When you think of “Hackers,” you may remember a 1995 movie where teenagers harmlessly competed to prove their skills. However, hackers have evolved into a world of cybercrime with highly organized, well-funded crime syndicates launching sophisticated attacks from around the globe. This new generation of cybercriminals dedicates immense quantities of time and resources to building better viruses and online scams. From fake Rolex watches to bogus software and phony discount pharmacies, cybercriminals reap billions of dollars every year through scams planted in emails, pop-up windows, Twitter and Facebook messages, and even links inserted on legitimate sites.¹  

Real Villains of Cybercrime

continued

Some cons target individuals, tricking them into revealing credit card numbers. Others infect personal computers to build zombie networks used in coordinated attacks on university, corporate, and government databases.

Cybercriminals are running smarter scams and producing more ingenious software. No longer are hoaxes easy to spot through bad grammar or poorly constructed web sites. Scammers have honed their skills to develop sites and emails that closely resemble legitimate businesses. Improved viruses have been designed to mask symptoms, such as programs running slowly or closing unexpectedly.

What can we do to protect ourselves?
• Keep your computer’s software and operating system updated.
• Do not click links in an email or open attachments unless they are from a trusted source.
• Be suspicious anytime a web site or email asks for your personal information.
• Never click Internet pop-up ads.
• Do not use Facebook games or applications that require downloads.

Learn more about how to stay safe at security.tamu.edu.

A special IT Forum on October 27th from 3:00 – 4:30 p.m. in Rudder 601 will be dedicated to discussing the new generation of cybercrime. See the back page for more details.

Spam

Spam is unsolicited junk email, often generated for criminal or fraudulent schemes such as identity theft. To combat spam, delete unsolicited email or move it into the Junk folder. Use the junk mail handling tools in your email program, such as block lists. To protect your @tamu.edu email, obtain a free account, such as Gmail or Yahoo Mail, for filling out web registration forms.

Reporting Spam

See the Spam section of the Information Security web site (http://url.tamu.edu/stayingsafe) to learn more.

What to Do if it Happens to You!

IT Recipe

Listen to KAMU Streaming Radio

1. Go to http://kamu.tamu.edu
2. Click “Listen Now”
3. Choose “Original Format” or “Talk Radio”

Now you can listen to the “Computer Tip of the Week” on Wednesday at 7:30 a.m.

979.845.5611 | penny@kamu.tamu.edu
Take Charge of Your Online Reputation

An online reputation is the public perception of a person based on their online behavior and what is shared about that person by others.

From keeping in touch with friends and family, investigating a job applicant, to seeking information about a potential date, searching online about other people is a common occurrence. As online information about us proliferates, the effects of your online reputation on your personal and professional lives may increase. Also, your information may be harvested for all the wrong reasons – such as identity theft and online fraud. Taking charge of your online reputation is important not only to avert misunderstandings or embarrassment – it helps thwart online thieves.

How can you manage your online reputation?

- Safeguard personal information online. Do not publically reveal your full birth date, address, or phone number.
- Be aware of how you are perceived online by searching for your name.
- Use privacy settings on social networking sites to limit who can view your full profile.
- Be diligent about removing embarrassing or false information by deleting unwanted comments or untagging photos.
- Separate your personal and professional online profiles, such as using Facebook and LinkedIn.


Facebook Privacy Settings

Facebook’s recommended privacy settings reveal personal information that can be used by thieves to steal your identity. By default, anyone in a network you are a part of, including people who are not your friends, can see your full profile. To protect yourself, restrict your profile information to be viewable by only friends.

- Under “Settings,” go to the “Privacy” section.
- Click “Profile.”
- Change to “Friends Only.”

Default settings allow Facebook to release information about you to all site sponsors, including what you like or find interesting, your location, and email address. Default settings also make your profile searchable by Google and other search engines.

Facebook does provide many options to customize privacy settings. However, these options can be difficult to understand by the average user. Sophos, a leading IT security firm, provides an online guide to walk you through setting up secure settings on Facebook (www.sophos.com/security/best-practice/facebook/).
Mark Your Calendar

IT Forum
October 27, 2010
3:00 – 4:30 p.m.
Rudder 601

Mark your calendar for IT Forum. Chet Wisniewski from Sophos will present “How Hackers Become Millionaires.” This unique presentation will describe the ways cybercriminals attack and how you can protect yourself.

Chet Wisniewski is a Senior Security Adviser for Sophos with 15 years of network security consulting experience. He works with the SophosLabs to develop in-depth analyses of network security threats.

Free Upgrade to a Combo
Buy any regular menu item and get a free upgrade to a Rev’d combo: fountain drink and your choice of dessert or chips & dip.

For crossword solution and coupon details, go to http://security.tamu.edu/Crossword.php