SIU SOUTHERN ILLINOIS UNIVERSITY CARBONDALE COLLEGE OF EDUCATION AND HUMAN SERVICES

COMPUTER TECH SUPPORT NEWSLETTER

IT Computer Technical Support Newsletter

March 7, 2016

Vol.2, No.18

TABLE OF CONTENTS

The IT Computer Technical Support Newsletter is complements of Pejman Kamkarian

Secure Your PC

Too often, computer and network security is not thought about until a problem arises. At this point, a breach in security can cause huge and potentially harmful problems to your business and/or your customers. By setting up a security plan and an emergency action plan, you can know that the information held in your computers and networks is safe and secure.

Computer Security

What is computer security?

Computer Security is the process of preventing and detecting unauthorized use of your computer. It involves the process of safeguarding against intruders from using your computer resources for malicious intents or for their own gains.

Computer security encompasses several security measures such as software programs like anti-virus suites, firewalls, and user dependent measures such as activating deactivating certain software features like Java scripts, ActiveX and being vigilant in using the computer and the network resources or the Internet.

Computer Security is concerned with four main areas:

1. **Confidentiality:** Only authorized users can access the data resources and information.
2. **Integrity**: Only authorized users should be able to modify the data when needed.
3. **Availability**: Data should be available to users when needed.
4. **Authentication:** are you really communicating with whom you think you are communicating with

Why is computer security so important?

Prevention of data theft such as bank account numbers, credit card information, passwords, work related documents or sheets, etc. is essential in today's communications since many of our day to day actions depend on the security of the data paths.

Data present in a computer can also be misused by unauthorized intrusions. An intruder can modify and change the program source codes and can also use your pictures or email accounts to create derogatory content such as fake, misleading, or offensive social accounts.

Malicious intents can also be a factor in computer security. Intruders often use your computers for attacking other computers or websites or networks for creating havoc. Vengeful hackers might crash someone's computer system to create data loss.

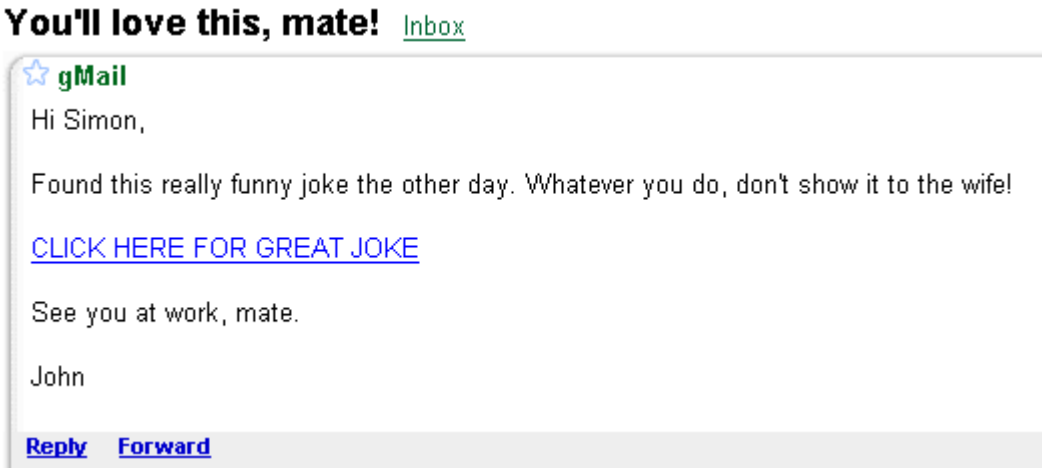
Spyware

What is Spyware?

- Broadly speaking, Spyware is something that sneaks on to your computer, usually with the intentions of extracting money or information from you.
- Spyware can take control of your computer, directing you to unwanted web pages, downloading files, and even harvesting email address, passwords and your credit card details
- Spyware, generally, gathers information about you and your online habits, and sends that information to third party. And all without asking for your permission!
- If you've ever been plagued by annoying pop-ups when your computer loads, had strange new icons, or are redirected to strange websites, then you may have been infected.

Where does Spyware come from?

Spyware can come from a whole host of different sources. But Spyware mainly gets on to your PC through deception. For example, suppose you receive this email:



You'd assume that this email was sent to you in error but the web page is actually trying to sneak something on to your PC! You may also have seen a harmless-looking popup window asking you to click a button to proceed. Do not click it! That will get your PC infected.

Other sources of Spyware infection are freeware or shareware software, an operating system that hasn't got the latest security software, downloading files from peer-to peer applications - the list is long.

Since Spyware is not considered a virus, relying only on your anti-virus is not secure enough. The best tool for the job is a dedicated Spyware Detection system.

How do I avoid Spyware?

