6/22/12

By: Guest Author, John Breyault, National Consumers League

Many consumers find the popular social media site, Twitter, useful for staying in touch with friends and family and getting updates from organizations or famous people. Unfortunately, scammers see the millions of Twitter users very differently: as potential targets.

Scams on Twitter usually involve some kind of link or promise from either a user you don't know or a user whose account has been compromised.

A common scheme is for a scammer to create an account then follow or direct message hundreds or thousands of other users. Each time a user is followed, they receive an alert with a link to the scammer's profile. The profile often contains links to malware or phishing sites. A recently popular method of this is a direct message or tweet with a message like "lol is this really you?" with a link attached.

Yet another scheme scammers use is to post something that leads to a link that looks like a Twitter login page, but isn't, and thus when a user types in his username and password, the fraudster has access to their account and can use it to target others.

Other signs of a fraudulent account are: repeatedly posting duplicate updates, abusing basic functions of Twitter to get attention, and posting links with unrelated tweets.

How can Twitter users avoid falling for a scam?

Twitter users should ignore any direct messages or tweets that promise that by simply clicking on a link they will receive thousands of followers. Any "get followers quick" method promised by someone else is a way to steal money or private information.

Twitter is aware of scammers using its site, and shuts down the accounts of spammers users report, so users shouldn't hesitate to report a suspicious Twitter handle that displays any of the

red flags. Other tips for using Twitter and avoiding the pitfalls of a scam are:

- Use a strong password
- Always make sure you're on Twitter.com before giving login information
- Use HTTPs for security
- Beware of direct messages from people you don't know, especially if they promise to help you "immediately" get thousands of followers
- Be suspicious is you are followed by someone posing as a celebrity. Well-known Twitter users often have Verified Accounts (signified by a check mark next to their profile name)
- If you don't know someone following you, don't click on links in their profile.
- If you encounter abusive and/or annoying behavior on Twitter, block and ignore the profile responsible and report it to Twitter.

There are many organizations with Twitter accounts that work to protect people from online fraud and other consumer issues such as the Better Business Bureau (@BBB_US) and the Federal Trade Commission (@FTCgov), Visa Security Sense (@visasecurity), StopBadware.org (@StopBadware), StopThinkConnect.org (@StopThinkConnect) and the National Cyber Security Alliance (@StaySafeOnline).

Twitter's Help Center (@Support) also provides useful information on identifying spammers and protecting your account.

Stay safe and have fun in the Twittersphere!