Tips for Avoiding Viruses and Malware

The term **malware** is used to describe "malicious software" -- software you do not want on your computer and which is capable of doing bad things. There are many terms used to describe different kinds of malware: viruses, trojans, keyloggers, spyware, worms, spambots, backdoors, rootkits, and more. For most of us, the jargon used to describe different kinds of malware is less important than understanding what malware can do, how it gets on your computer and how you can deal with it.

This handout covers some tips and tricks you can use to protect yourself from infection by malware. It focuses on Microsoft Windows, and is by no means complete. There are other threats we do not discuss in this handout (such as phishing) and other steps you can (and should!) take to protect yourself. That being said, our emphasis is on anti-malware techniques that are easy to implement and effective.

Before diving in, we should emphasize that although computer threats do exist and this handout covers some scary topics, responding to malware by living in fear is not sensible. Learning about the threats that exist is already an important step towards computing more safely. The more you know the better you will be able to weigh costs against benefits to decide what level of risk you feel comfortable taking on with your computer.

How Malware Infects Machines

Malware doesn't come from nowhere. How can it get on your machine? Here are some infection paths:

- An attacker or automated program might break into your computer via your Internet connection. Often this involves exploiting **software vulnerabilities** -- bugs that allow remote users access.
- Malware can be spread via e-mail -- especially infected e-mail attachments.
- Some websites contain malware that installs itself onto your computer while you are surfing the internet.
- Some malware is hidden inside other software you install, from the Internet or on physical media like CDs.
- Malware can be transmitted via infected USB keys or floppy disks. Your USB key might catch a virus from an infected computer at a friend's house or a public lab.
- Certain kinds of malware will first infect your computer, then go out to the Internet to attack other services you use like e-mail or social networking sites.

Many of the tips below involve cutting off some of these paths so that malware has fewer ways to get into your computer.

Use Limited Users for Daily Activities

If you use the Internet at home, one of the easiest things you should do is make sure that you and your family use so-called "limited accounts" for daily computer tasks.

In Windows, an **administrative account** is capable of installing software and changing anything about your computer's configuration, while a **limited account** is prohibited from installing software.

Using a limited account is of special benefit while surfing the Internet. Malware that is transmitted via your web browser will often try to install itself on your computer, which usually requires administrative access. If you use a limited account when surfing the web, it will be harder for that malware to install itself.

In Windows XP, you can see what account types you are using by going to `Start -> Control Panel -> User Accounts` If your account is already limited you will probably see only your own account name. Otherwise you will probably see all the user accounts on your computer.

It is best to create one account for administration. You can call it "Admin Account" and set a password for it. Then make all other user accounts on your computer limited. If somebody needs to install a program they can use the administrator account. Otherwise the limited account will be good enough to surf the web, do e-mail and run almost every Windows program.

Use a Hardware Router

Many types of malware try to infect your computer by attacking it remotely, using your Internet connection. A **hardware router** can help protect against such attacks.

A hardware router is a device that sits between your ADSL or cable modem (which was probably given to you by your Internet provider) and your computer. Companies that manufacture these routers include Linksys, D-Link and Netgear. Sometimes they provide wireless access throughout your home.

The job of a hardware router is to share your Internet connection to multiple computers in your home. In doing so, almost all hardware routers implement a **firewall**, which is intended to keep the outside Internet from unintended access to your computer. It is this firewall that helps protect the computers in your home.

You may have heard the term "firewall" before -- there are software programs called firewalls, and Windows itself comes with a firewall program. Furthermore, hardware firewalls will cost you money. But unless you know what you are doing, using a separate hardware firewall is the easiest, most effective way to keep remote attackers from getting through your internet connection.

These days some internet providers (like Sympatico) integrate hardware routers into their ADSL modems. This is a good (and long overdue) solution. Having said that, in most cases you won't hurt anything by having an additional firewall between your internet connection and your computers.

You usually configure hardware routers via a web interface. This is not difficult, but you may want to ask a computer-savvy friend to help you do this. You will want to make sure to do the following:

- Change the default password on the router to something strong
- Disable remote configuration of the router from the Internet (if this is not done already)
- If your router is wireless, either disable the wireless (if you don't need it) or use strong encryption (WPA or preferably WPA2) for wireless connections
- Make sure the router is upgraded to the latest **firmware** (which will either be available for download from the router interface or from the manufacturer's website).

Keep Software Up to Date

Virtually all computer programs have flaws (or "bugs"). Some of these bugs are merely aggravating. Others are **exploits** -- mechanisms that malware and attackers can use to gain control of your computer. Malware that uses freshly-discovered exploits can appear quickly on the Internet. Meanwhile, software manufacturers

release **updates** (also called **patches**) to their software that attempt to fix the exploits.

