The Virus, Spyware, Adware, and Spam Survival Guide

prepared by Mike Powell of Technology**Masters** (updated 3/14/10)

What are they?

Virus – a **computer program** written by a person to **intentionally** cause malicious mischief or harm to your computer and that is installed on your computer ***without** your permission*..

Worm - A self-replicating virus designed to propagate across many systems and/or networks without any user interaction. You can become infected just by being connected to the internet or by accessing an infected website. Worms can lay dormant and explode their payload of code at a predetermined day and time and use your computer as a new base of operation to scan for other unprotected computers on the internet. They can worm their way through and set up another base on those computers to then infect them. This affect multiplies exponentially at near the speed of light – also known as a Zero Day Virus.

Adware - a **computer program** written by a person to present you with pop-up ads. It is installed **with** your permission by piggy-backing on another piece of software such as a free game, free screensavers, etc.

Spyware - is generally adware that, in many instances, tracks where you go on the internet and reports back to a central computer in order to target the ads in response to the sites your browse to. One symptom of some spyware is to visit one website and "poof" you are automatically taken to a sponsor's website (a recent well-known instance of spyware occurred when visitors to L.L.Bean's website were automatically redirected to JCPenney's website. L.L.Bean sued JCPenney). Spyware can also contains key loggers that can watch what you type. And when you enter 16 numbers it takes a snapshot of 100 characters in front and 100 characters behind and sends it all to a server in another country (Russia and other eastern block countries are well known.) It has become a business model for organized crime. Last year alone, more than 9.9 million Americans were victims of identity theft, a crime that cost them roughly $5 billion. Your credit card number used to be worth $60. Now, because this has been so successful, each card can be purchased on the internet for between $1 and $6. Organized crime has also become involved in spreading viruses and spyware to mine the data on your computer.

What can they do?

Affect your computer and those of others

- Extract excerpts from documents on your PC and e-mail them to people in your address book which slows your computer, the e-mail system and the internet down.
- Cause your computer to e-mail viruses to infect millions of other people's unprotected PCs which slows your computer, the e-mail system and the internet down.
- Cause your computer to send out spam to millions of other's on the internet which slows your computer, the e-mail system and the internet down.
- Cause your computer, as one of many, to send so many requests to a website server that no one else can view the website. Since the website server cannot handle your request your computer slows, or you get the response "page not found."
- Clog and slow down the entire e-mail system
- Reduce your productivity and that of your fellow employees

Affect your computer directly

- Give someone unbridled access to your computer without your knowledge
- Send your confidential financial information to a foreign country and steal your money and/or identity
- Cause your ISP to cancel your service because your computer is sending mass viruses, spam, or requests on behalf of the virus/spyware writer
- Delete all the data on your computer
- Scramble the data on your hard drive
- Cause annoyances such as over-riding your browser's default web page to change it to their sponsor's web page. Every time you try to change it back to what you want, it changes back to what it wants.
- Display pop up ads
- Slow down your computer

- Cause a situation where there is no other solution but to start over from scratch by backing up and re-installing Windows.
- The list goes on...

How can you prevent it?

Start with the Big Three
(Updated anti-virus software, a firewall, and allowing automatic Windows Updates.)

Ensure anti-virus software is installed and updated. If you don't know how to tell if you're up-to-date, then you are probably not. Anti-virus software that is not updated daily is not much more effective than not using any at all. You should only have one anti-virus program installed otherwise they may conflict with each other.
For Businesses: employees should understand that only the system administrator should install programs. Otherwise, a software conflict can occur, create problems that can affect everyone on the network, and create licensing issues.

Ensure you are behind a firewall. Without a firewall, you can be infected within 12 minutes of connecting your computer to the Internet[1]. If you use a router, then you have a hardware firewall that protects you against inbound hacker attacks and against some virus worms. If you have Windows XP with Service Pack 2, then you have a software firewall that will protect you if another computer on your network downloads a virus.
For Businesses: employees should understand that only the system administrator should install programs. Otherwise, a software conflict can occur, create problems that can affect everyone on the network, and create licensing issues.

Ensure all Windows Critical Updates are installed
If you have Window XP, ensure auto update is turned on. If you are using Windows 2000 or earlier go to the Windows Update website regularly to check for the most recent updates. Updates fix the code in Windows that virus writers take advantage of.

Install a free Adware / Spyware detector/removal tool
For Adware/Spyware removal software go to www.download.com
Search for, download, and update
Spybot Search and Destroy
For Businesses: employees should understand that only the system administrator should install programs. Otherwise, a software conflict can occur, create problems that can affect everyone on the network, and create licensing issues.

