Facebook fights 'phishing' scam

May 1 2009, by Glenn Chapman

The logo of social networking website 'Facebook' is displayed on a computer screen. Facebook Thursday said it has blocked a link at the heart of a "phishing" scam being used to dupe members into revealing passwords to accounts at the social networking website.

Facebook Thursday said it has blocked a link at the heart of a "phishing" scam being used to dupe members into revealing passwords to accounts at the social networking website.

Facebook also announced it is expanding an alliance with Internet security firm MarkMonitor to better protect users from hackers and online subterfuge.

"The meteoric success of Facebook makes it a natural target for malware attacks that seek to capitalize on their trusted and recognizable brand," said MarkMonitor chief marketing officer Frederick Felman.

"Our experience ... allows us to expertly address Facebook's concerns about malware and phishing, and to help protect their platform and their users from ongoing attacks."

Cyber criminals were sending Facebook users messages with links to a realistic-looking replica of a log-in page at the social-networking service.

The bogus page then captured password information so hackers could access people's Facebook profiles and impersonate users of legitimate accounts to lure other members of the social-networking community into the trap.

"We've already blocked www.fbstarter.com from being shared on Facebook, which stops this from spreading," a spokeswoman for the California-based firm told AFP.

"We also blocked access to the URL so if someone does find it on Facebook (on their wall, in their inbox, or in an email notification) it won't send them to the destination."

She added Facebook is deleting the booby-trapped link from "walls" and inboxes at the website and resetting passwords of users whose accounts were used in the phishing scam.

"Thus, the data becomes useless to the bad guys very quickly because the passwords they've stolen have been changed," Facebook said.

MarkMonitor maintains "browser blacklists" of scam Internet links and works to get treacherous websites taken down, according to Facebook.

"MarkMonitor demonstrated that it understood the complexity of the phishing issue we were facing so it was a natural next step for us to bolster our own security systems with their anti-malware solution," said

Facebook threat analyst Ryan McGeehan.

Online social networking services are prime targets for hackers because they provide trusted gateways into users' networks of friends, according to computer security specialists.

"I love Facebook and MySpace; social networks are a wonderful use of the computer," said David Perry, global director of education for computer security firm Trend Micro. "But, it is really being abused."

Hackers can use breached social networking accounts for "nefarious purposes" such as infecting computers with malware, malicious software, that steals valuable data or commandeers control of machines, according to MarkMonitor.

Facebook advises users to shun messages, posts or links asking for log-in information and to always make certain they are visiting the social networking website's legitimate address of facebook.com.