



FRONTLINE

SPRING 2004

TIPS AND TECHNIQUES TO PROTECT YOUR INFORMATION

INSIDE

4 Department of the Interior

Story highlights

2 Proof Positive

Has your Web site suffered unauthorized access or misuse in the last 12 months?

3 Special Tactics

Phishing: the latest Internet attack to gain popularity among the hacker crowd

3 Under the Microscope

Witty worm? The first virus we've seen in a long time that tries to harm the PCs it infects

Giving Away the Store



Back in early March of this year, an employee of an Atlanta-based corporation used the company president's password to hack into the purchase order system and approve several orders that supposedly came from the president. The president of the company, needless to say, changed his password as soon as the hack was discovered. He also issued an e-mail to the company warning that the perpetrator would be summarily fired if caught.

The memo said, in part: *If I find out who you are, it will be your last day with the company, GUARANTEED! (your "severance package" will be someone escorting you to the front door!).*

Up to that point, the incident was an internal company matter. But at least one recipient of the e-mail forwarded it to a public Web site. Not just any Web site, but a widely read one with an obscene name.

It's not a story that made the news headlines—it's just not that big of a story, especially since the problem was caught before the ordered goods arrived. But just about any company would rightly prefer that employees didn't forward internal e-mails of this sort to the outside world. You should know that an increasing number of companies monitor outbound e-mail traffic for messages that contain company secrets or inappropriate content (such as profanity).

The CEO at a company that makes monitoring tools recently shared with us the usual experience of what happens when their tools are installed at a corporation. They catch people sending out information that they shouldn't be sending—but mostly it's not ill-intentioned, disgruntled employees like the one who forwarded the company president's e-mail (though they catch those, too). Most of what their monitoring systems snag are files that well-meaning employees either send out by mistake or don't realize they shouldn't be sharing.

[Continued on page 2]

Making Firewalls Personal

Worried about securing your personal PC? You may have cast an eye at one of the several "Internet Security" products on the market now, and noticed that, along with filters designed to weed out spam, the main ingredient in these packages is a "personal firewall."

Firewalls, at least when it comes to the Internet, are a special kind of filter that tries to keep out messages from those who mean you harm. As each bit of data arrives at or leaves your computer, it is inspected by the firewall software to determine whether it should be allowed to pass through or whether it should be blocked.

When would such a firewall decide to block data? If it's data that's leaving your computer, it might be blocked if it is being sent from an application that hasn't communicated with the Internet before. Your Web browser sends requests to the Internet all the time, so a firewall will let those requests go through, but if a new application called "Badhacker.exe" starts trying to send data to the Internet, a firewall will recognize that it hasn't seen this sort of communication before and will pop up a window on your PC asking you if this is OK.

For inbound data, the firewall will allow communications that are associated with normal

[Continued on page 3]

We're not talking about accidentally disclosing closely guarded secret recipes and the like. Usually, the vast number of employees in a company don't have access to these "company jewel" sorts of information. But plenty of information that company insiders routinely have access to really ought to be treated as sensitive, confidential information.

One way to think about what information might be sensitive is to think about what kinds of information would be useful to an outsider who was performing corporate espionage and trying to learn about your organization. It can be very useful to such spies to know when a product is likely to go to market. Or if the product is specialized hardware with top-secret plans, a great deal might be learned just from finding out what companies are supplying parts for the product. They'll want to know if you've been hiring an unusual number of support representatives.