Because malware that uses new exploits gets developed so quickly, it is important to make sure your software (especially Windows and your web browsers) have the latest updates installed. Some software (such as Mozilla Firefox) will notify you when updates are available. Other updates (such as Windows updates) are released on a regular basis.

Although older versions of software can remain useful, using very old versions of operating systems (such as Windows 98) on the Internet is ill-advised. Either you should keep such computers off the Internet or you should upgrade your operating system.

Updates and Pirated Software

Pirated software is software that is installed without the consent of the software manufacturer. In order to dissuade people from pirating their software, Microsoft has developed the "Windows Genuine Advantage" system. If this software (which appears as an update) is installed, your computer connects with Microsoft's servers, and Microsoft's servers check whether you have a valid **licence key** for your software.

Installing the software check is optional, but if you refrain then you will not receive other updates from Microsoft's servers -- including security updates. This leaves your computer vulnerable to malware. For this reason alone it is inadvisable to use software illegally.

If you have a pirated copy of Windows, you have three options. You can assume the risk of being infected with malware, which will limit your ability to bring your computer to a shop to have it repaired. You can purchase a legal copy of Windows and use that software key to make your software legitimate. Or you can explore alternatives such as **open source software**, which you can legally download and use without registration. Often open source operating systems provide security updates automatically and for free, which sidesteps the piracy issue entirely.

Be Cautious About Attachments and Strange Software

Strange e-mail attachments are a common source of malware. If you get attachments that you are not expecting (for example, unexpected photos or screensavers) then you are best off deleting the attachment without opening it. You should do this even if you know the sender -- that sender may have been infected with an e-mail virus that sent mail to all of his or her contacts. If you think the attachment might be legitimate, you can contact the sender and ask.

Another source of malware takes the form of strange software downloads -- especially of pirated software, which is often packed with viruses. This can be a particular problem if others who use your computer (such as your children) are continually installing strange new programs. This is tricky business, however, because there is a lot of legitimate, malware-free software that you can download and install. It helps to develop a sense of trust about download sites that are safe versus those that are not. Danger signs include the mysterious appearance of software that ordinarily costs hundreds of dollars (like Adobe Photoshop) and software that goes by the term **warez**.

Again, open-source software can help here. Although some malware now advertises itself as "open source", software collected into **distributions** like the OpenDisc or OpenEducationDisc http://www.theopendisc.com/education are generally safe.

Before installing a new software program, it can be helpful to research it online. Look for reviews, download sites and discussion of the product. How much does the software cost? Does it have a good reputation? Do people report getting viruses or other malware from the product?

Consider Alternative Software

Many malware programs target programs that are in the widest use. This is one reason so much malware targets Microsoft Windows and Internet Explorer. One strategy for avoiding malware is to look at well-regarded alternative software for your daily work. For example, you might consider an alternative web browser such as **Mozilla Firefox**, **Google Chrome or Opera** to Internet Explorer. You might even consider switching operating systems.

For many years, people used to strongly recommend switching away from Internet Explorer to alternative browsers because Internet Explorer had a rash of security problems. In recent years Microsoft has put in a lot of effort into securing their web browser, so this may be less of a concern than it was in the past.

In general, switching software just because it is different and more obscure does not work well as a security strategy. If written poorly, obscure software can be more vulnerable to malware. When considering alternatives, the following questions can be helpful:

- Is the software regularly updated for security issues?
- Do the software developers take security issues seriously (as opposed to brushing them off)?
- Is there a sizable group of people who use the software and report problems?
- Does the software work well? Does it do the bulk of what you need?

Choose a Variety of Strong Passwords

One common technique malware (and human attackers) use is to try logging into your computer and online accounts with well-known passwords. Examples of guessable passwords include dictionary words ("password"), dictionary words with numbers added to the end ("zinc32"), or words where numbers are substituted for letters ("v1n3gar").

The following pages have some tips on choosing stronger passwords:

- http://www.microsoft.com/protect/yourself/password/create.mspx: A fairly thorough site
- http://www.cs.cmu.edu/~help/security/choosing_passwords.html: Has a few quick tips and password generation methods
- http://frpeter.blogspot.com/2009/06/how-to-choose-very-strong-passwords.html: Another interesting method

Another trap many of us fall into is using the same password in many places. If an attacker or piece of malware can get into your computer account with a certain password, it can then try the same password for your e-mail account, your banking account, your social networking sites, and other valuable places. Varying your passwords and keeping them secure helps here.

One final warning concerns web browsers. Many web browsers offer to remember your passwords for you, which means that an automated program (or human attacker) can automatically log into websites if they get access to that web browser. Having your web browser remember passwords is convenient, but it is a questionable security practice.

