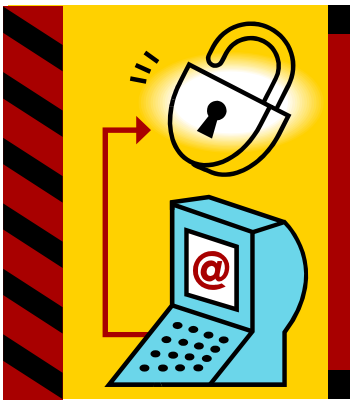


Consumer Choices: Computer Security Software

Prepared by:

Dave Palmer, Instructional Media Faculty, University of Florida/IFAS Extension, South Central Extension District

Laura Royer, Extension Faculty, University of Florida/IFAS Osceola County Extension Services

Situation

Use of the Internet has exploded during the last decade. Internet criminals see this increase as a never-ending opportunity. As a result the number of security threats detected has doubled every year since 2006. The number of websites seeking personal information to commit a crime has increased by 100% during the 1st half of 2009 alone. Over 100 billion e-mails are sent daily and experts say 90% of it is spam. Identity theft, an act where someone takes some piece of your personal information and uses it without your knowledge to commit fraud or theft has become rampant online. Losses to online scams are estimated to be between $one- to $two-billion per year.

Media stories often blame teenagers, stating that they are showing off their computer skills and causing the problem. Nothing could be further from the truth. Malware, which stands for **mal**icious soft**ware,** is created by organized, sophisticated and well-funded criminal gangs. Their goal is to make a lot of money quickly and they've found a variety of ways to reach that goal. They design malware to search your computer for usernames, passwords, bank account and credit card numbers, in addition to names and e-mail addresses. Other malware records everything you type and sends it back to the criminals. Some malware makes it possible for them to control your computer remotely. Then it can be used to send illegal spam, attack websites, businesses and even other countries. It may also be used to acquire, store and distribute child pornography. You'll never have a clue that it's happening until the police knock on your door.

UF UNIVERSITY of FLORIDA IFAS Extension

Despite law enforcement's best efforts, they are currently unable to protect people from malware. It's up to us to be educated, install appropriate safeguards on our computer, and change our online behavior to reduce the threat.

Main Types of Security Threats

Malware

The word malware is an abbreviation for **mal**icious soft**ware**. Malware includes viruses, spyware, Trojans and more. Malware is designed to slip into your computer unnoticed. Depending on the type of malware, it may spy, steal personal information, steal your identity, download even more malware, send your information to other computers, control your computer, and even send spam to others using your computer.

Spam

Spam is unwanted e-mail, usually sent to hundreds, or thousands of e-mail addresses. Spam is the primary way Internet criminals distribute malware.

Virus

A virus is a type of malware capable of reproducing itself, harming or deleting other files on one computer.

Spyware

Spyware is a type of malware designed to steal confidential information, like e-mail addresses, credit card details, user names, passwords, birthdates, social security number or any sensitive information. The information gathered is then sent to Internet criminals.

Trojan

A Trojan is a type of malware that appears to be a useful program but actually contains a payload that is something harmful, usually malware. Trojans hide in the computer system and are designed to activate when a specific action occurs, like inputting personal information at a website.

Phishing

Phishing is a process Internet criminals use to gain sensitive information such as usernames, passwords and credit card details. Phishing is usually done through e-mail. The writer of the email masquerades as a trusted organization such as a large well-known company, a bank or even part of the government, making it harder to detect it is a scam.

SMiShing scams are similar to phishing scams. You get a text message from a bank or service provider asking you to do something. SMiShing scams often direct you to visit a website or call a phone number. If you dial the number, you'll be asked for sensitive information like a credit card number. If you visit the website, it may attempt to infect your computer with malware.

Spear phishing is more targeted type of online scam. Unlike phishing, where a single, mass e-mail is sent to thousands of people, spear phishing attacks are more focused on one person at a time. A Spear phishing email typically includes personal information such as a name, employment, etc. and usually includes a link that leads to a spoofed, or fake, web site that requests personal information. The email and website may look so legitimate that the experts are fooled by spear phishing emails. In some cases, spear phishing emails may have an attached downloadable file. They're just as convincing and the file contains some type of malware.

Peer to Peer (P2P) File Sharing allows users to share files online by running the same software on a computer. People like to file share because it provides access to a lot of information,. However, P2P file sharing exposes the computer to many risks. Some risks include downloading copyright protected files, viruses or malware or material you didn't want to download. It could also lead to mistakenly allow other people access to files you do not want to share.

Social Networking Websites allow people to connect and exchange information about themselves with others. Information exchanged includes pictures, videos, blogs and private messaging to communicate with friends or others with common interests. It's important to be aware of the possible pitfalls that come with networking online because of the information shared and with whom it is shared.

Wireless internet offers convenient access and mobility. However, there are some security risks when using public "hot spots." Often the wireless (WiFi) connections open to the public are not secure and you should assume that other people can access any information you send or see when using it.