Use Mozilla Firefox instead of Internet Explorer (IE)
www.getfirefox.com
IE uses ActiveX technology. Firefox does not. ActiveX makes computers susceptible to viruses just by visiting an infected web site. ActiveX also allows spyware to be loaded easier. Do not uninstall IE. Windows depends on it. And, you may need IE to view certain websites that take advantage of ActiveX features. For all the other internet browsing you do, use Firefox.

Change your behavior (cannot be emphasized enough!)
Ensure employees understand that the computers they use in the office are for business approved purposes only. Employees need to know that installing any software can cause a conflict (like an allergic reaction) and cause minor to major problems including crashing Windows. If Windows needs to be restored it will cost $200 and up. Changing settings can also be an issue. The less a business computer is changed, the less that will go wrong.

Don't open files attached to e-mail – especially from someone you know. Why? Because you are on their e-mail address list which is how the virus sent itself to you. Ask yourself, is opening that attachment worth getting a virus?

Don't send or open links for greeting cards – it's not worth it.

Don't buy ***anything*** from an unsolicited e-mail (spam) or a pop-up ad. If you do, then you are actively promoting spam, pop-up ads, spyware, and viruses. We get spam because the spammers make money from people buying products advertised in spam.

Pictures can contain viruses. Just by viewing a picture the virus can install itself.

Stay out of the bad side of town. (Casinos, porn, free games, free fonts, free wallpaper, free screensavers, free themes, and other free software.) They are the candy from strangers your mother told you not to take

Only download free or trial software from software libraries like Download.com who guarantee through testing that their software downloads are free from adware, viruses, and spyware.
For Businesses: employees should understand that only the system administrator should install programs. Otherwise, a software conflict can occur, create problems that can affect everyone on the network, and create licensing issues.

If Windows, your software firewall, or a pop-up asks permission to install software that you're not sure about, don't grant permission. Do not click on any buttons like Yes or No, or OK or Cancel. Clicking no or cancel means yes. In the upper right-hand corner of the window, only click on the red button with the white X.

If you receive a pop-up telling you that you have spyware and that you should install their spyware – don't. Their solution will probably uninstall all other spyware and install its own. AOL bought a company that did this and was required to pay millions in fines.

Don't use Facebook, My Space or other Social Networking sites

For those of you who use facebook, it's necessary for everyone to know the information below . I'm not making any judgment. My intent is to provide you with information and you decide. Some people don't care. But, remember, once the toothpaste is out of the tube, you can't put it back.

Summary

1. Your private information may no longer be private.
2. All information marked as private, is still easy to obtain.
3. facebook Applications such as quizzes and survey's not only give the application provider private information about you, but they also receive your friend's private information – without their permission.
4. Scams that lock you out of your account by changing the password then the hacker sends an e-mail plea to all your friends that appears to be from you asking for money from your friends – and you can't do anything about it.
5. facebook, My Space, and chat rooms are havens for sexual predators
6. Nasty viruses are spread over facebook and My space
7. E-mail phishing attacks

Expanded Information

1. Your private information may no longer be private due to a recent change in facebook's terms and conditions. One of the reasons so many people migrated from My Space to facebook was that their information on My Space disclosed to others more openly. facebook was supposed to be more private and gave users more control over their privacy. I found this changed recently.

If you are one of the many users who **have never set their privacy settings**, facebook made a change where user's information is no longer private, it is now open to everyone. By being open to everyone, one consequence is that all user's facebook information will be scanned and indexed by search engines such as Google and therefore searchable by anyone on the internet – even those without facebook accounts. Yes, information and pictures you thought were private are now publicly available worldwide.
http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html
http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php

2. All information marked as private, is still easy to obtain by anyone who wants to put forth a little effort. These are hacks for anyone in the world to use to access private data on facebook.
How to sniff out private information on Facebook
http://www.theregister.co.uk/2007/06/26/sniffing_private_facebook_info/
Is Privacy An Illusion? Facebook 'Fans' Claim Hack Exposes Private Profile Information (Update)
http://www.techcrunch.com/2009/06/22/is-privacy-an-illusion-facebook-fans-claim-hack-exposes-private-profile-information/

3. facebook Applications such as quizzes and survey's not only give the application provider private information about you, but they also receive your friend's private information – without their permission.
Are Facebook applications safe?
http://www.themiamihurricane.com/2008/10/15/are-facebook-applications-safe
Exclusive: The next Facebook privacy scandal
http://news.cnet.com/8301-13739_3-9854409-46.html
Warning: Your Facebook Photos Still Aren't Safe
http://www.allfacebook.com/2009/02/facebook-photos-warning/

