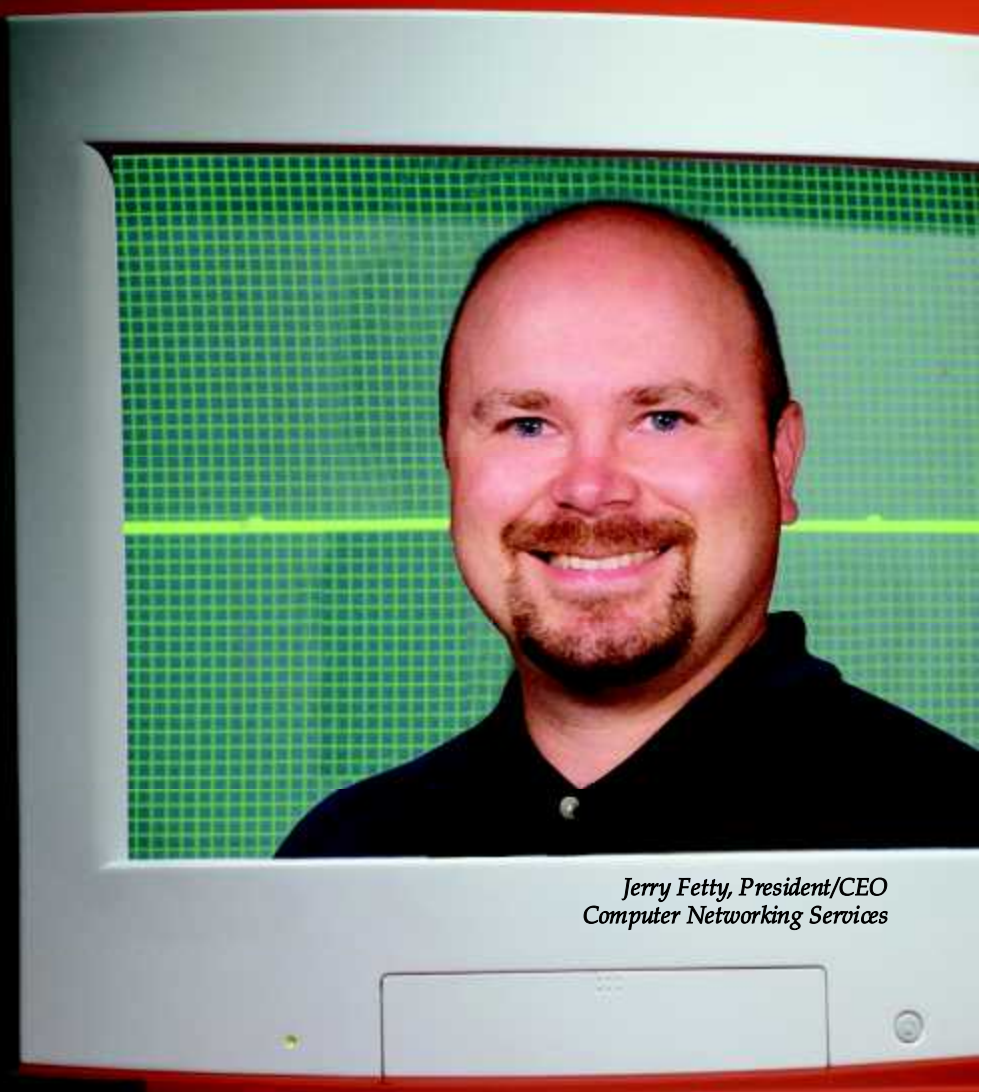
SECURITY—PRONOUNCED "SECURE-I-T"

Tips, techniques, and thoughts for keeping computing systems and resources safe and secure

By John Chivvis

For many insurance agencies, when computers stop computing, servers stop serving, and networks stop networking, there is no IT support staff on call to handle the problem. "It's in these agencies of 20 employees or fewer—and there are a lot—where you find an employee has assumed or been delegated the job of 'computer person' due to a perceived knowledge of computers," says Jerry Fetty, president of the Sterling Heights, Michigan-based Computer Networking Services (www.compserv.net).

It's these same employees to whom Fetty speaks at seminars, sessions and conferences such as the Michigan Association of Insurance Agents' Great Lakes Automation Day. Fetty knows that it is no easy task to keep an agency's computer resources safe and secure from problems stemming from spyware, intrusion, spam and viruses. As he "preaches" to the masses, Fetty says that by implementing some simple policies, establishing some basic procedures, and following some simple tips and techniques, some of the IT problems agencies face could be reduced or eliminated—thus reducing IT expenses and increasing productivity for the IT staff.