Ways to Protect Yourself and Your Computer

1. First, understand that there are no, 100% "safe" websites. Any legitimate website can be compromised.

2. Use strong passwords where money or sensitive information is involved. Computing power has greatly increased in recent years. Experts say that this increased power allows criminals to crack many short or simple passwords easily. They say anything less than a 12-character password that uses numbers and special characters can be easily broken.

3. Keep your laptop with you at all times when not at home. Treat it as you would your wallet or purse.

4. Update your operating system and your other software programs on a regular basis.

5. Use a layered approach to Internet security. No single tool can adequately protect against the wide range of threats that exist today. Also, no single security tool is perfect. The best defense is to use multiple tools or layers.

6. Know what information should be kept private such as full name, social security number, address, phone number, and birth date. Be sure to choose a screen name that doesn't reveal too much personal information. Realize that once information is posted to the Internet, it may be there permanently.

7. Install P2P file-sharing software carefully so you know how it works and what is being shared. Consider adjusting the file-sharing controls so it is not connected all the time.

8. Use privacy settings when using P2P software or Social Networking sites to block out exposure to specific information or files you do not want shared.

Security Software

New PCs usually contain a free trial version of a security suite from a company. After the trial period you are given the option to renew or you can shop for another security software company. It is critical that you maintain effective security software due to the various online threats and privacy issues previously discussed. Also, failure to protect your computer can shorten the machine's life and lead to the theft or corruption of data.

Prior to shopping for security protection options, it's important for you to know the terminology used.

IM protection - This feature will block attempts of malware through instant messages.

Anti-Spam - This filters and blocks unwelcome email. The anti-spam feature offers supplementary assistance if too many junk e-mail messages are still getting through.

Child filter – Will block access to certain sites unsuitable for children.

Privacy filter – Before sharing personal information without your knowledge, a privacy filter will provide a warning.

Browser toolbar - These toolbars are placed into popular browsers and help prevent phishing.

Anti-malware programs - Offers protection from malware or related security risks.

Firewall - Protect your computer from incoming and outgoing threats such as keeping malware from downloading or preventing a malicious Web site from grabbing data off your computer. It is best if the firewall pops up alerts when a potential breach is detected. Then you must decide if it's okay to let the data go through.

Spam filters - Filters out unwanted email messages. Though often built into pay suites, there are some free options available online such as SPAMfighter at spamfighter.com, which is recommended by Consumer Reports.

Anti-phishing toolbars - Security toolbars are available for all major browsers and they provide extra protection against phishing sites.

File shredders - Erase files to prevent their recovery from your hard drive. Simply deleting a file does not remove all electronic traces of it from your hard drive. This could allow someone who accesses or inherits your old computer to recover some or all of the file's data. Some pay suites include one, or you can download Eraser free from eraser.heidi.ie.

File backup - Periodically backs up your files to another drive to protect them.

Security suites – These offer an all-in-one package that combines levels of protection. There are many types of security suites available. The free security suites generally offer malware protection and a firewall. In some cases the free suites will offer other extras such as a filter to avoid certain websites. The free suites don't include other features such as anti-spam protection, built-in backup software and a browser toolbar that will alert you when you're visiting sites that host malware.

You generally have to pay for a security suite that includes those features. Such suites promise comprehensive protection in one package. They offer malware protection, a firewall, an anti-spam filter, and other extras. The latter usually include a child filter, often include a browser toolbar that will alert you when you're visiting sites that host malware, and sometimes include a file shredder and file backup software. The security software is usually downloadable online. The suite can used to protect up to three computers in the same household. Prices typically range from $40 to $80 a year.

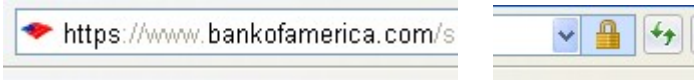
Browser Security

1. Watch web addresses (URLs) to know for sure where you are surfing. Don't assume a website is what it claims to be unless you've typed in the URL yourself. Even then you might be wrong.

2. Delete cookies, flash cookies, adware and spyware unless you have a good reason to keep them.

Stay Safe When Shopping Online

When shopping online, never enter passwords, credit card numbers or other sensitive information into a website that doesn't display **https:** or the padlock icon.



If possible make payments through a 3rd party like PayPal. Fewer vendors will have your credit card number. If you can't use a 3rd party for payment, use a credit card for online purchases rather than a debit card. Credit cards limit your liability, debit cards don't.

E-mail

1. Be very suspicious of e-mail attachments. Internet criminals often attach malware to e-mail.

2. Don’t allow your browser to remember your passwords.

3. Don’t assume that any e-mail is actually from the “From” address.
4. Delete obvious spam without opening it. Criminals can attach programming to an e-mail so they know when it’s opened. Opening spam will alert the criminals to send more spam.