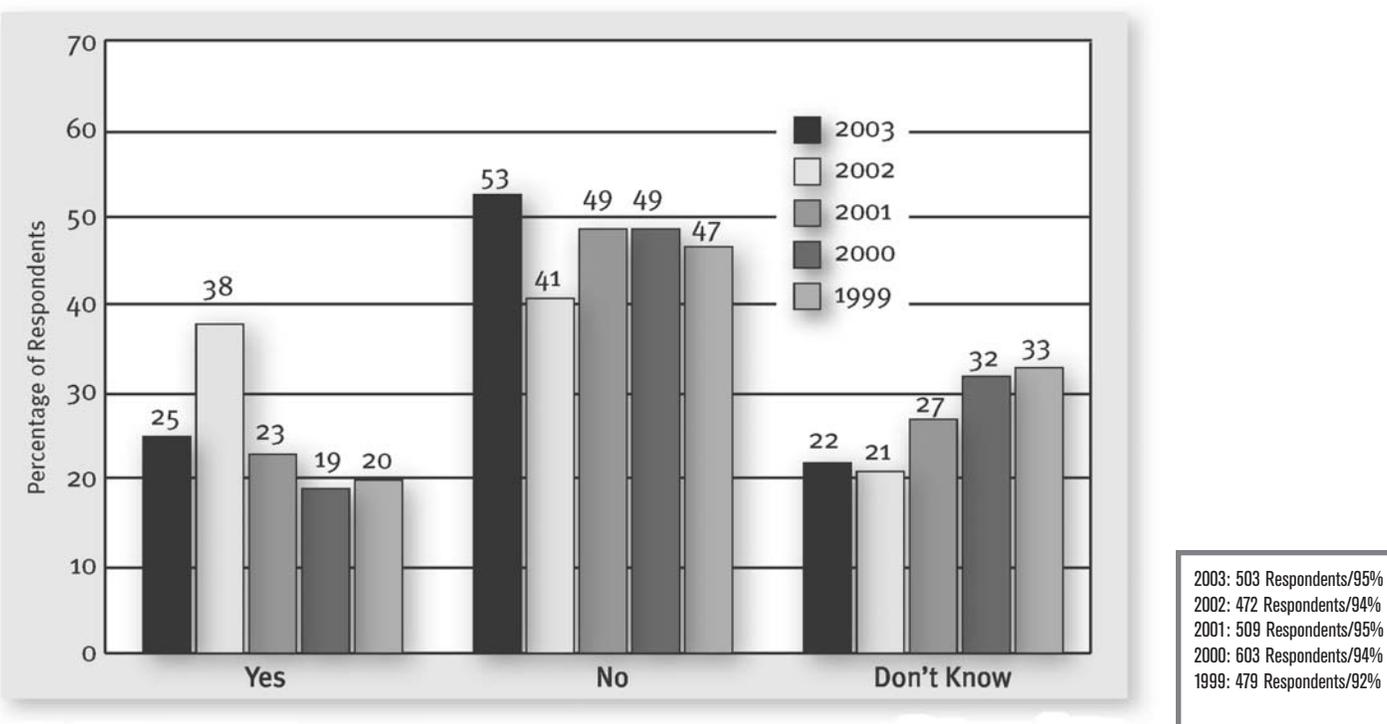
1. Make sure you understand all internal systems for handling company data. Information such as customer credit card numbers is sensitive, of course, but so is other customer data. It may not even be appropriate to acknowledge to a third party that a given person actually is a customer—make sure you understand the rules before you disclose information.
2. Make sure you really know who you're talking to when you disclose a company's inside information. If you've been called by someone you haven't dealt with before, verify their number and call them back before you proceed.
3. Most e-mail systems preserve the "thread" of a series of replies to an original message. When you read down through the message, you can see how the discussion progressed from the original message. While this is one of the most useful features of e-mail, be very careful to con-

sider the contents of the entire e-mail any time you decide to forward an ongoing conversation to new recipients, especially if they are to people outside the organization. Don't forget to double-check any attachments to the e-mail as well.

4. Make sure that price lists and marketing materials have been cleared for public release before you send them to potential customers.
5. Don't volunteer extra information. Say your colleague is "out of the office," not "on a plane to Phoenix." In some cases, this may tip your hand about who potential new clients or suppliers could be.
6. Don't leave sensitive information in voicemail messages, even if you're sure that you've got the right person's voicemail. Many voicemail systems have poor security and hackers are well aware of this.
7. This may seem obvious, but it's worth the occasional reminder: don't leave data where it can be stolen. Don't leave folders with draft documents on your table at the coffee shop while you're over picking up your latté. Don't leave your notebook computer in your car.

