Tech Hub, Hackers escalate attacks on social networks (6.7.12)

Security breaches at LinkedIn and eHarmony have highlighted an escalation in attacks on social networks from hackers seeking to exploit personal data, according to security firms.

The professional networking and dating sites have both confirmed that some of their users' passwords have been stolen, after hackers posted a total of 8m encrypted passwords online, 6.5m of them from LinkedIn, the company said.

LastFM, a UK-based social music site owned by CBS, on Thursday said it was investigating a potential leak of its users' passwords. Like LinkedIn and eHarmony, it advised users to change passwords.

Experts said the LinkedIn hack was one of the largest yet seen and a sign that cybercriminals are showing an increasing preference for targeting social networks over email.

High quality global journalism requires investment. Please share this article with others using the link below, do not cut & paste the article. See our Ts&Cs and Copyright Policy for more detail. Email ftsales.support@ft.com to buy additional rights. http://www.ft.com/cms/s/0/2c348bba-b0c5-11e1-a2a6-00144feabdc0.html#ixzz1xmnSGZ9y

“Now they’ve switched over to social networks, like Pinterest, Twitter, and Facebook,” said Graham Cluley, senior technology consultant at Sophos, a security research firm. “The anti-spam features on these sites are nowhere near as mature as places like Hotmail and Gmail.”

In April, social networks replaced financial organisations as the top target of phishing attacks, according to data from Kaspersky Lab. Phishing scams usually take the form of a fake email that tries to trick people into giving personal information to cybercriminals.

Kaspersky said social networks accounted for 28.8 per cent of these attacks in April, a 6 per cent increase from March, due mainly to a surge of attacks aimed at Facebook users.

How the hackers accessed the sites in this week’s breaches is unknown. LinkedIn has since added an extra layer of security to its password encryption, a practice Mr Cluley said they “should have been doing earlier”.

Various features of social networks already make them more vulnerable to hackers, Mr Cluley said, such as the openness of social networks to external programmers who develop applications. Also, the personal nature of the networks makes it easier for criminals to impersonate someone, using their name and photo to contact their friends and work colleagues.

“If I get a message from someone who is a LinkedIn contact of mine, I’m much more likely to respond,” said David Emm, senior security researcher at Kaspersky Lab. “They’re using it as a layer of trust to spread their malware.”

Cybercrime on social networks is turning into its own industry, said Jim Walter, manager for McAfee Threat Intelligence Service, as criminals hire underlings to generate more traffic and even ad revenue from these sites through automated botnets, or collections of compromised computers.

“There’s a whole underground economy around LinkedIn bots, Pinterest bots, Facebook bots, you name it,” he said.