Jerry Fetty, President/CEO Computer Networking Services

Passwords—secret, strong and shifting

"Passwords are the keys to the network; if someone else knows them, then a firewall, for example, is useless," says Fetty. "Most agencies running Applied or AMS systems still have the administrator passwords set as the default. This means there are literally tens of thousands of people who know the password to an agency's system."

Fetty says that while at first it may seem difficult to do, an agency must define a password policy for employees. Passwords should be at least seven characters with a mix of upper and lower case letters, numbers and even special characters such as #$%*. According to Fetty, simple passwords like dictionary words, home addresses, and numbers are usually the first to be tried by hackers.

The password policy should also set an "expiration date" after which employees must change their password. "This is where a principal must not give in," says Fetty. "Too

Reprinted from the March 2005 issue of **Rough Notes** magazine

often, employees will freak out the first time they have to change their password. Even though it may throw employees for a loop at first, training and persistence is important, because eventually it becomes a non-event."

By implementing some simple policies, establishing some basic procedures, and following some simple tips and techniques, some of the IT problems agencies face could be reduced or eliminated.

—Jerry Fetty

Spyware—show no mercy

Fetty is a strong proponent of agencies implementing an Internet usage policy, if anything, just to keep spyware off computers. "A good number of the agencies that call us about computers that are slow or not running turn out to have a spyware issue," says Fetty. "However, if an agency uses the Internet for business purposes only, how much spyware do you think they'll get from a vendor or carrier Web site?"

While not technically a virus, spyware is any program that is unknowingly or unwittingly installed on a computer and uses the machine's bandwidth, memory and file space to record and send information across the Internet regarding the employee's computer usage patterns. With computers being used for more than just office work—even something as innocuous as listening to music on a computer or online—the opportunity is great for spyware to propagate on a machine or on a network. To illustrate the point, Fetty describes an experiment he conducted using a simple music-sharing program called Kazaa.

"All we did was install Kazaa on a computer," says Fetty. "We didn't download any music or use it in any way, but just left it for 12 hours. When we came back, there were already a couple hundred spyware programs that had installed themselves on the computer."

To seek and destroy spyware, Fetty recommends installing anti-spyware software and running it on a regular basis (usually once a week or as needed). While there are commercial grade spyware blockers on the market, Fetty notes that for most agencies, simply downloading, installing and running Lavasoft's free Ad-Aware application will identify most of the programs. As an overlap, Fetty also recommends Spybot Search & Destroy to catch what Ad-Aware may miss and vice versa.

Viruses—not just for office desktops anymore

"When a principal tells me that the agency doesn't have a virus scanning solution in place, I can't figure how they managed to get to this point without problems," says Fetty. And considering the increase in technology investments beyond an employee's desktop, such as mail servers, databases, laptops, and file servers, it's even more puzzling why an agency would put that investment at risk by not having an antivirus solution.

First and foremost, Fetty says, an agency needs an antivirus solution that will protect the agency's entire network including servers and all workstations. "The same holds true for remote users," says Fetty. "Those that dial in from home also need to have antivirus protection on their remote workstations or laptops."

Second, Fetty says that antivirus software must be checked regularly to see if updates are being received and

TOOLS TO FIGHT THE FIGHT

Safe and secure computing means having the right tools—whether it's for two users or 200 users. Listed here are the Web site addresses and more information on a number of the tools that Computer Networking Services' Jerry Fetty mentioned.

- **Ad-Aware SE** by Lavasoft (www.lavasoft.com). Free basic download is available for the removal of adware and spyware. It can scan a computer's RAM, registry, hard drives, and even external drives as well as computers with multiple accounts. It also has an auto-update feature to keep up with the latest components.
- **Spybot Search & Destroy** by PepiMK Software (www.safer-networking.org). Free download detects and removes adware and spyware. Functionality includes the ability to review what programs load when a computer is started up as well as adware and spyware blockers. Auto-updates keep program up to date.
- **Symantec AntiVirus 9.0/Norton AntiVirus 2005** by Symantec (www.symantec.com). Symantec is geared for the networked office, providing antivirus protection to desktops, file servers and offers the IT administrator a number of controls and reporting features. Norton is geared for single user computers or for remote users dialing in.
- **McAfee Active Virus Defense SMB** by Network Associates (www.mcafee.com). AVD offers a complete antivirus suite protecting desktops, print/file servers, mail servers, and the Internet gateway. It includes an easy wizard-based interface for installation and management.
- **ZoneAlarm** by Zone Labs (www.zonelabs.com). Free download for home use provides basic firewall features including making a PC "invisible" to hackers. ZoneAlarm Pro (for purchase) provides firewall functionality plus pop-up blocking, privacy and data protection and more.
- **GFI MailEssentials** by GFi (www.gfi.com). Commercial product for mail servers, which prevents the need for anti-spam software on each desktop. It employs a number of technologies such as Bayesian analysis, black/grey/white listing and automatic environment adaptability to detect spam upwards of 98% of the time.

