



Identity theft 'almost effortless' in social networks

By *Liau Yun Qing, ZDNet Asia* on April 27, 2010

Summary

Cybercriminals find new ways to steal identities on social networking sites but naive users make such theft easy, say security experts who offer tips to protect identity.

Topics

[cybercriminal](#), [facebook](#), [financial](#), [identity theft](#), [malware](#), [network](#), [phishing](#), [social engineering](#), [social networking](#), [social networking site](#)

Users of social networking sites are making it easy for cybercriminals looking to steal identities for financial gains, according to security experts.

In an e-mail interview with ZDNet Asia, Ang Chye Hin, director of sales for SonicWall Asean, pointed out that committing identity theft is "almost effortless" as users often naively post seemingly harmless pieces of personal information on their social networking profiles, such as their full names, birthdates, addresses, phone numbers and names of relatives.

When these information are pieced together, identity theft is as easy as creating a fake profile on one of these social networking sites, Ang said.

Vincent Goh, managing director for RSA Southeast Asia, noted that social networking sites appeal to online criminals because of their global reach and the participation of hundreds of millions of active users.

He said in an e-mail that [20 percent of online attacks are now targeted at social networking sites](#), and cybercriminals are continually finding new ways of attacking even with the ever changing technology.

Malicious hackers apply methods such as social engineering, phishing and planting malware in third-party applications as new ways to steal user identities.

In her report titled "To Facebook or Not to Facebook", Chenxi Wang, principal analyst at Forrester, described the popular social networking site as "a perfect social engineering backdrop for targeted attacks". Wang noted that [account hijacking that leads to phishing and malware distribution](#) is Facebook's biggest problem.

Using the hijacked account, cybercriminals are able to use "blatant social engineering tactics" by crafting their messages based on information shared by other users on social networking sites. The messages are then used in phishing and malware distribution campaigns.

Apart from social engineering attacks, cybercriminals are also using sophisticated phishing technologies.

Goh said cybercriminals have resorted to replicating the design of legitimate Web sites and misleading users to reveal their personal details on the fake Web site.

Lack of apps testing

Less than rigid testing of third-party applications can also open up security holes.

Ronnie Ng, senior manager of systems engineering at Symantec Singapore, noted that social networking sites [are now providing third-party developers access to their API](#) (application programming interface), in efforts to provide more integration and better user experience. However, some developers do not run comprehensive tests for their third-party apps, Ng told ZDNet Asia in an e-mail.

Cybercriminals are likely to identify vulnerabilities in such applications and plant malware and tracking bots to steal users' identities. They will then use the stolen information for financial gain or to launch future attacks, he said.

But while cybercriminals are becoming more advanced in their attacks, the significance of identity theft is not reflected by law enforcement, where a [CNN report in March](#) quoted the U.S. Justice Department Inspector General to say identity theft initiatives have "to some degree...faded as priorities".

Top five tips to protect online identity

So users themselves need to be vigilant about protecting their online identities. Security experts highlighted five ways users can better safeguard their personal data:

1. Limit information posted on Internet.

Avoid revealing information such as birthdates, addresses and names of relatives, that will make identity theft easy for cybercriminals.

Ng said users need to be aware of the amount of personal data they post on the Internet as these can be used in malicious activities such as phishing scams or e-mail harvesting.

2. Be discerning about accepting strangers into your online network.

Goh noted that social networking sites are vulnerable to phishing attacks because strangers who are accepted into a user's network might be phishers.

Ang added that users should restrict access to their profiles. They should only allow people they actually know to access their profiles and not accept friend requests from strangers and unknown users.

3. Keep antivirus software updated.

Cybercriminals are now equipped with sophisticated tools that are able to infiltrate computers, said Goh. Therefore, users must stay vigilant and have proper antivirus software and firewalls.

Ng added that users must ensure their computers are updated with all necessary security patches from their operating system vendors.

4. Be familiar with the site's privacy policy.

"Familiarize yourself with the [social networking site's] privacy policy, especially if you are asked to provide confidential and personal data," Ng said.

Recently, users of Facebook [expressed their frustration when the social networking site](#) changed its privacy policy to allow third-party sites to access user data without users' prior permission. In a ZDNet Asia report, a lawyer [cautioned businesses against working with companies that make frequent changes to their privacy policies](#).

5. Be aware of personal computer safety.

Ng advised against storing online account credentials with the "Remember Password" feature offered by Web browsers.

Ang added that users must be more thorough about scanning all files that enter and leave their PCs. "Scan 100 percent of your data, there should be no exception," he said, noting that some users cite issues such as complexity, inadequate infrastructure, and lack of time and skills as reasons for selectively scanning or not scanning files at all.