

Article

Virus-Proof Your Computer

A whopping 92% of new information is stored on magnetic media—mainly hard disks; it is no wonder that electronic pests like viruses, worms and Trojan horses are viewed as threats on a global scale. In the electronic data realm, names like Sobig.F and Blaster enjoy similar infamous celebrity status as people like Osama Bin Laden or Charles Manson in the real world. With Microsoft making headline news with a \$5 million reward fund for tracking writers of malicious codes, does it surprise anyone that we have moved to an age where cyber attacks on a global scale is just as scary as a nuclear threat?

However, no matter how firm the governance is on virus creation and dissemination, it will not stop the hackers from hacking into the system to propagate their digital handiwork. There is capital punishment for murderers, but that doesn't stop them does it? In a world where Microsoft is viewed as the Empire, the hacker who cripples the system is king, which is good news for people who dream about world domination, but bad news for the rest of us. Therefore, it is futile (and naïve) for people to think that this is all going to blow over, that viruses and worms are harmless little pests created for someone's mindless amusement, or that this will all be gone, like the Plague.

In 1998, there were 3,734 reported cases of cyber attacks. In 2002, there were 82,094. During the first half of this year alone, there were 76,404 reported cases. The problem is not going away. As you read this, another strain of virus, MiMail.C, is trying to sneak into your computer. Now, it is no longer a question of will this virus find you, but how can you prevent it from harming you?

There are several preventive measures you can employ to thwart these cyber assailants. The following tips will provide that extra padding of safety precaution. After all, an ounce of prevention is worth a pound of cure.

1. Educate employees/end-users on computer usage
2. Keep desktops and servers patched
3. Install firewall and antivirus software
4. Respond to security issues promptly

Educate Employees/End-Users on Computer Usage

Let's face it: Not everyone is tech savvy. They are not all going to be cognizant of a new virus that's rampant. They are probably not going to understand that it is imperative they do not open unknown files—especially ones coming from someone they do not know, with promises of nude pictures or outtakes of the popular HBO comedy, *Sex and the City* (read: Torvil-A worm). This is where education plays a key role.

If you have employees who spend most of their time on the computer and who are not part of the IT crew, you are going to want them to be very careful with how they navigate the World Wide Web or how they respond to e-mails, which happens to be second only to the telephone in terms of information flow. More often than not, people who help spread a virus do so unintentionally, out of ignorance. Some of the key things you should do to make sure your company's network is well protected in personnel security are:

1. **Provide them with up-to-date information and instructions.**

During the height of the Sobig.F virus crisis, one out of ten computers were affected, and over five million emails were infected, which is not surprising, considering 31 billion emails are sent worldwide everyday, a statistic taken from the "How Much Info 2003" research compilation conducted by the University of Berkeley research team.

The figure indicates that the probability of infection on your computer is very high. To avoid infection, you have to educate your employees on the dangers of the virus and the importance of knowing the source of a file sent through email. Since Sobig.F appears under the guise of a zip file, rather than an executable file, it slips under the radar of most network security applications, which means the recipient has to be informed enough to NOT open the file, and subsequently unleashing the terror within. Notify employees on the types of emails and attachments to look out for and what they should do to prevent their computer from being infected.

2. **Implement and enforce policies to increase the effort of each individual to scan the system for virus regularly and update their own computer with the latest virus protection method.**

Corporation size can range anywhere from two people to several thousands. For a more sizeable company, it is not always easy to have an IT team large enough to manage every computer on a personal level in the company. Most

of the time the IT department will have people to secure the applications from the network end, but individual desktops will have to be managed by the user.

This scenario is ripe for a computer security policy for each company personnel. Each user should be required to protect their own system by scanning for virus on their desktops regularly. They should also observe security bulletins disseminated by the IT department that notifies them to update their software. These policies would hold each person accountable for their own system and ensure that they are more aware of the importance of computer security.

Keep Desktops and Servers Patched

In a perfect world, computer software will have no flaws. But here's the syllogism that makes the preceding sentence moot: Human beings are not perfect. Human beings make computers. Since human beings design software, it is only logical to think that the software is not going to be perfect. This is where the security patch comes in.

