Take Back Control of your PC

Andrew Pollack, Northern Collaborative Technologies
December 5, 2005

In the last few weeks, I've had to help several people clean up their personal computers because they starting having problem. In every case, the problem was caused by "Malware" of one kind or another. I thought I'd take an hour or so and write this document to give you some clues on how to avoid this hassle. This document also contains links to sites with free, reputable, reliable software to help you make your pc safe.

Author's Note: ***This document reflects products and product versions that change frequently. All of the information in this document is accurate to the best of my knowledge on they day I am writing it, however it may have changed since then. Please use caution when following this advice. Always make a backup of important information before trying new things.***

Aside from the hassle, malware is very dangerous to you. More than just making your PC stop working, it can cost you a fortune.

According to Dell Corporation, most of the support calls they get where users are having trouble end up being related to malware. This is actually good news. Most of the problems happen because the malware is badly written. If it were written by real professionals and didn't wreck your PC, you'd be in much worse shape because you'd never know it was there.

A brand new machine, if connected to the internet directly out of the box without a firewall or anything else, is likely to be infected with at least one worm within only 20 minutes – less time than it takes to run the update program to get the machine's protection up to date. The very newest machines are somewhat better, but not perfect.

What is "Malware"? Malware is a computer program of one kind or another which is designed to do something on your computer that you don't know about and wouldn't want done if you did know. Everyone pretty much knows about computer viruses. Viruses are one kind of "Malware" – but not the only one, and not the most common one any more. It's O.K. to think of all "Malware" as viruses if you want because for all intents and purposes it amounts to the same headache for you, but you should be aware that it's not really accurate.

Kinds of Malware:

Viruses & Worms – To be considered a "virus", the program has to be totally automatic. Without you doing a thing, it has to be able to "infect" your computer and then make copies of itself and spread to other computers. A worm is a kind of virus. The difference used to be more important than it is now. Before we were all connected to the internet, viruses spread through shared disks. Worms take advantage of the connection between an infected computer and the rest of the world to spread much faster. Almost all viruses now are worms.

Trojan Horses – Just like the story, these require you to do something to allow them inside the protection of your computer, but once you do they can do whatever they want. Trojans are how most otherwise protected computers end up with malware installed. The user (you) runs a program that claims to do something useful or fun. It probably does do what it says it does. It also does other things that you don't want in the background without telling you.

Spyware – Spyware is usually installed through Trojan horses. Its job is to silently run on your machine and report everything you do to a central site. It will then either capture your password and credit card data, or show you pop-up ads. It also does things to your computer to make it very hard to remove. This is usually what causes your PC to have problems later.

Why do these people want to put Malware on your machine?

There are two categories of reasons why these people want to put software on your machine. The juvenile types who used to be more common just did it to make a name for themselves in their little communities. Most of the garbage they wrote causes problems by accident. Most of what it is designed to do is nothing more than spread to more machines with no real purpose. The other type, the more sophisticated type, is making serious money through this stuff. They make money one of three ways.

The most common way they make money is to show you pop-up advertisements while you're using the web. These ads are made to look like they're on the page you're viewing, but they're not. For example, one of the companies which used this technique was called "Gator" (they're now changed their name to Claria and claim to be cleaning up their act). The company sold advertising to companies based on the number of times people clicked on the ads. The company also made software designed to show the ads and paid any developer who included that software with their own so that it was automatically installed. Someone could write software and give it away, but still make money because it also included (unknown to you) Claria's hidden software which let the developer get paid every time someone saw or clicked on an ad. LL Bean discovered that when some people went to their web site they were being shown ads for JC Penny. It turned out that JC Penny had (allegedly) paid Claria to show these ads specifically on the LL Bean website. Interestingly, LL Bean sued both Claria and JC Penny. It made the press because its one of the first times the company buying the advertising was to be held responsible for where and how it was shown. (See http://www.clickz.com/news/article.php/3355321 for more information.)

More commonly, less reputable advertising vendors pop up ads for the same kinds of offensive things you see as unwanted email.

