Internet security and privacy. She joined CNET News in 2005 after working as a foreign correspondent for Reuters in Portugal and writing for The Industry Standard, the IDG News Service, and the Associated Press. E-mail Elinor.

Topics: **News**, **Privacy & data protection**, **Vulnerabilities & attacks**

Tags: **Facebook**, **phishing attack**, **spam**

Related

From CNET

Phished Facebook accounts pass along malware

Facebooking while out sick gets employee fired

Report: Facebook to open up to developers

From around the web

Facebook hit by phishing attacks for a s... CNN - Tech

Facebook Targeted in Spam Scam eWeek

More related posts powered by Sphere