5. Never click on links in e-mails. Type the URL into the browser yourself.

Security Software Shopping Tips

Free may be fine - If you surf safely, meaning you only download software from familiar sites or avoid clicking on e-mail links to access bank or other personal accounts, then the free anti-malware programs tested by Consumer Reports should adequately protect you. The two top picks were Avira AntiVir Personal 10 and Microsoft Security Essentials. Please note that these two programs do not include a firewall, but Windows 7's firewall was comparable to those in most suites. You can also add a firewall such as CheckPoint's free ZoneAlarm at *http://www.zonealarm.com/security/en-us/free-upgrade-security-suite-zonealarm-firewall.htm*.

Consider the type of computer
Vulnerability to security risk will vary based on your computer's operating system. In a survey conducted by Consumer Reports, Apple computers were less likely than PCs to have been attacked by viruses and spyware. However, Macs are able to transmit infected files to Windows PCs, including those connected to a Mac over a network in your home.

Be sure to check the security suite’s necessary operating demands. For example, computers with less than a gigabyte of memory might run too slowly causing some programs' scans to take longer than others.

Choose a pay suite mostly for convenience and features
Security suites are advantageous because it simplifies your security regimen. It takes one download and install and requires only a single upgrade to its database when necessary. Its single interface can also be easier to use than multiple stand-alone programs.

The extras you get with a suite include a built-in firewall, which can block attempts by malicious software to access data on your computer. Based on Consumer Reports testing, the firewalls in the best suites offered slightly better protection than the Windows operating systems in Vista and Windows 7 and much better than the firewall in Windows XP.

Generally with free products, support for the product help is limited to online FAQs, forums, and tutorials. Most of the tested pay suites offer free e-mail and chat support. Pay suites may offer phone support, though there could be a charge for it.

Final notes

1. Backup your data, or your whole system, regularly. There's a lot you can't defend against. A backup of your data or computer will make recovery much easier.

2. Turn your computer off when not in use. Broadband and an always-on connection can be a dangerous combination.

3. Nothing is foolproof. Good security practices such as these don't eliminate the risk, but they make you less of a target.

Comparing Advantages and Disadvantages of Security Software

Choose at least 3 security software products. Use the chart below to identify what you believe to be the advantages and disadvantages of each of the products. Be prepared to explain why you think each item is an advantage or disadvantage.

Security Software	Advantages	Disadvantages
#1		
#2		
#3		

1. Which security software do you think is the best one for you?

2. Why do you think this is the best security software for you?

Practice Situation - Computer Security Software

Linda's parents bought her a new laptop three months ago to be used for school, surfing the internet, social networking and downloading music, games and movies. The computer came with a three-month, free trial period, anti-virus software. Since her three months is up, she needs to shop for a security software suite that primarily protects against malware, anti-spam and anti-virus. She doesn't need a firewall because her computer does have the Windows 7 operating system which has a decent firewall. However, if the suite comes with a firewall she will use it. She would like stretch her dollars as the purchase is coming from her personal money. Help Linda find the best security software program that meet her security needs and is within her budget.

	Choice #1	Choice #2	Choice #3	Choice #4
	Check Point Zone Alarm Extreme Security 2010	**Symantec Norton Internet Security 2010**	**BitDefender Internet Security 2010**	**Panda Internet Security 2010**
Price	$80.00	$70.00	$50.00	$80.00
Net Threats	Fair	Very good	Fair	Fair
Anti-Malware Performance	Good	Very good	Very good	Fair
Anti-spam Performance	Good	Excellent	Very good	Very good
Firewall Performance	Good	Very good	Very good	Good
Scan Speed	Very good	Excellent	Very good	Excellent
Browser Toolbar	Yes	Yes	Yes	No
Child filter	Yes	Yes	Yes	Yes
Clear alerts (firewall)	No	Yes	No	Yes
File backup	Yes	No	No	Yes
File Shredder	No	No	No	No
IM Protection (anti-malware)	No	Yes	Yes	Yes
Focused Help (anti-malware)	No	Yes	No	No
Privacy filter	Yes	Yes	Yes	Yes
Renewal Fee	$60	$55	$50.00	$80.00

UF UNIVERSITY of FLORIDA IFAS Extension

Practice Situation
Computer Security Software Answers

Answers: 3-2-4-1 **Cuts: 2-3-5**

First Place #3: BitDefender Internet Security 2010 which meets all of Linda's primary criteria. Though is slightly rated less on anti-virus performance, it is still ranked as very good. Also, the price is the least of all four options. Since choice #2 and #3 were close in their ratings price won pushing Choice #3 to the first slot. Since she is using social networking websites, this suite also provides protection for IMs.

Second Place #2: Symantec Norton Internet Security 2010 was rated either very good or excellent on all of the criteria Linda is looking for in a security system. It was marked second because of the price being $20.00 more than choice #3,

Third Place #4: Panda Internet Security 2010 comes in third because it ranked lower in net threats and anti-malware performance than choice #2 and #3. Additionally, it ties with choice #1 as the most expensive. However it does rank higher than choice #4 on security concerns.

Fourth Place: #1 Check Point Zone Alarm Extreme Security 2010 is last because though it sustains rankings of good in the security concerns, it was the lowest ranked of all four choices. It also is an obvious rule out with price being $30 than the first place choice.