Keep Backups

We all know that we should back up our data regularly in case computer hardware (such as our hard drive) goes bad. However, backing up your data is also important for malware reasons. If your computer gets infected with malware, you have a (hopefully clean!) backup of your data that you can use. This also comes in handy if you take your infected computer to a repair shop and they wipe out your hard drive.

The best backups are those that you don't have to remember scheduling. This is a big topic, but some ideas include:

- Backing up data over the Internet
- Backing up data to USB keys or external hard drives (which you have to remember to insert periodically)
- Backing up data to a second hard drive on your machine

Backups by themselves will not help you avoid getting infected by malware, but they can help you recover if your computer does get infected.

Investigate Antivirus and Anti-malware Options

There are many antivirus and anti-malware options on the market. Usually they require annual subscription fees.

Antivirus programs can be useful in conjunction with other techniques such as using hardware firewalls, but they are not sufficient protection on their own. Antivirus programs do not catch all viruses, and a lot of malware attempts to disable antivirus programs so that it will not be caught and cleaned off.

If your budget is tight there are some antivirus and antimalware programs available legally for free. None of the antivirus programs below are great, but they all offer some protection:

Windows Defender is an antimalware program that is available from Microsoft. In order to use it you need to have a genuine copy of Windows.

Avira http://www.avira.com and **Avast** http://www.avast.com are two antivirus manufacturers that offer free and legal versions of their products. Getting these programs can be tricky -- they both try to "upsell" you to paid versions of their product, so you have to pay attention in order to download the free versions. Some will also try to install toolbars (like the Yahoo! toolbar) that you probably don't want.

ClamWin is http://www.clamwin.com an open-source virus scanner that is free to download and use. Updates are also free. The big disadvantage to ClamWin is that it is not capable of **online scanning**, so it will not protect you as soon as you visit a website containing malware. It can be an option if you schedule daily virus scans.

SUPERAntiSpyware http://www.superantispyware.com and **Malwarebytes** http://malwarebytes.org are anti-malware programs. They both have versions that are free and legal for private use.

There are some anti-malware products that once were highly regarded, but which no longer offer good protection. Examples include **Ad-Aware** and **Spybot Search and Destroy**.

Use Virtualized Installs

Virtualization is a trendy technology that involves using a software program that **emulates** another computer. This means that you can run Microsoft Windows inside Linux, for example.

Virtualization is interesting because it provides easy and efficient access to **snapshots** which store the state of your computer at a particular point. You can take a snapshot of your Windows installation as soon as you have installed it, and after installing important updates or new programs. If your computer gets infected with malware, you can then "roll back" the snapshot to a previous version that is clean.

This technique requires quite a bit of technical knowledge to implement, but if done correctly it can offer some interesting advantages in recovering from malware attacks. If you are interested in this approach you might look into the open source **VirtualBox** program.

Scare Stories: How Malware Can Be Harmful

Given that all of the steps above take effort and sometimes money to implement, why should you bother? The sad truth is that malware does exist, and it can infect your computer astonishingly quickly if you do not take precautions. At the very least malware can cause you time and aggravation when it slows down your computer to a crawl and you have to pay somebody to clean it off. But there can be more serious consequences as well:

- Some forms of malware infect your computer and then connect to the Internet to infect more computers or send spam. A single infected computer can attack tens of thousands of other computers per day. Because of this, your internet service provider will cut off (or threaten to cut off) your internet service if it suspects you have been infected by one of these spambots.
- Some infected computers become "zombies" -- they are taken over by a central controller which uses them to attack websites or break banking passwords. This is actually big business in the organized crime world.
- Sometimes, your infected computer can be used as "storehouses" for files such as pirated software and movies. Others then connect to your computer to download these files, which can run up your Internet usage bill and result in overuse fees.
- Some forms of malware record your keystrokes and send them to a remote location. They do this in the hopes of capturing valuable information such as banking passwords and credit card numbers. The attackers can then use that information to impersonate you or empty your bank account.
- Some malware infects your documents and data, so that if you send those documents to others then your recipients will get infected as well.
- There are a few malware programs that corrupt or destroy data on your computer. For example, there are a few viruses that will delete spreadsheet and document files on your computer.

Malware can also install itself onto your computer incredibly quickly. In one case, a poor unfortunate soul (who shall not be named on account of being the author of this document) installed Windows onto a computer in an environment not protected with a hardware router. Because the copy of Windows on the CD did not have updated applied to it, the machine was highly vulnerable to attack, and it was infected by a virus within minutes. That computer then tried to infect thousands of other computers, which led to quite a lot of trouble and embarrassment.