And what should you do when someone sends you information that seems confidential? What if you receive an e-mail that contains information you probably shouldn't have? If it's significant confidential data from a competitor, talk to your manager. The best course of action (both in terms of what's legal and what makes business sense) can be hard to figure out in these cases—don't make the decision on your own. In less extreme cases, a friendly reminder to your correspondent may well be in order—most breaches are accidents and these kinds of accidents can be prevented. **FL**

Proof Positive: Has your Web site suffered unauthorized access or misuse in the last 12 months



CSII/FBI 2003 Computer Crime and Security Survey
 Source: Computer Security Institute

They Aren't Catching Trout

The latest Internet attack to gain popularity among the hacker crowd is called "Phishing," a play on words on "fishing." The idea is to throw a little bait to the victim and let them hook themselves into handing over credit card and other personal information.

The bait in a phishing scam is an e-mail that links to a Web site that pretends to

those Web sites is violated) and individuals (when their personal information is stolen and used to carry out credit card and other kinds of fraud).

The trick to stopping phishing scams is to notice the fake Web sites early, before users can be duped. One important line of defense here is you: if you deal with users of your organization's Web site and

When you're surfing the Web, never assume that a Web site is safe just because it looks like the real thing.

be the real site of a real company. Typically, the e-mail asks you to update your account information and the Web site pretends to be the real company, with faked forms that ask for your personal information. Companies that are most often the victims of these fake sites are eBay, Citibank, and PayPal, according to the Anti-Phishing Working Group (www.antiphishing.org).

According to the group, the phishing tide is rising. They recorded a 60 percent increase in phishing sites (from 176 to 282) from January to February of this year.

Phishing hurts both organizations (when their Web sites are faked and user trust in

they report an interaction with your Web site that sounds suspicious, check with your manager or support department.

For your own protection when you're surfing the Web, never assume that a Web site is safe just because it looks like the real thing—what makes phishing work so well is that copying the exact look of any Web site is easy. To make sure you've got the right Web site, don't give information to a Web site if you got there by clicking on an e-mail link. Instead, type in the main address for the Web site into your browser ("www.the-company.com") and follow the links on the site—that way you can be confident you've got the real thing. **FL**

Making firewalls personal

[Continued from page 1]

activities such as Web browsing. But if an outsider tries to access a part of your operating system that most home users aren't even aware exists on their computer, the firewall will again raise a red flag and ask for guidance. In the case of last year's Blaster worm, for example, users with firewalls found that the unusual path of attack that Blaster took advantage of was automatically blocked off. They were safe even if their anti-virus package hadn't yet been updated to recognize the new threat.

Do you need a personal firewall? Well, you should probably at least seriously consider it if you are attached full time to the Internet. Some organizations are considering (or have already) deployed them on their desktop computers. But the situation is a little different for organizations with large networks, because they already have bigger, whole-network

firewalls that protect the entire network where it connects to the outside world. Home users don't have the same "outside" layer of protection and will see more direct benefits. Microsoft likes them enough that there are plans to incorporate a no-frills personal firewall in the next major release of the Windows operating system.

Personal firewalls aren't perfect, though. They don't always detect malicious communications. Furthermore, they can be attacked just like any other software. The recent Witty virus (see the sidebar) used a defect in one vendor's personal firewall software to take control of its victims (the problem was patched within a day, however). As a general matter, personal firewalls increase a home user's security and are worth considering for the extra layer of protection they provide. **FL**

Witty Worm?



Almost any software running on a PC can have programming errors that make it vulnerable to Internet attacks—even when that software is sup-

posed to be protecting you from those attacks. The "Witty" worm, for instance, attacked a personal firewall application called BlackIce. This application scans through all the various "packets" of data that come from the Internet to the PC where it's been installed, but an error in the program caused it to malfunction when handed a particular kind of packet that had been loaded with data in an unexpected way. When the program trips up on the poisonous packet, the worm gets a chance to insert itself on the computer (the program was patched the next day and the spread was contained).