applied. For agencies with limited IT support, checking five computers for current virus definitions may not be difficult but as the agency grows to 10 or 20 users, the task becomes greater. According to Fetty, that's where advanced features in commercial packages such as McAfee's Active Virus Defense or Symantec/Norton AntiVirus make it easier.

These software packages provide reporting capabilities allowing administrators or IT people to run reports on the state of the network to see if every computer is up to date with virus definitions, which computers are getting the most virus hits, and if any computer has the virus scan disabled. "It takes only one workstation not updating properly to wreak havoc on the system—corrupting servers and bringing the whole agency network down," says Fetty.

Firewalls—stopping trouble at the door

According to Fetty, some agencies see firewalls as some kind of mystery box. "Some agencies have purchased a firewall and are doing nothing with it," he says. "Either it is turned off, because it seemed inconvenient, or all the ports are open because their vendor isn't used to insurance carrier sites and requirements."

Fetty says that agencies of all sizes need to have a firewall in place to prevent unauthorized access to their system. For small agencies of five users or fewer, Fetty says that software like Zone Labs' ZoneAlarm provides ample firewall protection. "It's also a good idea to install it on home machines for remote users," says Fetty. For larger agencies, Fetty says that it is better to have a network firewall installed by a trained professional.

However, just because an agency has a firewall doesn't mean a virus can't break through, or that virus updates or patches are no longer needed. "We recently had a 70-user agency call us," says Fetty. "They had a firewall and virus scanning, but nothing patched, and all an employee did was browse to a Web site, pick up a virus and the agency's whole network was down for three days."

Spam—one person's trash is another's treasure

While Fetty speaks on a host of topics, he *knows* spam. "We have 20 computer users in our company and we get about 40,000 e-mails a week," says Fetty. Built-in spam filters found in e-mail programs like Microsoft Outlook or Novell's GroupWise or commercial products like GFI MailEssentials may use a host of algorithms, lists and methods to reduce and remove spam, but Fetty notes, "you will always get spam."

Fetty says that the question an organization must answer is, "What is the acceptable threshold for spam?" If it is low, and a single spam e-mail is too much, then there is a strong possibility that good e-mails will end up in the spam folder and be deleted. If the threshold is set fairly high, then agencies will find themselves "whacking and stacking" e-mails as Fetty calls it.

Fetty says that the least expensive way to minimize spam is to simply not open it. "Spam is coded to send a reply back to the sender and say your e-mail address is a good one," says Fetty, noting that fake PayPal, eBay, bank and other "phishy" e-mails need to be deleted. Opening spam e-mail, or responding to a spam's "unsubscribe" feature usually means more spam is on the way.

But what Fetty finds many agents don't realize is that in their e-mail programs, using the "preview" pane is the same as opening the e-mail. On a recent agency visit, Fetty dealt with an employee who was getting all sorts of spam and viruses, even though that computer had been wiped clean a week before and the employee said he was deleting the e-mails without opening them. In fact, the employee was deleting them but because the preview pane was active, the e-mails were opening as they were being deleted. "Preview panes actually open the mail for you to preview it," says Fetty. "That's why we recommend the preview pane be turned off."

Support—an ounce of prevention or a pound of cure

For agencies of all sizes, IT staff can be stretched beyond their expertise. From IT duties by default in small agencies to sudden enterprise level IT issues in multi-office, multi-city agencies, learning tips from experts like Fetty and attending programs found at events like the Great Lakes Automation Day can help.

Besides education and training for internal IT staff, it's also important to know when to get help from external IT professionals. Fetty says it's best to seek an outside IT vendor's advice earlier, instead of after the damage is done. "It costs a lot more money to clean up a computer or server problem," says Fetty "than it does to prevent it." ■