When Web 2.0 Becomes Security Risk 2.0

Hackers are manipulating the trusted nature of Facebook, MySpace and other social networks to launch exploits and spread malware attacks. Kaspersky Lab security evangelist, Ryan Naraine, discusses this growing threat and recommends some basic social networking rules that will allow you to protect your organization.

By Ryan Naraine
Security Evangelist
Kaspersky Lab Americas

Social networking is all the rage these days. Facebook. MySpace. LinkedIn. Hi5. Orkut. Twitter.
The names may sound strange to the uninitiated, but for hundreds of millions of computer users around the world, these social networks offer efficient and powerful ways to communicate with friends, family and co-workers. Addictive and popular, end users -- including businesses – are spending countless hours on social networks, sharing everything from photographs, videos, personal messages, and notes with potentially millions of others around the globe.
At their most basic level, social networks like Facebook and MySpace provide a set of features for end users to set up and customize a personal 'profile' and privacy settings to approve other members who can view their profile. It also offers the ability to block an unwanted member.
This creates a facade of trust where end users feel comfortable enough within their network to click on every link they receive, and post the most intimate details about their private lives. In our research, we have seen that people do not exercise the same amount of caution on social networks as they would when communicating in person, setting up scenarios where it becomes very easy to manipulate these trusted networks for malicious purposes both within and outside of your organization. Activities conducted by employees can easily spread inside your company.
In November 2008, a Google executive in Australia named Karina Wells received a message on Facebook from a friend who was within her circle of connections on the social network. In the message, the friend said he was stranded in Lagos, Nigeria, and desperately needed $500 wired there for a ticket home.[1]

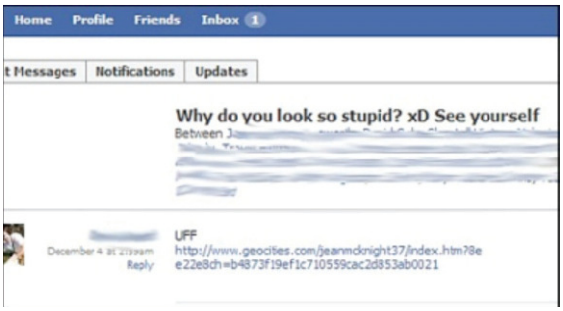

smh.com.au
The Sydney Morning Herald
Ads by Google
Redaction Software
Automated TIF/PDF Redaction, Automated Indexing/Docketing
Technology
Gadgets Games @Home Biztech Security Connectivity Tech Tips iPhone Insider
You are here: Home » Technology » Security
Cyber criminals target Facebook users
Asher Moses
November 10, 2008 - 2:27PM

It was a familiar scam (we've all received those Nigerian gold bullion emails) that has now been exported to social networks, exploiting the "trusted" nature of the friend circles to steal money. In Wells' case, a scammer had obtained her friend's Facebook username and login – either via phishing or via a password-stealing malware attack – and had spent enough time on the Facebook account to impersonate the friend and look for likely targets.

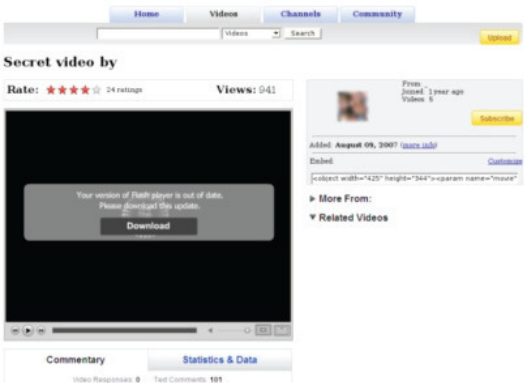
A Social Engineer's Dream

Social engineering, which is the act of using clever lures to trick people into divulging confidential information, is also prevalent on social networks. It's a technique perfected on email networks where users are typically lured to a fake banking site controlled by cybercriminals. Once the data is entered into the fake site, it is stolen and used in identity theft crimes.

On social networks, it becomes even easier to exploit trust and launch social engineering attacks. We have monitored several phishing scams targeting Facebook or MySpace where a user received an email (from a trusted friend) with a link to a groundbreaking news event or an exciting photograph or video. A user clicking on that link is taken to a bogus site that imitates login page of Facebook or MySpace. The end result is another stolen credential.



This type of social engineering attack scenario becomes even more dangerous when the URL lure is associated with a drive-by malware download (see first paper in this series).
In one major attack, called Koobface2, malware authors manipulated Facebook's private messaging system to infect computers via a link promising a video file. Unsuspecting users started receiving private messages (again, from trusted friends) with a link to a third-party site



and a message that said simply: "You look just awesome in this new movie."
By clicking the link, the user is directed to a web site that pops up an alert that the user needs to download a Flash Player update. That Flash Player update was actually a malicious executable programmed to steal sensitive data from an infected machine.
Once that executable is installed on a Facebook or MySpace users machine, the victim then becomes a pawn in the attack. The next time the user of that infected machine logs into Facebook, the lure is then sent to all of their friends and the infected link is automatically added in comments on friends' pages. This creates a network worm capable of propagating an infection across the globe.
As more and more teenagers, adults and businesses turn to Facebook, MySpace and popular social networks to communicate and do business, it's important to understand the risks and threats.

Protect Yourself

Here are some basic rules you should implement within your organization and have all employees observe when using social networks whether on or off your company's network:

- **Distrust everything.** That friend sending a link to a funny video might have had his/her account compromised. Get into the habit of not clicking on links, especially those for videos or news-related events. In most cases, these are linked to social engineering attacks. When using private messages and live-chat features on social networks, ask a lot of questions and go the extra mile and make a phone call to ensure you are indeed talking to the right person.
- **Limit the amount of personal information you willingly post to social networks.** Try to avoid posting information like your home address, personal phone numbers or details about your schedule or routine. This type of information could make you vulnerable. Assume that anything you post on Facebook or MySpace can be seen by a stranger and act accordingly. Be wary of the type of information, including photographs that you post about your friends. That information can put them at risk.
- **Question everything you receive from a stranger.** Limit who can contact you on social networks. It's very easy to impersonate or misrepresent identities on the Internet.
- **Don't post anything that you wouldn't want the public to see**. Most social networks offer settings to keep profiles private and restrict access to your photographs or other personally identifiable details.
- **Invest in an anti-malware software solution and ensure definition signatures are kept up to date.** This can help reduce your exposure to known virus attacks.

[1] http://www.smh.com.au/news/technology/security/cyber-criminals-target-facebookusers/2008/11/10/1226165454265.html
[2] http://www.kaspersky.com/news?id=207575670

Contact Information

To find out how Kaspersky Lab technology can help protect your business, call the Kaspersky Lab UK team on **0871 789 1631** or visit www.kaspersky.co.uk