- **Don't click on links within pop-up windows** - Because pop-up windows are often a product of spyware, clicking on the window may install spyware software on your computer. To close the pop-up window, click on the "X" icon in the title bar instead of a "close" link within the window.
- **Choose "no" when asked unexpected questions** - Be wary of unexpected dialog boxes asking whether you want to run a particular program or perform another type of task. Always select "no" or "cancel," or close the dialog box by clicking the "X" icon in the title bar.
- **Be wary of free downloadable software** - There are many sites that offer customized toolbars or other features that appeal to users. Don't download programs from sites you don't trust, and realize that you may be exposing your computer to spyware by downloading some of these programs.
- **Don't follow email links claiming to offer anti-spyware software** - Like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating.
- Adjust your browser preferences to limit pop-up windows and cookies

How do I remove Spyware?

- Run a full scan on your computer with your anti-virus software.
- **Run a legitimate product specifically designed to remove spyware** - Popular products include Lavasoft's Ad-Aware, Microsoft's Window Defender, Webroot's SpySweeper, and Spybot Search and Destroy.
- Make sure that your anti-virus and anti-spyware software are compatible.

Spam

What is spam?

Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender.

How does spam work?

At its simplest, spam is the mass mailing of a single email to thousands, millions or billions of recipients. The spammer obtains a list of valid email addresses from one of several sources and then fires out as many emails as they want, hoping to get one or two percent of profitable responses.

How do I avoid spam?

- Keep your email address to yourself as much as possible.
- When posting on a forum, do not include your email address as part of your signature.
- Review privacy terms on websites before registering.
- Do not use the unsubscribe links in spam emails, in some case that will actually confirm the email address is valid to the spammer.
- Never click on links in spam email.
- Do not open attachments in spam, you could get infected with Trojans that will send your email contacts to a spammer as well as entrap you in a spammer distribution chain i.e. your computer might be the one that the spammer uses to send spam emails.

Anti-Virus

Antivirus or anti-virus software sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software. Antivirus software was originally developed to detect and remove computer viruses, hence the name. However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats

Antivirus do's and don'ts -

- Do run the antivirus program in full-time, background, automatic, auto-protect, or similar mode.
- Do enable Macro Virus Protection in all your Microsoft Office programs.
- Don't allow your e-mail programs to "auto open" attachments.
- Don't open attachments from people you don't know or attachments that seem suspicious.

Trojans

What is a Trojan?

A Trojan is small, malicious program that is installed along with a more attractive one. For example, that great freeware program you got from that sketchy website? It may well be the program you wanted but someone (3rd party) may well have attached a Trojan to it. The Trojan will be installed as well as the software you wanted.

Trojans are not viruses, in the sense that they don't replicate or send copies of themselves to others. They are just another program that can be installed on your computer, albeit a nasty one.

What do Trojans do?

A Trojan can be very malicious indeed. Most of them are intent on controlling your PC. These are called Remote Access Trojans, or RATs for short. If someone has placed a Trojan on your computer, they'll be able to see everything that you can. Some of them can even control your webcam.

Most Trojans are placed on your computer by criminals. If you type your credit card details in to a website, for example, then the attacker can record what you type. If a criminal has control of a lot of computers, they could also launch something called a Denial of Service attack. A DoS attack is when a lot of malicious computers attack a particular network or website. The network has so many request that it can't cope, so has to shut down.

A Trojan can also disable your security software, leaving you wide open on the internet.

How Can I Protect Myself?

The best defense against Trojans is a dedicated Trojan scanner. There are several free online Trojan scans available.

Consider buying separate software just for Trojan protection. Not only will these detect the latest threat, but they will also rid your computer of any infection.

Trojans can be far more harmful than viruses, so it's well worth getting the right tool for the job. Don't skimp in this area!

Rootkits

What is a RootKit?

A rootkit is a program, script or set of software tools that allows an attacker administrator-level access to your PC or network. A rootkit is really the technique for getting harmful things like Trojans, Spyware and Viruses on to a system.

Why are RootKits so dangerous?

The main form of an attack for a rootkit is stealth. They will hide away, deep in the recesses of your computer. Because they have administrator-level access they can do things like hijack your Windows searches and hide any information about the RootKit, control your Anti-Virus software and tell it to ignore the RootKit, hide from the list of active processes. And a whole lot more besides!

Example: The most famous RootKit was one that was installed by some Sony audio CDs. Sony hid a RootKit on people's computer as part of its Digital Rights Management strategy. This gave them effective control of a user's PC. A security expert called Mark Russinovich discovered the Sony RootKit, and it made the news the world over. Sony had to issue a download so that people get the RootKit off their computers. They also recalled all the music CDs that had the RootKit software.

It's the fact that RootKits are so difficult to detect that makes them dangerous.