

Staying Safe Online

A. Computer security

Run regular full-system scans of your computer and eradicate any malware that's reported.

Virus protection

Viruses attach themselves to programs or documents.

Worms send themselves around the internet.

Trojan horses appear to be cute screen savers or games, but are actually destructive.

See "Protecting Your Computer"

http://www.kuhnfamily.com/Kuhn_Consulting/Computer-items/Protecting_your_computer-Summary.pdf

Firewall

Anyone concerned with the threat of spyware or data leakage from other malicious software should spend some time configuring their firewall. A firewall acts as a gatekeeper, tracking and monitoring the applications that exchange information with a network. The firewall is a cornerstone of any secure PC, so you should always take the time to understand and work with this important tool.

Start by verifying that your firewall is enabled. This option is typically displayed prominently in the firewall portion of your security software. If the firewall is disabled, you should check if there is other security software providing firewall services (such as Windows Firewall). A computer doesn't need more than one firewall, so if you are using Windows' built-in firewall, you can opt to leave the firewall in your security software disabled.

A firewall can also allow or block communication from each program.

Programs on every computer built by my computer builder (Larry Golub):

Avast Home edition Anti-Virus (very small memory footprint, works very fast, and seems to catch anything that tries to slip in)

XP Firewall enabled (In conjunction with a broadband router) but doesn't seem to hurt performance; unlike Norton, McAfee and Zone Alarm-UGH!)

Ad-Aware

SpywareBlaster (recommended by the makers of Spybot, but two separate companies)

CCleaner

These are other defense software worth mentioned by Noel: Windows Defender, Microsoft Security Essentials, Malwarebytes, and AVG Version 9. (this is a strong protection package although it does consume more system resources than does AVAST). These are all free programs.

· **Malicious Software Removal Tool** checks your PC for infection by specific, prevalent, malicious software and helps remove an infection if one is found. Microsoft releases an updated version of this tool on the second Tuesday of each month.

· **Windows Defender** helps you stay productive by protecting your PC against pop-ups, slow performance, and security threats caused by spyware and other potentially unwanted software. Real-time protection helps prevent new spyware from installing, while a streamlined alert mechanism minimizes interruptions. From installation to maintenance and updates, Windows Defender is easy to use and comes with pre-configured settings designed to help you stay secure. Information and guidance is provided by dedicated analysts to help you stay safe. Windows Defender and on-going updates are available for no additional charge to Windows XP and Windows Vista customers.

Staying Safe Online

[Microsoft Security Essentials](#) provides real-time protection for your home PC that guards against viruses, spyware, and other malicious software. Microsoft Security Essentials runs quietly and efficiently in the background so that you are free to use your Windows-based PC the way you want—without interruptions or long computer wait times. Microsoft Security Essentials is a free* download from Microsoft that is simple to install, easy to use, and always kept up to date so you can be assured your PC is protected by the latest technology. It's easy to tell if your PC is secure — when you're green, you're good. It's that simple.

Product name and intended users	Spyware: Scan and remove	Spyware: Helps protect	Viruses: Scan and remove	Viruses: Helps protect	Scheduled scanning provided	Provided at no additional cost
Windows Defender — Consumers	X	X			X	X
Malicious Software Removal Tool			X			X
Microsoft Security Essentials — Consumers	X	X	X	X	X	X
Microsoft Forefront Client Security — Businesses	X	X	X	X	X	

B. Now that your computer is protected, there is a lot that YOU can do to enhance your online security.

Phishing

Emails that look authentic, but are scams, are made to look like them came from credit card companies, banks, lotteries, and sweepstakes. Don't click on any link in these emails; instead, open a new browser tab or window and go to your company's website and login.

Personal information

Don't enter any sensitive personal information such as Social Security number, bank account numbers, or credit card numbers, expiration date, or security number, on a connection that is not secure.

Secure data transfer

Example: <https://mail.google.com/>. The "s" after the "http" shows that there is a secure connection between your computer and the server at the site you are communicating with, such as google.com. A secure connection has all transmitted data (to and from your computer) encrypted so only your computer can show the correct information. Data that is in-transit between your computer and your internet site appears as garbage to anyone trying to view the data.

Staying Safe Online

Be suspicious

View all emails and websites with caution.

Reasonable and logical? Does the information appear to be reasonable and logical? If you win a lottery or prize, there are better ways to notify you and with an email.

Correct? Is the information in the email or website correct, well-written, and specific? Do you have an account at that company?

Specific? Is the email addressed to you, or to anyone?

Secure? If there is a link in the email (don't follow it!), does the link take you to a secure web page?

Use one-use credit card numbers

Most credit card companies offer the ability to use one-use credit card numbers so if someone at an internet company steals your credit card number, that information is useless to that person.