There are even scarier reasons they want to put software on your computer. The right kind of software can turn your computer with its processing power and its high speed internet connection into a weapon they can point at a company. By itself, your PC is harmless, but in groups of thousands, these "drone" machines can be used to force an important web site off line by simply overwhelming it with requests it can't possibly respond to. Groups of hackers who control these kinds of drone armies commonly extort online retailers, demanding huge sums of money in return for not disrupting their business during people retail seasons. Remember, they're harder to track down than you think. Frequently they are based in Eastern Europe or Africa. **Yes, this really happens.**

The other big threat to watch out for is this same software can be written to track every web page you visit, every form you fill out, and every key you type. This can give them access to your bank account information, credit cards, passwords, and other confidential information.

How does your machine get infected with this stuff?

To put their software on your machine, hackers exploit two kinds of weakness; the weaknesses of your machine itself, and the gullibility of the operator. I'll talk about operator weakness first since people know the least about this. A huge number of worms and viruses are sent by email using a process known as "Human Engineering". That means, literally, manipulating you. You see this all the time in your email folder spam. A common trick is to send you a file from someplace claiming it is mail you sent out that can't be "processed". To see your original mail message you're supposed to click on the attachment. Guess what? The attachment is the program they want you to run. It contains software designed to take advantages of weakness in your computer software, but it needs your permission to start running. By clicking on it, you've given it that permission. You've been manipulated into giving control of your computer to software written by someone you don't know. Another common "Human Engineering" trick is called "Phishing" (the "ph" is hackers being clever, though very few have any idea that this comes from the old days when hacking was about getting telephone calling card numbers through repeated random dialers. In those days, it was called "Phone Phreaking" and the resulting codes were called "Phreak Codes").

Phishing is the technique of tricking you into putting your bank, email, eBay, or other online passwords and private information into a web site that LOOKS like the right place but really isn't. eBay and PayPal are the most common of these I've seen. In one case, someone registered a site called www,paypa1,com (I used commas instead of dots so it won't work if you click on it). If you look really closely, you'll see that the last letter in the fake paypa1 is a one, not an L. Most computer email fonts show the L and the 1 the same way. The email is created to look like an official email, but the link is disguised and really goes to a mock-up site designed solely to capture your name and password so they can then quickly go and log on as you, and empty your bank account. There are many other ways to disguise a web site address. Some may link to somewhere entirely different from what is listed as the address you're clicking on in the same way someone can say click "here" and have that work link to some long address.

The key goal of "Human Engineering" is to make you click on a button or run a program that gives their software permission to run with more control over your PC than it should have. Web pages do this a bit differently. Your web

browser is designed to allow websites to add software with your permission, to do cool things like play video or whatever. These controls run in what's called a "sandbox" where they have permission only to do things on that one page. To get outside this sandbox and install permanently or to do things on your computer outside that web page, the software had to ask your permission. One common way to doing that is to pop up a browser window designed to LOOK like an operating system menu with an "OK" button on it. I've seen some that say "Click OK to close this window" for example. What you don't know is that by clicking "OK" you've given something permission to run on your machine.

By the way, one of the most common "Human Engineering" tricks is to offer you software which claims to remove Spyware, but which is Spyware. You have to love these guys. Well, no you don't.

How do you avoid getting Malware on your computer?

1. Keep your computer software up to date. Use the Windows Update service to automatically download and installed "Critical" updates and check it periodically for the "recommended" ones. This includes your web browser. 90% of web browser and operating system updates come out because someone figured out a way to get past the security in the last version. By the time the updates come out, some sites are often already taking advantage of the flaw in your software.

2. Don't install software if you aren't sure about where it comes from, who made it, and that it doesn't have Spyware built in. Music and file sharing software like Kazaa was famous for installing Spyware. So was "Weatherbug" and "Comet Cursors".

3. Don't fall for fake emails that want you to click on things like file attachments or claim to need updated account information. They are meant to look like they come from somewhere legitimate. They almost never do. Some look like error reports, some look like security "warnings" from real places. Ignore them.

