Facebook rolling out new security features

BARBARA ORTUTAY - AP Technology Writer - Associated Press

Facebook's millions of users are a lucrative target for Internet criminals looking to steal passwords and more. To combat malicious attacks, phishing scams and spam, the online social network is rolling out new security features.

You can ask to be notified by e-mail or text message when your account is accessed from a computer or mobile device you haven't used before. The log-in attempt may be legitimate when you're traveling, but if you haven't left home in a week, you probably ought to change your password.

Facebook is also adding roadblocks when it notices unusual activity, such as simultaneous log-ins from opposite sides of the planet. For example, you might be shown a photo with your friends tagged, and be asked to correctly identify who they are before the second log-in goes through.

Users will also be able to check where the latest log-ins have come from. This is similar to a feature Google Inc. offers on its Gmail service, where users can view the date, time and location of the most recent log-ins to their account. Gmail also states whether the account is open on another computer at the same time.

Some of these changes are already available, while others are still being tested and will launch over the next few weeks. Facebook typically rolls out changes over several days, if not weeks, so not all users will see them at the same time.

The new features come as Facebook faces growing criticism over the way it handles users' privacy. It has been pushing them to share more about themselves with one another and with the outside world. The security upgrade is a sign the company is working to keep its users' trust in the way it handles the private data they post, even as it fends of complaints from privacy advocates, users and politicians.

Hemanshu Nigam, former chief security officer at Facebook rival MySpace, said Facebook has many incentives to be mindful of privacy complaints.

"A little thing like this can turn into a big thing, and could turn into an advertiser saying, 'Well, I can take my dollars elsewhere,'" said Nigam, who now runs online security firm SSP Blue but still consults for MySpace. "The moment a lawsuit or government investigation begins, advertisers get very nervous of that."

Facebook already has automated systems in place that detect when users access the site in a way that "doesn't make sense," said Jake Brill, product manager at Facebook. This can include sending out an avalanche of messages or logging in from different countries at the same time.

The secondary account verification system that Facebook is rolling out makes sure

that when people log in from elsewhere, they are authorized to do so. Many websites try to do this by asking people to type words displayed in an image to prove they are human, rather than a computer seeking automated access. But this only helps keep those software robots out, not people, Brill said.

The requirement to enter information that only you would know — such as the identity of your friends — can help stop unauthorized access should your password somehow become compromised.

To get notified when someone accesses an account from a new computer or device, you have to turn that feature on. To do this, go to "account settings," scroll down to "account security," then click "change." There, you can choose to be notified of log-ins by e-mail or text message.

Facebook is asking users to activate, or "opt-in" to, the security setting, even as it takes an "opt-out" approach with some of its marketing and personalization features. With opt-out, participation is automatic unless the user takes action.

Without giving an exact figure, Facebook says only a tiny percentage of its users have their accounts compromised. But a small percentage of 400 million can still be sizable.

The site's users are a good target for cybercriminals because of the implicit trust people place in Facebook. They are more likely to respond to scams and other messages that appear to come from real friends, but are actually sent by hackers able to game the system.