How to protect yourself: 2 million Facebook, Google accounts compromised

By Sasha Bogursky Published December 05, 2013 FoxNews.com

http://www.foxnews.com/tech/2013/12/05/passwords-guidelines-for-protecting-internet/?intcmp=obnetwork

More than 2 million Facebook, Google and other accounts have been compromised, security experts warn, compromising countless accounts and leaving Internet and financial companies scrambling.

Some online networks responded by disabling the affected passwords, or requiring affected accounts to choose new passwords. But there are several things you can do to minimize further threats, even if your account isn't among the millions that were compromised.

"The most important thing is to have a different password for every site that you are registered to," former chief security officer for MySpace.com Hemu Nigam told FoxNews.com.

Nigam, who founded the online security company SSP Blue, said that most people tend to use the same password for every site they visit. This leaves a person vulnerable to attacks, Nigam warned: Once a hacker accesses one of your accounts, they can access all of them.

"In the real world, we have a different key for your house, bank, gym locker and car so that if a thief breaks into one of those, they can't break into everything. The same should be true for the online world," he said.

People who hack into social network sites are not interested in exposing users' embarrassing photos; hackers are after information they can use to access bank accounts.

"Most of the time when people [hack into accounts], the goal is to do fishing on other account information," Nigam said. "There is very little interest in looking at your pictures. It's about at looking at your account as a jumping point to get to your friends' accounts."

Many of the companies involved, including Facebook and LinkedIn, rushed to address the breach.

"LinkedIn proactively seeks out credentials dumped on the Internet by hackers as well as credentials gathered by malware; we then compare the credentials to those of our members and any matches result in immediate invalidation of those passwords. We’ve already been working with Spiderlabs to reset the passwords of the accounts whose LinkedIn credentials were on the list," the company said in a statement.

“Facebook takes people’s information security extremely seriously and we work hard to protect it. It appears that people’s computers may have been attacked by hackers using malware to scrape information directly from their web browsers. As a precaution, we've initiated a password reset for people whose passwords were exposed," the social network said.

Nigam said he suggests everyone change their passwords -- hackers may remain idle for months before beginning their mayhem.

"The other thing that everyone needs to worry about is sometimes hackers will obtain compromised account and then not do anything with them until 3 to 4 months later. So it's something to keep our guard up," he warned.

Although there is no full proof way to prevent unwanted visitors from accessing your account, having up-to-date security systems can help.

"Unfortunately, there's no way to completely protect yourself against breaches that happen in this way," senior vice president of Equifax Personal Solutions Scott Mitic said in a press release. "Having anti-virus and anti-spyware on your computer can be helpful, but they're far from 100 percent effective."

Financial services firm ADP said that, while the company and its customers were not specifically targeted, some customer passwords were affected.

"ADP has determined that none of its internal networks and servers has been compromised, and no intrusion has occurred," it said in a statement. "ADP is requiring a password reset for the approximately 2,400 clients whose credentials were impacted."

In 2012, $4.9 billion was stolen from consumer banking accounts through malware takeovers according to a 2013 report by Javelin Strategy & Research.

While keeping multiple and complicated passwords will help to protect consumers, it is important to monitor your bank accounts in case you have been hacked.

"With the proliferation of attacks like these, it's more important than ever for consumers to take steps to help protect their identity and monitor their credit," Mitic said. "If you become a victim of identity theft due to a data breach or malware attack, it could be costly and time-consuming to clean up your credit."

Following these recommendations, "if your Facebook account is compromised that should not result in bank account being compromised," Nigam said.