Social networks posing security threat

By SYAHRIR MAT ALI

THE Internet is a lot more than just a means of staying informed. It has evolved into something much more than what it was originally intended to be.

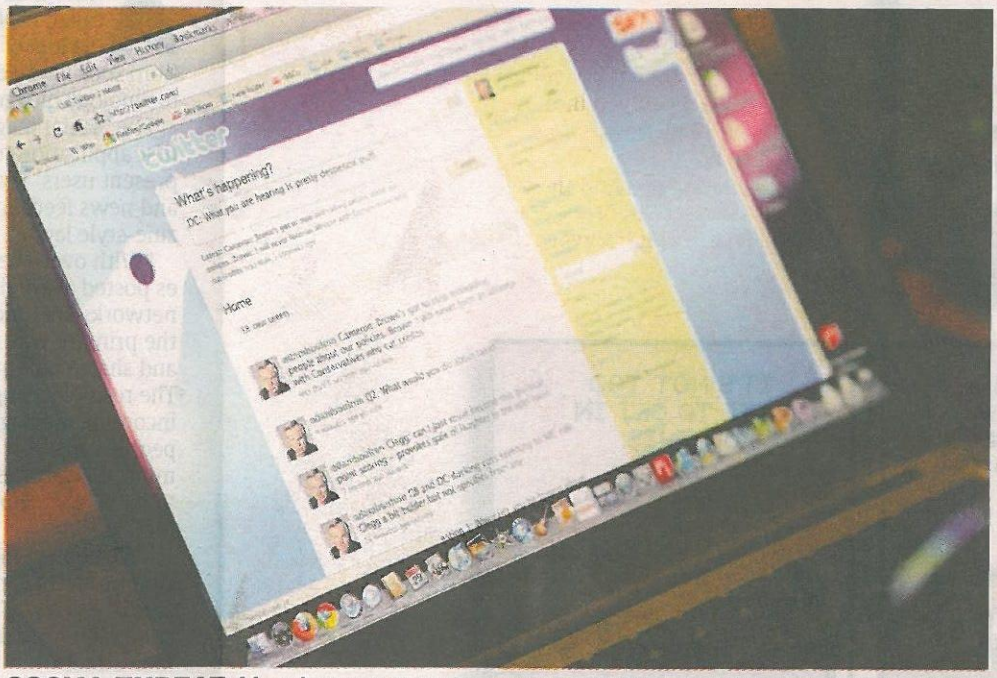
For some, it is an avenue to avoid the long queues at banks and service counters. For others, it is a place where you can work collaboratively.

But for most, the Web is a communication tool that connects them with family and friends via the many social networking tools.

Most Internet security experts conclude that cyberattacks on social networking sites will increase over the years. Since 2008, Facebook, Twitter, MySpace, LinkedIn, and other such sites have been in the limelight as social networking grew and grew.

These services compete with each other to increase their user base by coming up with mobile tie-ups, applications and games.

All these efforts are worthwhile because social networking sites are the biggest thing on the Internet at the moment, and perhaps for many more years to come. Unfortunately, this trend has also been attracting all sorts of security threats.



SOCIAL THREAT: Most Internet security experts conclude that cyberattacks on social networking sites like Twitter, Facebook, MySpace, LinkedIn and other such sites will increase over the years. — AP

New year, new threats

In its 2010 Threat Predictions report, McAfee Labs said it anticipates an increase in threats related to social networking sites such as Facebook.

It also said that criminal tool kits will be evolving rapidly this year to capitalise on new technologies that increase the sophistication of the attack on unsuspecting users.

And, as a result, there is a good chance of an increase in rogue services that exploit Internet users' eagerness to download and install the various and freely available Web 2.0 applications.

According to a Sophos survey in December 2009, 60% of the respondents believed that Facebook presents the biggest security risk compared to other social networking sites — way ahead of MySpace, Twitter and LinkedIn.

Cisco Systems' 2009 Annual Security Report mentioned that the Facebook user base has tripled from 100 million users in 2008 to 350 million in 2009.

There is no doubt that such a huge increase in the number of users within a year's time is phenomenal, and it is attracting cybercriminals from all over the world to migrate their attacks to Facebook.

Mitigating threats

In order to stay safe while using social networking tools (or in fact, other Internet-based applications), users are urged to observe the following practices:

1. Never click on any URL links in unsolicited e-mail (i.e. e-mail that you are not expecting nor asked for);

2. Never log in your online credentials through pages opened up by the URL links you get from any e-mail. In order to be safe, type the URL yourself in the browser. If you have been using shared PCs, be sure not to click on the links provided by the browser bookmarks;

3. Never jot down your online login credentials in an e-mail, even if you think of it as a note to yourself. e-Mail is not the proper place to store your online login credentials. This is to minimise the risks should your e-mail system be compromised;

4. Always verify the validity of the services or links you get via e-mail, even if it appears to be sent by a social networking tool you subscribe to. Google it or better yet, e-mail the service administrators and ask them. Pay extra attention to the given URL as a slight difference would mean a different site altogether;

5. Change the passwords of your online credentials from time to time and do not use the same password for all of them. For a secure password, use a combination of uppercase and lowercase alphabets and numbers, and try to use words that do not exist in any dictionary; and

6. Do not arbitrarily download any updates for your applications. If you really need them, visit the official website and get more information.

Conclusion

It is imperative that Internet users understand that the threats and security issues which come with social networking tools aren't necessarily caused by vulnerabilities in the software or the user's PC ... at least, not all the time.

Software vulnerabilities are reported from time to time and they will always be the cornerstone of cybercriminal activities. But for them to work, they have to be initiated by the users themselves in one way or another.

(Syahrir Mat Ali is senior executive of the cybermedia research department at CyberSecurity Malaysia — the national cybersecurity specialist under the Ministry of Science, Technology and Innovation. These are his personal views expressed here.)