In addition to now sharing what you thought was your private, facebook and My Space are known for the following issues

4. Scams like this one that locks you out of your account by changing the password then the hacker sends an e-mail plea to all your friends that appears to be from you asking for money from your friends – and you can't do anything about it.
Facebook Scam Targets Parker Woman's Friends
http://www.thedenverchannel.com/news/20352912/detail.html
Hackers take aim at Facebook users http://www.eagletribune.com/punews/local_story_011042538.html

5. facebook, My Space, and chat rooms are havens for sexual predators
Wake Up Call: Facebook Isn't A Safe Haven
http://www.techcrunch.com/2009/02/08/wake-up-call-facebook-isnt-a-safe-haven
facebook and My Space are where Dateline NBC "To Catch a Predator" series finds many of the predators lured to the houses where Dateline can interview the predators.
http://en.wikipedia.org/wiki/To_Catch_a_Predator

6. Nasty viruses are spread over facebook and My space
Facebook, MySpace Hit By Koobface Worm
http://www.huliq.com/1/78015/facebook-myspace-hit-koobface-worm
In addition to the Koobface work, there's the Storm worm, Fan Check virus and many others that can steal your identity and gain access to your bank accounts.

7. E-mail phishing attacks
http://news.cnet.com/8301-27080_3-10396786-245.html
A legitimate-looking Facebook e-mail asks people to provide information to help the social network update its log-in system. Clicking the "update" button in the e-mail takes users to a fake Facebook log-in screen where the user name is filled in and visitors are prompted to provide their password. When the password is typed in, people end up on a page that offers an "Update Tool," but which is actually the Zeus bank Trojan.
More on the Zeus bank Trojan
http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1367410,00.html

Here are some tips, if you continue to use facebook, that you should know.
Cyber Security Is a Shared Responsibility
http://blog.facebook.com/blog.php?post=168259887130

How to Avoid Being Spammed

Protect your primary e-mail address. Never use your primary or business e-mail address to sign up or order anything on the Internet – anything – ever! Limit the use of your business or main personal e-mail to friends, co-workers, and customers. This can potentially delay your getting spam for a long while. Protect it like an unlisted phone number.

Get a free e-mail account. from Yahoo, MSN's Hotmail, or Google's Gmail. Whenever you sign up for or buy anything give them your free account e-mail address [emphasis added]. These free services are getting much better at filtering out the unwanted spam.

Do not publish your e-mail address on the internet. Never have your business e-mail address listed on any web site. Spammers use computers to search web pages that have an @ sign – a solid clue it's an e-mail address. Use an uncommon, generic addresses such as get_info@ etc. These can also be easily and immediately changed to prevent spamming. Do no use common addresses such as info@, webmaster@, sales@, etc. These common addresses are automatically spammed.

Delete spam immediatly. Do not respond to spam. Do not read spam. Delete spam. Out of the many millions of spam sent every day, if spammers can get even under a 1% return of someone responding to spam, they've had a good day. If all users would ignore spam, the spammers would be out of business.

Do not 'reply' or ask to be 'removed' from their list. This just confirms that your e-mail address is a good one that can be sold on the internet.

Do not use the Preview Pane in Outlook XP (2002) or before. Use AutoPreview to preview your mail instead of the Preview Pane. In Outlook click on View in the menu bar and then click on **AutoPreview** to activate. Click on View again and click on **Preview Pane** to deactivate.
If you are using Outlook 2003 and 2007, the Preview Pane is immune until you right-click on a picture and download pictures. So, do not download pictures on spam.

The following paragraph applies only to owners of a web site address (domain name).
Prevent spammers from finding your e-mail address in Whois.net. – If you have a domain name (web site address: e.g. www.yourbusiness.com) Whois.net is a directory of web site contact info. Go to www.whois.net and type your domain name and click on Go to find the e-mail address, street address, and phone number. Your domain name registrar can protect your e-mail address by adding Privacy Protection which is the same as having an unlisted number.

Links to other sites
For Anti-virus software go to:
Go to www.download.com
Search for AVG Free
Download and install (on your home computer only)

For more information on viruses, go to:
Microsoft.com / Security At Home
http://www.microsoft.com/athome/security/viruses/default.mspx

For more information on identity theft, go to:
US Postal Service Identity Theft Tips (Enter into Google and click I'm Feeling Lucky)
or go to http://www.usps.com/postalinspectors/idthft_ncpw.htm

ID theft: It's only a matter of time, CNN Money.com
http://money.cnn.com/2005/07/18/pf/security_idtheft_0508/