BBC NEWS

Cyber thieves target social sites

By Mark Ward
Technology Correspondent, BBC News website

It is not just the average net user who is a fan of social network sites, so are hi-tech criminals.

So say security professionals predicting what net criminals will turn to in 2008 to catch people out.

The quasi-intimate nature of the sites makes people share information readily leaving them open to all kinds of other attacks, warn security firms.

Detailed information gathered via the sites will also help tune spam runs or make phishing e-mail more convincing.

Friendly faces

There was no doubt that 2007 was the year that sites such as MySpace, Facebook, Bebo, Orkut rose to prominence as millions of people signed up to use them and started posting information about themselves and what they were up to.

But in 2008 these sites will become an attack vector for the hi-tech gangs who are now behind the vast majority of cyber crime.

Mary Landesman, senior security researcher at ScanSafe, said social sites would prove popular for two reasons.

"The technologies that play there and the third party add-ons make it an environment that is susceptible to compromise," said Ms Landesman.

Already at the end of 2007 Brazilian users of Google's Orkut were subject to an attack by a worm that tried to steal bank account details. The malicious program, which also tried to hijack compromised computers, propagated via booby-trapped links placed on the personal page of Orkut users.

Still other attacks have tried to capitalise on the popularity of video clips seen on sites such as YouTube by putting booby-trapped links on pages that show the short

films.

Alongside technical vulnerabilities in the networks go other problems with the amount of information that people share on social networking sites.

This data can give criminals knowledge about the names of employees at a company, insight in its managerial make-up or information about its processes to lend credibility to other attacks.

"That information can be very specific, very focused," she said. "It can mention company names, actual events and people."

This information, said Ms Landesman, could help attackers embarking on social engineering attacks which attempt to con employees by posing as another worker or a business partner.

David Porter, head of security and risk at Detica, said the apparent familiarity of social network sites, which often help people build connections with people who share their interests and outlook meant many people were cavalier with their personal information.

"It is remarkable that people use social networking websites to publish details about their lives, loves, jobs and hobbies to the entire world that they would not dream of sharing with a stranger in a bar," he said.

"Such data is invaluable to identity fraudsters," he said.

This move to exploit social network sites would also fuel a move away from attacks that exploit vulnerabilities in the Windows operating system to gain control of a PC or steal data.

Far better for the criminal, said Paul King, senior security advisor for Cisco, is to use those phishing e-mails to exploit the end user.

"So many attacks now are nothing to do with an exploit. It's about persuading you to click a link," he said. "There's no vulnerability involved in you clicking on that. None."

The big challenge in 2008 for individuals and companies was coming to terms and recognising the sheer number of threats ranged against them.

But, he said, consumers and PC users should not feel stifled by all the potential security problems.

There were a lot of benefits to using social networking sites, said Mr King and the downsides should not put people off using them.

"It's about trying to manage risk rather than avoid risk," he said.

Story from BBC NEWS:
http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/7156541.stm

Published: 2008/01/03 09:15:53 GMT