4. If you think an email may be legitimate, but you're not 100% sure, open your browser and manually type in the address listed on the email – don't copy and paste, and don't click on it. Pay close attention to a misspelled link name or something close to but not exactly where you think you're going.

5. Run antivirus software. Frankly, I don't like any of them but you need one anyway. Grisoft makes a fairly simple one that's pretty good, and they have a free version for home use. Of course they want you to buy the more full features versions, but the free one is good enough for most home users.
   http://www.grisoft.com/doc/289/lng/us/tpl/tpl01

6. Run firewall software or hardware. If you have a "router" between your PC and cable modem like one of the ones from Linksys, Dlink, Belkin, Dbridge, etc., you're doing well for this part. You may still want a software firewall because they add value as well. If your PC is connected directly to a cable, DSL, or dialup connection -- or if you use a laptop and connect at wireless 'hotspots' like Starbucks (and soon McDonalds) – you need personal firewall software running on your machine. Windows XP, if it's properly updated, includes a personal firewall and will bug you to turn it on and keep it on. This 'adequate' but hardly great. The Norton firewall isn't bad, but can be expensive. ISS makes a product called "Black Ice" that is well respected, Zone Labs makes a product called "ZoneAlarm", and Grisoft (see the link for their Antivirus software above) makes one as well. All three vendors have free evaluation versions, and some may even have free for home use versions. I'm currently testing the one from ISS called "Black Ice". http://www.digitalriver.com/dr/v2/ec_dynamic.main?SP=1&PN=10&sid=26412

7. Run anti-Spyware software. The two biggest competitors in this space right now are "Ad-Aware" by Lavasoft, which has an excellent reputation, and strangely enough Microsoft Antispyware. If you have a Spyware problem, you may need both to get rid of it. Each one is better and some things and worse at others. Microsoft's product is something they bought from a company called "Giant" and it's pretty good. It's in "Beta" right now and free. They're working on a full software suite of "protection" products so I don't know how long theirs will continue to be free. I'm using it and it works pretty well.
   http://www.microsoft.com/athome/security/spyware/software/default.mspx
   http://www.lavasoft.com/software/adaware/

8. Consider using alternative programs for your web browser and email client. The truth is that both Outlook Express and Internet Explorer are constantly being hacked. There are excellent alternatives to these programs. Instead of Internet Explorer, try using Firefox. Its free, and its better. If you already use Firefox, they just released version 1.5 last week. Go get it and install it. It will automatically keep itself updated with security patches. Just as Firefox replaces Internet Explorer, Thunderbird can be used instead of Outlook Express. It's also a much better program. Thunderbird will automatically keep your settings from Outlook Express so it's easy to install. Firefox does the same for your bookmarks and cookies in Internet Explorer. Try them. They're free, and they're good. http://www.mozilla.com/firefox/ http://www.mozilla.com/thunderbird/

How can I remove Malware once it's installed?

Removing Spyware and other such things can be VERY hard – even for professional computer techs. The first thing to do is try both the Lavasoft and the Microsoft product to see if your particular infection can be removed by one or the other. They each work differently. READ the help screens they give you. MOST Spyware can be removed by these tools. If you have some that can't, you'll need to find a professional who knows what he's doing to help. Note that you need someone who is not just a professional, but actually knows what they're doing. Many say they do but don't. Be careful – they're worse than car shops.

Do not believe you need to BUY anything to get rid of Spyware. The software I've linked to above will do the job. If you aren't having success, you may have to pay someone who knows more, but you do NOT have to replace your computer and you do NOT have to buy expensive software. If anyone tells you that your machine is "junk" as a result of something you typed in or installed as software, they're full of it. It may be and old machine, but it will still do what it did when you bought it. At the very worst, it might have to be re-installed with the software as if it was new in the box. In that case, you could loose programs you've installed if you don't have the original software, and you could loose documents and pictures and things you've saved or created. Frequently this can be saved if the person doing the work is good enough.

Contact, Copyright, and License Information:

Andrew Pollack
President, Northern Collaborative Technologies
andrewp@thenorth.com
http://www.thenorth.com
(207) 221-2547