



Home Computer Security

Recommendations for Keeping Your PC Safe

Presented by
Karr Tuttle Campbell

Objectives

- n Prevent viruses and worms
- n Protect your data from malicious programs and hackers
- n Ensure your computer is not being used as a “zombie”
- n Make your computing experience more efficient and pleasant

What Are Some Symptoms of Having a Virus?

- n Computer may slow down or stop responding or crash
- n Annoying messages
- n Corrupted or deleted data
- n Computer may restart every few minutes
- n Computer hijacking
- n Disabled email
- n Computer may not start at all

Unless you have up-to-date antivirus software installed on your computer, there is no way to know if you have a virus or not

What Symptoms Do Not Necessarily Mean You Have a Virus?

- n Getting a non-delivery report for messages you never sent
- n Receiving an email that says you have a virus
- n Spam that comes with your name as the sender

Unless you have up-to-date antivirus software installed on your computer, there is no way to know if you have a virus or not

Where Am I at Risk for Viruses?

Email messages and attachments	Shared floppy disks or CDs	Downloaded files
Visiting a web site	Instant messaging	File sharing networks
Online 24/7	Wi-Fi	Documents and spreadsheets

The Basic Toolkit



- n Most important - practicing safe computing habits!
- n Current Windows security patches (critical updates)
- n **Up-to-date** antivirus software
- n Firewall – hardware and/or software

Phishing messages and attachments
Spam messages and attachments

Safe Computing - Email

- n Never open an e-mail attachment even from someone you know, unless you were expecting it and know exactly what the attachment is.
 - u Viruses can forge the From field in an email, so you cannot tell where the message really came from
- n Delete suspicious emails without opening them. Some viruses can run malicious code without an attachment
- n Spam – do not reply to it or unsubscribe from a list you did not sign up for; this will get you **more spam**

Phishing messages and attachments

Safe Computing - Email

- n Phishing – never divulge personal information in response to an email, even if you think it is from a trusted source such as your bank, PayPal or EBay
- n Internet hoaxes – including virus hoaxes and urban legends– learn how to recognize them; do not forward them on
- n Watch out for email scams
 - u Never “pay money” to “get money”
 - u Never use credit cards for ID or age verification
 - u Never send money for “limited editions or specials”

Using IM
Visiting a web site

Safe Computing - Internet

- n Disconnect from the Internet when you are not using it (don’t just close the browser)
- n Consider raising your security settings in Internet Explorer
 - u Tools, Internet Options
 - u Security tab
- n Consider using a browser other than Internet Explorer for most of your surfing

Wi-Fi

Safe Computing - Wireless

- n If you have a wireless connection on your laptop secure it with a password
- n If you take your laptop outside your home use a Windows password as well
- n Make sure you have a firewall enabled

Using IM

Safe Computing – Instant Messaging

- n Using Instant Messaging opens a gateway to your computer
- n It’s the “Instant” part of Instant Messaging that is the problem - new viruses spread rapidly and can infect before virus updates or security patches are available
- n Beware of file transfer requests - don’t use IM for transferring files
- n The less you use IM the better – keep it closed when you are not using it

Home Networks - File Sharing

- n If you have a home computer network and you want to share a folder or folders:
 - u Turn on sharing only for those folders you need to share
 - u Place a password on the share

File sharing
networks

File Sharing – Internet Peer-to-Peer

- n File sharing programs that allow you to download programs like music, videos or games are a security risk to your computer. Some examples are:

nKazaa	nE-Mule
nLimewire	nBit-Torrent
nBearshare	nGrokster

Windows Security Patches



- n Windows Update – recommended **weekly**
 - u Start, Control Panel, Windows Update, Scan for Updates
 - u Download and install all critical updates

OR

Windows Security Patches

- n Set up your computer to get updates automatically
 - u Right click on My Computer, select Properties
 - u Click Automatic Updates tab

Antivirus Software

- n There are many options for antivirus software:
 - u Norton / Symantec
 - u Network Associates / McAfee
 - u AVG (is a good free one)
- n Stingers

Antivirus Software

- n What's most important?
 - u Update the pattern files for the software weekly; most software can be set to go look for the updates automatically
 - u Set the software to scan live any files that are introduced to the computer
 - u Run a full virus scan of your computer weekly

Popups, Adware, and Spyware

Downloaded files

- n Popups can come from the site you are visiting, OR
- n As a result of spyware or adware which is downloaded onto your machine.
- n Be careful what you download – software you want (such as a fun toolbar or weather utility) sometimes comes with some “extras.” Read the full terms of service or conditions of license.

Popup Prevention and Cleaning Off Adware and Spyware

- n The Google Toolbar's popup blocker is a good first start.
- n Lavasoft Ad-aware – simple and there is a free version for personal use
- n Spybot – Search & Destroy – a little more advanced, but very useful if you have a bad problem with ads and pop-ups
- n Run Ad-aware and/or Spybot monthly or more frequently if needed

Zombie Machines

- n Zombies are computers that have been taken over by hackers and spammers, who then use the machine as a launching pad for malicious attacks.
- n What could happen if your machine is used as a zombie:
 - u Computer could run slower because it is busy helping the bad guys
 - u ISP might cut you off or blacklist your site
- n Good firewall protection can prevent much of this

Firewalls

- n What is a firewall and when is it important?
- n What are the options?
 - u Hardware firewalls (router)
 - u Firewall software (best when used in conjunction with a hardware firewall)
 - † ZoneAlarm
 - † Sygate's Personal Firewall
 - u Windows XP firewall (better than nothing but don't rely solely on this one)
 - u If you want the most secure setup, use all 3!

What to Do If You Get Infected



- n If you can see your computer actively running a program you did not intend, turn the PC off
- n Make sure you have the current Windows updates and pattern files for your antivirus software
- n Clean the virus using your antivirus software
- n If you can't get to your antivirus software or if it is disabled, the KTC IS Team can provide Stinger on a CD for your use.
- n Get some professional assistance if necessary.

Kid Safety

- n Kim Komando's 10 Commandments for Kids Online
- n Consider content filtering software
- n Microsoft has some great articles on how to keep kids safe online (see handout for URL). Includes:
 - u Blocking unknown contacts in Windows Messenger
 - u Checking History so you know where your kids have visited
 - u Adjusting browser security settings

Help at Home


- n "My computer is a total mess and I would be willing to pay someone to come help me with it. Who can help me?"
 - † Get advice on your specific computer
 - † Help with home networks; broadband, firewalls, wireless, viruses, spyware issues; content filtering
- n G Assistance (card available)
- n Geek Squad

More Information

n Check out the Training Corner at:
<http://training.karrtuttle.com>
Click on Cyber Security
Includes:

- More information and articles
- Links to helpful downloads

THE END



#793