

Twitter users pounded anew by hackers

Posted By [Computerworld Philippines](#) On March 3, 2010 @ 4:28 pm In [Mobile & Wireless](#), [Research](#), [Security](#), [Today's News](#) | [No Comments](#)

By Computerworld Philippines Staff
March 3, 2010

Hackers launched a one-two punch combination to Twitter users recently, recruiting hijacked accounts to launch cybercrime campaigns.

Only two days after launching the "LOL" phishing attack, hackers struck again by launching the "This you?????" phishing attack, both designed to steal login details and hijack accounts, reported Sophos, an IT security and data protection firm.

Sophos said messages asking "This you?????", followed by a link to a bogus Twitter login page, have caused such a scare on the micro-blogging network that the phrase is currently a hot trending topic on the site.

The attack, which is the latest in a storm of phishing attacks that have occurred on Twitter since the weekend, is designed to steal passwords and could use hijacked accounts to spread money-making spam campaigns, steal identities, and distribute malware, Sophos added.

Graham Cluley, senior technology consultant at Sophos, explained the "This you?????" messages are accompanied by clickable links which take unsuspecting users to a fake Twitter login page. Users who are tricked into believing they might see a picture or information about themselves, may enter their username and password without thinking about the possible consequences.

"Twitter users have been battered with phishing attacks in the last few days, all taking advantage of people's curiosity," Cluley said. "But if you click on the link and enter your details you could be taking your online identity and handing it over on a plate to hackers. They can then take your username, email address and password and not only use it to spread more attacks via Twitter – they can also try your credentials at many other websites – potentially opening your other online accounts to abuse. Anyone hit by this kind of attacks must change their passwords immediately."

Cluley reported crime on social networks is on the rise.

"We saw a 43% rise in the number of people reporting being phished via such sites in the last 12 months, and the way things are looking that figure can only go up," he said. "As the social networks grow in size and power there will be more and more hackers attracted to commit crimes through them."

Sophos recently made a YouTube video, which journalists and bloggers are free to embed on their own websites, demonstrating the attack: <http://www.youtube.com/watch?v=yFVqfqzV6M> ^[1]

During the Twitter "LOL" phishing attack, thousands of accounts were compromised by hackers creating Web 2.0 botnet. Twitter users found that fellow members of the micro-blogging network had posted messages disguised as humorous inks, but actually aimed to phish passwords credentials from unsuspecting users.

Messages, which began with phrases such as "Lol. this is me??", "lol , this is funny.", "Lol. this you??" and "ha ha, u look funny on here", were accompanied with clickable links which redirected users to a fake Twitter login page hosted on a website based in China.

Sophos researchers claimed to have discovered that although the main wave of poisoned messages has been via private direct messages between individual users on Twitter, dangerous links are also being posted in public feeds. This means that innocent users can stumble across the links even if they are not sent it directly, or even if they are not a signed-up user of Twitter.

"It appears what is happening is that the messages are being shared more widely because of third-party services like GroupTweet which extend the standard Twitter direct message (DM) functionality and allow private messages to be sent to multiple users and optionally made public," Cluley said. "This has resulted in the bizarre site of Twitter accounts warning their followers about the phishing attack, only to subsequently fall victim to it themselves."

Sophos also identified that the phishing campaign appears to be already bearing fruit for the hackers as they are now distributing spam selling herbal viagra from the compromised accounts.

"Unless the hacked Twitter users change their passwords, the intruders can continue to spread spam and other attacks from their hijacked accounts," Cluley warned. "Cyber-attacks via social networks are becoming more and more common. Last month Sophos published its Security Threat Report which revealed that there has been an astonishing 70% rise in the number of users reporting spam and malware attacks via social networking sites." — **Tom S. Noda**