



March Newsletter: Malware 101

Hello!

Your computer is acting funny, you can't browse the internet without dozens of pop-ups blocking the screen, and friends are getting strange emails from you – eek! A virus!

In this month's newsletter, we'll address what's happening to your computer (hint: it's probably not an actual virus) and what you can do about it.

All the best,
Your friends at Cartwheel

Malware 101: What is malware?

Sometimes it feels like there's no end to the rise of computer "viruses" – in air quotes because the programs that most often attack computers these days aren't actually viruses at all. They belong to a larger family of malicious software called malware (for short) – software designed to install itself on a computer system without the owner's permission or knowledge. The malware family includes the following types of hostile, annoying, or intrusive programs:

Computer viruses

A computer virus is a piece of malware that's able to copy itself in order to spread from one computer to another. Virus is often a blanket term for various kinds of malware, as we mentioned above. But really, what makes a virus a virus is its ability to reproduce – to make a copy of itself, attach itself to an existing file, and then infect another computer when that file is spread (through email, networks, or a CD, DVD, or USB drive).

Worms

Like viruses, computer worms are also self-replicating programs. Unlike viruses, worms don't need to attach themselves to an existing file. Worms spread through networks (like your office network or the internet), replicating until they've proliferated so widely that their mere presence does damage to the network. It's a little bit like a pen of bunnies reproducing, and then trying to run through the same narrow corridor at once. Too many bunnies will clog the corridor, just as too many worms spreading through a single network will hog resources, causing slowdown or a crash. Viruses, on the other hand, usually cause damage to files on a particular computer (rather than on the network itself).

Trojans

Sometimes called a Trojan horse, this type of malware doesn't replicate itself. Trojans are designed to appear as if they're a real, useful program – something that a user might want or intend to have on his or her computer. They're designed to lower the computer's defenses (for example, its firewalls or antivirus software), allowing outside access; when the user opens the



software, the program is actually allowing other programs to get into the compromised computer and perform a number of actions such as stealing valuable data, installing other unwanted software, modifying or deleting files, and downloading or uploading files. Some Trojans annoy users with pop-up ads, or fraudulently warn them about bogus “infections” and exhort them to buy fake “Trojan removal” programs.

Spyware and adware

In today’s malware landscape, spyware and adware (along with the Trojans mentioned above) are the most common culprits. Spyware is loosely defined as malware that, when installed on computers, collects information about the computer’s user without his or her knowledge. Spyware can be designed to quietly collect data from a user’s keystrokes and web browser. Adware can more aggressively interfere with computer operations. It can install other malicious software, change settings, affect your internet browser, cause issues like constant crashing or slowness, or annoy a user with constant pop-ups and warnings. These pop-ups, while often designed to appear like warnings offering to help deal with the attacking program, usually perform the function of installing yet more malware on the infected computer, much like a Trojan.

So, now that you know about these common types of malware... what should you do about it? We have a few easy tips.

1. Avoid using file-sharing or pirating applications such as Limewire and BitTorrent. Since you don’t know the source of files downloaded using these applications, you can’t trust that they’re safe. Often, individuals seeking to do harm will populate file-sharing groups with malicious applications to take advantage of unaware users.
2. Unless you’re sure you can trust the source of a free download, avoid it. Free software isn’t inherently bad, by any means. But some free programs are bundled with annoying adware; better to steer clear where possible.
3. If you don’t know what an email attachment is, don’t open it. In fact, it’s best to treat all email attachments with some degree of suspicion, even those from known senders. Some malware programs can access a user’s address book without their knowledge, sending innocent-looking emails with malicious attachments. You could be on the receiving end of one of those messages, and your contact might not have any idea that it had been sent from his account. Also, take special care never to open attachments from emails in your junk folder – those are even more likely to be suspect.
4. When web browser pop-ups appear, close them by clicking the red “x” button in the upper right corner of the window. Never click a “cancel” or “close” button inside the window itself, since often that click could actually trigger a malware attack.



Computers displaying messages or warnings that the computer is infected, or that you need to download antivirus software to avoid an infection, are probably already under attack by malware. Real antivirus programs will never introduce a pop-up of this type, so these types of warnings are more likely to infect your computer than they are to protect you against anything. Downloading the fake antivirus software these pop-ups offer will compound the problem and potentially introduce more malware to the situation. If you're seeing pop-ups with antivirus warnings or offers to download free software, the best thing to do is stop using your computer immediately (don't click anything else).

We have a lot of experience identifying and eliminating malware of all types, so feel free to give us a call at 212 206 9619 and we'll let you know if your computer is at risk.