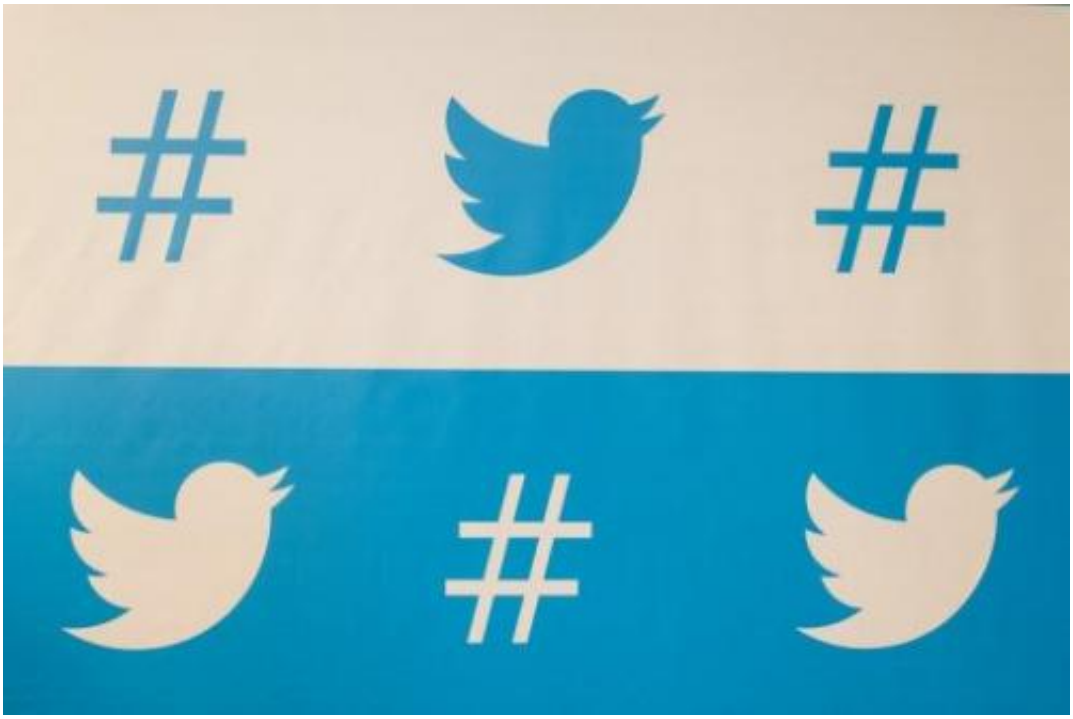
Twitter tightens security after high-profile breaches (Update)

May 22 2013



Twitter said Wednesday it was stepping up its security measures for the popular messaging service following a series of high-profile breaches by hackers hitting media organizations and others.

Twitter said Wednesday it was stepping up security measures for the popular messaging service following a series of high-profile breaches by hackers hitting media organizations and others.

Twitter said it would implement a new login verification system, "a form

of two-factor authentication" which is "a second check to make sure it's really you" when a user signs in.

"Of course, even with this new security option turned on, it's still important for you to use a strong password and follow the rest of our advice for keeping your account secure," said Jim O'Leary of Twitter Product Security.

Some recent attacks took over Twitter feeds and delivered fake tweets using the accounts of Agence France-Presse, the Associated Press, Financial Times and other news organizations.

Last month, hackers spooked markets after breaking into the AP Twitter account and falsely reporting President Barack Obama had been injured after two blasts at the White House.

Twitter said the new system would be an option for users, and would allow them to require a verification code for each sign-in.

"You'll need a confirmed email address and a verified phone number. After a quick test to confirm that your phone can receive messages from Twitter, you're ready to go," O'Leary said.

The security system will send a text message to the user's mobile phone with a verification code that would be entered for the login.

While Twitter has seen phenomenal growth as a social media outlet, its security has been questioned. Twitter said in February it was hit by a "sophisticated" cyber attack and that the passwords of about 250,000 users were stolen.

Johnannes Ullrich, a security specialist with the SANS Technology Institute, said two factor authentication "is the right step forward" but

may not thwart the kind of attacks seen on Twitter feeds.

"With compromised media accounts, another issue is password sharing, which may hinder adoption of two factor authentication in environments that need it most until respective social media suites that are used by larger companies are updated to support Twitter's two-factor authentication scheme," Ullrich said.

James Gabberty, professor of information systems at Pace University, said the new verification system appeared positive but "it depends on how they deploy it."

He said the decision to use a separate communications channel such as a mobile phone is "generally very safe" but that it is preferable if the phone and Internet services are different carriers with "a different architecture."

"If it is a different company, then this is extremely safe and gives a very high level of assurance that the integrity of the message is not compromised."

But Gabberty said Twitter still has other security problems which need to be addressed, such as requiring strong passwords and frequent changes in passwords.

"I stay away from Twitter because it's such an insecure system. It's begging to be hacked," he said.

The Syrian Electronic Army, which appears to be aligned with the government of President Bashar al-Assad, has claimed credit for hacking AFP, AP and other news organizations.

Earlier this month, the Twitter feed of satirical US news website The

Onion was also taken over by the Syrian group aiming to inject its own sardonic spin on the deadly conflict.

The Onion posted details of how its feed was hijacked, describing how emails were sent to some employees in a phishing spoof to gain access to passwords.