# More computer worms, viruses expected to target social networks

January 15 2010, By Bridget Carey

Social networkers of the world, it's time to amp up your security software and put on your cynical cap before clicking on friend requests and links to "funny videos." Facebook and Twitter will be the top targets for cyber attacks in 2010, according to several security firms.

Networks like Facebook are a gold mine of information for identity theft scams. You may have stumbled upon a cyberattack or two before on Facebook. It's usually an inbox message from someone you don't talk to often, with the message: "Hey is this you in this video? LOLZ!!!" followed by a strange link with random letters in it.

Click on the link, and it can take you to a site that will download a program designed to steal your personal information and spread the malicious link to all your Facebook connections, without you even knowing it. The Koobface worm was one such program. In 2009, the CA Internet Security Business Unit found more than 100 mutated strains of that worm.

But it's more than just inbox links. It can be a friend request from a fake account, or an invitation to an event that takes you to a page that looks like a Facebook event, but instead takes you to a page to download something.

Dave Marcus, director of security research and communications at McAfee, has seen a few of those tactics on Facebook, as well as sites with advertisements for fake products that steal your credit card info

when you think you're just buying something.

Those that recognize fakes are in the vast minority of users, Marcus said. This is because on social networks, people are more trusting of links and get click happy. Users may think twice about clicking something unusual in an e-mail, but they are more likely to click without thinking on Facebook or Twitter.

The growing popularity of URL shorteners adds to the problem. Sites like bit.ly or tinyURL.com let you paste in a really long URL and then generate a link that is just a few characters long -- usually just random letters and numbers. URL shorteners are widely used on Twitter, which limits how many characters you can type. Some shorteners also let you track how many clicks that link got.

These URL shorteners mean users are getting used to clicking links, not knowing where they are going, and trusting that nothing bad will happen.

"I think people need to look at the Internet with a little more skepticism and stop always accepting things being sent to them as real," Marcus said.

Since cybercriminals are constantly changing their tactics, Marcus said the best way to keep protected is to keep your computer security software up to date -- and if you're not sure about a link, just ask the IT folks in your office.

They would much rather help you figure out if a link is malicious, rather than spending the day cleaning up a worm you spread through the office.