

Web sites you maintain

Any web site you maintain, blog you write, or pages on social networks like Facebook or MySpace you set up could give away too much information. You can limit who has access to your information on social networking sites, but people often wind up with a very large circle of “friends,” including people you meet in passing or exclusively on the Internet. Not knowing exactly who you are sharing your information with means you could open yourself up, or those close to you, to harassment and threats.

Online information about you can also make it easier for someone to steal your identity, or set you up for some sort of scam. For example, if you write about plans for an upcoming vacation on a blog or social networking site, you could be telling a thief when to burglarize your home.

You are also at the mercy of how well these sites are protected. On several occasions, “programming errors” have exposed people’s information on social networking sites.

How can you protect yourself?

- **Limit the amount of personal information you post** - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine.

- Remember that the internet is a public resource.

- **Be wary of strangers** - The internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who are allowed to contact you on these sites.

- **Be skeptical** - Don’t believe everything you read online. People may post false or misleading information about various topics, including their own identities.

- **Evaluate your settings** - Take advantage of a site’s privacy settings. The default settings for some sites may allow anyone to see your profile. You can customize your settings to restrict access to only certain people. However, there is a risk that even this private information could be exposed, so don’t post anything that you wouldn’t want the public to see. Also, be careful when enabling applications, and check your settings to see what information the applications will be able to access.

- **Use strong passwords** - Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.

- **Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.

What is social engineering?

Microsoft .com

Online criminals can use sophisticated technology to try to gain access to your computer, or they can use something simpler and more insidious: social engineering.

Social engineering is a way for criminals to gain access to your computer. The purpose of social engineering is usually to secretly install spyware or other malicious software or to trick you into handing over your passwords or other sensitive financial or personal information.

Some online criminals find it easier to exploit human nature than to exploit holes in your software.

Types of social engineering

- Phishing - attempts to get your user ID and password
- Spear phishing - personalized email in an attempt to get your user ID and password
- E-mail hoaxes

Do not reveal any personal information in e-mail or online unless you know who you are dealing with and why. Additionally, make sure you are in a secure environment: that’s the key to help you avoid any type of attack.

Destructive Koobface virus turns up on Facebook

December 4, 2008 | usatoday.com

Facebook's 120 million users are being targeted by a virus dubbed "Koobface" that uses the social network's messaging system to infect PCs, then tries to gather sensitive information such as credit card numbers.

It is the latest attack by hackers increasingly looking to prey on users of social networking sites.

"A few other viruses have tried to use Facebook in similar ways to propagate themselves," Facebook spokesman Barry Schnitt said in an email. He said a "very small percentage of users" had been affected by these viruses.

"It is on the rise, relative to other threats like e-mails," said Craig Schmugar, a researcher with McAfee Inc.

Koobface spreads by sending notes to friends of someone whose PC has been infected. The messages, with subject headers like, "You look just awesome in this new movie," direct recipients to a website where they are asked to download what it claims is an update of Adobe Systems Inc's Flash player.

If they download the software, users end up with an infected computer, which then takes users to contaminated sites when they try to use search engines from Google, Yahoo, MSN and Live.com, according to McAfee.

Facebook requires senders of messages within the network to be members and hides user data from people who do not have accounts, said Chris Boyd, a researcher with FaceTime Security Labs. Because of that, users tend to be far less suspicious of messages they receive in the network.

"People tend to let their guard down. They think you've got to log in with an account, so there is no way that worms and other viruses could infect them," Boyd said.

Privately held Facebook has told members to delete contaminated emails and has posted directions at <http://www.facebook.com/security> on how to clean infected computers.

McAfee has not yet identified the perpetrators behind Koobface, who are improving the malicious software behind the virus in a bid to outsmart security at Facebook and MySpace.

"The people behind it are updating it, refining it, adding new functionalities," said McAfee's Schmugar.



Information & Technology Services

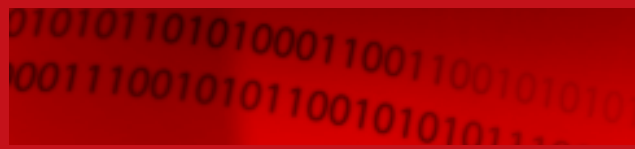
Web 2.0 Safety Tips

Because we care, we're security aware

Just as the Internet makes it easy for you to find all sorts of information, you risk others finding out things about you that you don't intend to be public. You may think of sitting in front of a computer as a private experience, but at some level your activity can be traced.

There is always the chance that the information you send over the network, or store on a network server, could fall into untrustworthy hands.

As an experiment, see what happens when you put your name into Google or another search engine. You might be surprised at what is out there.



WEB 2.0 SAFETY TIPS

Because we care, we're security aware
www.SBUniv.edu/ITS/CyberSecurityAwareness/