Every so often, you will be informed about a new patch that will reduce the vulnerabilities on your computer or increase the security of the server. These patches are also created in response to certain emergencies (like the Sobig.F and Blaster threats) and are dispersed to users to arm themselves against imminent danger. Therefore, it is imperative that you keep up to date with the security bulletin that is circulated every month or every other week.

Microsoft is known to send out patches quite frequently to inform users on vulnerabilities. However, this past year alone, Microsoft has already sent out more than three dozen patches. With 90 percent of the world's computers running on a Windows platform, this also means that more than 90 percent of the world is prone to vulnerabilities, which is quite a sobering statistic. The only good news is that IT personnel will never have to worry about job security!

Daunting statistics aside, being proactive is certainly better than being reactive, like in most cases, where companies do not step up computer security until they experience the crippling consequences of an attack. After all, taking the flu shot whether or not we are likely to be exposed to the virus is much better than the possibility of being bedridden and feeling wretched for a couple of weeks. Just updating software patches prevents most intrusions.

Install Firewall and Antivirus Software

When you have a firewall installed, it is like having a doorbell and a peephole at the main entrance to your house. If uninvited guests show up, you can see them and subsequently tell them to go away if they look suspicious. That is the basic function of a firewall. It is connected to your network gateway server to exercise control over data traffic between your local area network and the Internet. It protects the resources of your network of users from external networks.

The use of a firewall has its advantages, but there are also disadvantages to consider when setting up a firewall. While it guards you from certain attacks, the user's ability to use the Internet to its fullest potential is also limited. If your e-business is hampered by this disadvantage, perhaps the installation of a full-featured firewall is not the most ideal for your company. However, having a firewall-like feature like the packet filter, which looks at every packet of information entering or exiting the network and utilizes user-defined rules to accept or reject each packet, will enhance your network's security without impeding your business.

Before installing a firewall, weigh the risks and the benefits. You have to understand that even the most effective firewalls will not be able to prevent malicious codes designed to exploit software bugs. A firewall's effectiveness can be compromised if other security measures, like an unpatched known software vulnerability or an uninformed employee who opens strange files, are not in place.

Good antivirus software dictates how well your computer is protected from external threat. Norton, McAfee and TrendMicro are names to look for when shopping for antivirus software. The software should be configured to scan each file that comes into your computer via email, disks and instant messaging, and it should also have the most current definitions of known viruses. Every time you are connected to the Internet, you should get an update on these definitions, which means you not only have to buy the software, you also have to pay for a monthly subscription to receive the benefit of being educated on the latest information on viruses. However, do not even attempt to justify the money you spend on antivirus software versus the money you save when your computer is protected from a debilitating worm. The math is a no-brainer.

Respond to Security Issues Promptly

When a security bulletin is dispatched to suggest an upgrade, do not wait for the company's distribution of the updated version. Go to their website to download and install the new version yourself. Network administrators should be vigilant on learning about the latest virus definitions and methods to avert them, for example,

filtering against the viruses' known file attachments and scanning compressed files. When that fails, and a virus finds its way into the network, fast action is necessary. If someone is hurt, you contact 911 in hopes for a quick response to prevent disastrous results. The same applies to your computer.

To keep up with constantly evolving technology, viruses will become more virulent, more sophisticated. The implications of this growing problem are devastating. As Lee Neubecker, President and CEO of Forensicon, an electronic discovery and computer forensics company based in Chicago, puts it: "Can you imagine what will happen if someone creates a virus that extracts sensitive information like social security numbers, medical records or credit card numbers and broadcasts it to the public?" He further adds, "This virus will not only be detrimental to individuals but also corporations trying to be in compliance with HIPAA." HIPAA (Health Insurance Portability and Accountability Act) standardizes healthcare-related information systems, imposing a fine when customer data is compromised. With privacy regulations like HIPAA and the Gramm-Leach-Bliley Act (GLB Act) in place after the Enron and WorldCom fiascoes, corporation heads cannot afford to be anything but stringent with administering rigorous computer security policies throughout the organization.

E-businesses that put cyber security way down on the list will probably have to rethink their priorities. Even individual users have to exercise extreme caution. You do not want your social security number to fall onto the wrong hands any more than corporations want hackers to know their network passwords. You cannot stop the proliferation of these electronic pests. But you can at least be armed against them.