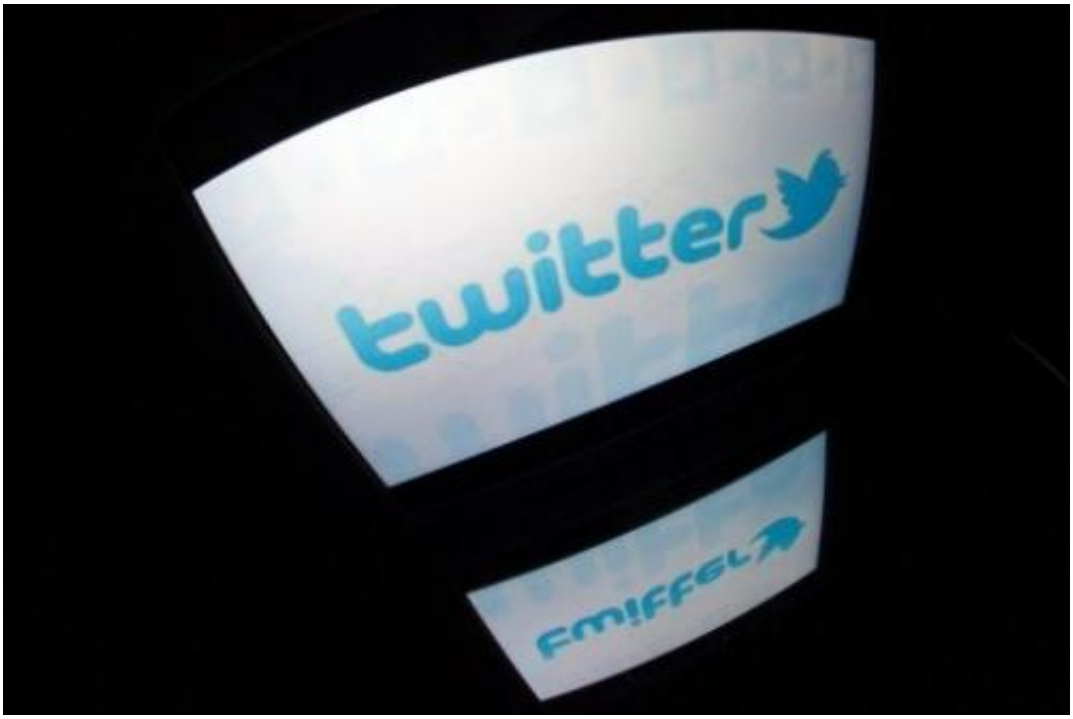
Twitter security in crosshairs after AP account hijack

April 25 2013, by Glenn Chapman



A hijacked Associated Press Twitter account that rattled markets with false word of an attack on the White House has put the security of social media in the crosshairs.

A hijacked Associated Press Twitter account that rattled markets with false word of an attack on the White House put the security of social media in the crosshairs.

The stock market rebounded from the nosedive triggered Tuesday by the

bogus tweet and the AP posted a message on Twitter that its account "which was suspended after being hacked, has been secured and is back up."

The AP Twitter page indicated more than 1.8 million followers as of early evening in San Francisco, where the one-to-many messaging service has its headquarters.

What remained were questions as to whether security was tight enough on Twitter and other popular social networks in an age when people increasingly turn to posts from friends or strangers for reliable news and information.

Twitter was firm that evaluating and improving defenses at the service remains an ongoing priority and that the hijacking of the AP account didn't prompt any immediate moves to toughen security.

AP's Twitter account appeared to have been breached after hackers tricked someone into revealing a password with a deceptive email message in what is referred to as a "phishing" attack.

Some online reports contended that Twitter was considering "two-factor authentication" that would require users to either know something or do something aside from just type in passwords to access accounts.

"When you look at the problem in mass, the most critical thing we see is people just have horrendous passwords and use them all over the web," said Mark Risher, chief and founder of Impermium, an Internet security firm.

While incorporating a second step such as sending a confirmation code in a message to an email account or mobile phone associated with a user's account is a big improvement, even that defense is flawed, he said.

Risher was 'spam czar' at Yahoo! Mail before leaving the Internet pioneer and launching Impermium in 2010. His team includes Sameer Bhalotra, a former senior director of cybersecurity for the White House.

Tourists are pictured outside the White House in Washington DC on April 24, 2013. A hijacked AP Twitter account that rattled markets with false word of an attack on the White House has put the security of social media in the crosshairs.

Phishing attacks are becoming increasingly sophisticated and convincing, sometimes with information harvested from social networks used to make pitches more personal and believable to specific targets, according to Risher.

A person conned into giving hackers a password could just as easily be asked for a second bit of information needed to get into an account, he reasoned.

"You really can't just expect users to never get duped, because they always will," Risher said. "Service providers should never be satisfied with a password."

Adding multiple layers of security to get into accounts treads on the ease of using online services, forcing social networks to risk aggravating members.

"There is a trade-off between convenience and safety," he said. "It is like putting five deadlock bolts on the door. It would make you more secure but it really would be a hassle if you wanted to pop out to the corner store."

Impermium and other companies specialize in ways to spot "bad guys" who use stolen passwords to get into accounts.

Signs watched for include whether an account is being accessed from a smartphone other than one typically used or if the visitor appeared to be trying to cover their tracks.

Last month, Twitter arranged with major web email service providers Google, Yahoo! and AOL to reject emails claiming to be from Twitter if they didn't have a special protocol that acts as a "handshake" of authenticity.

The intent was to block phishing email messages from even reaching targets. Twitter maintained that it has a variety of ideas about hardening security but would not disclose details.

"The answer is the service providers," Risher said. "Just like in the real world where a bank doesn't say that once you make it past the door you can do whatever you want."

(c) 2013 AFP