

Vaccinate your computer system



www.foundationsoft.com

The net effect of a single computer virus? Downtime and lost work, triggering lack of productivity and loss of money.

Welcome to flu season. Well, actually, we said hello to the arrival of this nasty virus a good month or so ago. It came with a flurry this year, the media calling it a strong mutated strain with deadly potential. The majority of us did what we could to protect ourselves by getting vaccinated, washing our hands until they turned raw and steering clear of anyone sneezing, wheezing or otherwise looking suspiciously ill. Lucky for us humans, the season peaks in February and fades away. Our computer counterparts, on the other hand, are exposed to deadly virus attacks *all year long*. These strikes can substantially hurt our business and put a dent in our reputation as well.

A computer's "flu" is every company's worst nightmare. A new virus gets past your company defense mechanisms (that is, if you have any) and wreaks havoc on your network. The net effect of a single computer virus? Downtime and lost work, which triggers lack of productivity and loss of money. And should you unwittingly pass the virus onto your customers or vendors, a substantial mark on the company reputation.

And if all this isn't bad enough, it gets worse. It has been reported that over 1,000 new viruses designed to attack the computer masses are written *each month*. The majority of these new viruses will still be carried through casual e-mail contact, but a rising trend in virus transmittal is coming from other, less obvious methods of infection. These can include open network file

Virus prevention tips that minimize your risk of infection



shares, visiting a contaminated website, application holes in popular software and Internet browsers...the list goes on and on.

Many nasty germs

Virus writers are never at a loss for new ideas either. Just look at some of their more memorable masterpieces:

SQL Slammer virus

This sneaky little code used a known vulnerability in Microsoft's SQL server application to spread its infection. And it did so rapidly.

MiMail

Some viruses use social engineering to make their way onto your PC. The recent "MiMail" strain of viruses appeared to be a legitimate email from PayPal—stating that the user's account had expired—and that their credit card information was needed to re-open

their account. The email then directed users to a spoofed PayPal website—where unsuspecting users gave their credit card information directly to the virus writers.

Dumaru

The Dumaru virus falsely claimed to be from Microsoft Security and offered users a patch to help protect their PCs from a "newly discovered vulnerability." Once "installed," this virus would log and report keystrokes back to the virus writers.

W32.Swen

The W32.Swen strain exploits a vulnerability in Microsoft Outlook and Outlook Express in an attempt to execute itself when you open or even preview the message. It also attempts to spread through popular file-sharing networks, such as KaZaA and IRC, and it also attempts to kill antivirus and personal

firewall programs running on a computer in its dastardly way..

Doctor, doctor

The good news: There are many precautions that you can take to minimize the risk of exposing your hardware and company network to a virus. Although not a miracle cure-all, done properly these tips offer some level of protection. These virus prevention techniques include:

Make sure that every PC in the company has antivirus software installed and frequently updated (all antivirus vendors offer regular updates so that the application can identify the latest viruses). *Your antivirus application is only as good as the "last known virus."*

Schedule and run periodic antivirus scans. These scans can take up substantial PC and server resources, so it's best to schedule them during off-peak hours (such as during lunch time and overnight hours).

Implement a secure firewall to protect the internal company network from the outside world. A firewall is a system designed to prevent unauthorized access to an internal network. Firewalls can be implemented using hardware, software or a combination of both. All messages entering or leaving the internal company pass through the firewall, which examines each one and blocks those that do not meet specified criteria.

Stop unnecessary services from running on servers. Examples of these vary widely depending on network needs, but may include blocking or restricting use of FTP (File Transfer Protocol), SNMP (Simple Network Management Protocol) and SMTP (Simple Mail Transfer Protocol), just to name a few.

Establish clear company rules about opening e-mail attachments and publicize them to your employees.

When in doubt, check with the sender prior to opening.

NEVER click on attachments from dubious e-mails.

Implement policies that prohibit employees from

downloading games, screensavers or executable files.

Keep applications and PCs patched/updated (for instance, SQL 2000 server has service pack 3a available for download).

Scan your network and remove highly vulnerable file sharing programs (such as KaZaA and Bearshare) and low security Internet chat programs (such as IRC).

Hopefully, this advice will help you to avoid getting hit by any of the numerous virus strains that travel the Information Superhighway. However, you do need to remember that these are only preventive maintenance measures. It is still possible to get hit by viruses, even when you play by all of the rules. **BXM**

Fred Ode is the founder and chairman/CEO of Foundation Software, Inc. Ode developed a construction-specific accounting software, Foundation for Windows, that suits a range of trades. For more information, visit www.foundationsoft.com or call 800-246-0800.



Your *h o m e* can **H E L P**
y o u . . .



I N D U L G E Y O U R S E L F I N
P A R A D I S E

Let The Ohio Educational Credit Union show you how the equity in your home can help you make fantasies realities. www.ohioedcu.com