Two things to note about Witty. First, it's the first virus we've seen in a long while that actively tries to harm the PCs it infects (it gradually corrupts their hard drives). Second, it attacks software that's supposed to be protecting you. Of course there's no way to know, but we suspect we'll see more destructive worms and viruses over the next several months. This probably isn't the only worm we'll see that feeds on security programs either. All the more reason, in other words, to make absolutely sure that your anti-virus software is completely up to date and functioning properly.

It's called "Witty," by the way, because of a remark embedded in the worm's software code: "insert witty message here." Apparently the worm's creator came up short in the wits department.

Horror Stories

Headlines throughout the world abound with tales of cyberspace crimes, misdemeanors, and foul-ups. These horror stories make the diverse threats to your organization tangibly and poignantly clear.

WEFTV HACKER

FBI agents recently arrested a Louisiana man under the cyberterrorism provisions of the USA PATRIOT Act for allegedly tricking a handful of MSN TV users into running a malicious e-mail attachment that reprogrammed their set-top boxes to dial 9-1-1 emergency response.

According to prosecutors, David Jeanson, 43, was targeting 18 specific MSN TV users in an online squabble when he crafted the script in July 2002, and sent it out disguised as a tool to change the colors on MSN TV's user interface. Though the code didn't mass-mail itself to others, some of the recipients were sufficiently fooled that they forwarded it to friends, for a total of 21 victims.

—*SecurityFocus*, 12/5/03

FREE MSN

A flaw in Microsoft's MSN Explorer software has allowed some Web surfers to gain free access to features and services that normally cost \$9.95 (£5.35) per month, the software giant confirmed.

Programmers in mainland China discovered the flaw sometime last year, a source familiar with the exploit told ZDNet China. This person, who spoke on condition of anonymity, said Chinese hackers have successfully created MSN Explorer 9 premium accounts that provide free access to 30 MB of online storage and a 25 MB e-mail inbox, as well as to applications such as MSN Money Plus.

—*CNET Asia*, 2/27/04

PHISHER GETS SNAGGED

According to the FTC, Zachary Hill of Houston, Texas, sent out official-looking e-mail notices warning America Online and Paypal users to update their accounts to avoid cancellation.

Those who clicked on a link in the message were directed to a Web site Hill set up that asked for Social Security numbers, mothers' maiden names, bank account numbers and other sensitive information, the FTC said.

—*Reuters*, 3/22/04

COMCAST KILLS ZOMBIES

Comcast has been contacting customers whose machines are being used as "zombies" to forward spam e-mail with warning messages. In some cases, the company has cut off Internet access to customers, some of whom are unaware their system is sending out the commercial solicitations, said Jeanne Russo, a spokeswoman for Comcast's cable division.

—*InfoWorld*, 3/9/04

WEATHER REPORT IS UNPREDICTABLE?

Before the system was shut down, viewers tuning into Time Warner Cable's News 14 Carolina for updates on February's record-breaking snow storm could read in the text ticker on the lower third of the screen that a company called "h4x0r3d Computer Services Inc." was among the businesses that would be shuttered the next morning because of the storm.

According to screen shots saved by observers, other messages sprinkled among the genuine closings that rotated through the ticker included "1337 5p34k Linguistic Services," "All Your Base Are Belong To Us," and a note that "Tutone Inc." would be closed, and employees should call "Jenny at 867-5309" for more details.

—*Security Focus*, 3/4/04

PIRACY VIGILANTES

A pair of coders nurturing a deep antipathy for software pirates set off a controversy when they went public with a months-old experiment to trick file sharers into running a Trojan horse program that chastises users and reports back to a central server.

As of March 18 the crime-busting duo's server had logged over 12,000 victims of "Walk the Plank," and a sequel they call "Dust Bunny," since the cyber sting secretly launched in January. The programs have circulated disguised as activation key generators and cracks for Unreal Tournament 2004, Pinnacle Studio 9, Norton Antivirus, TurboTax, and as a copy of the leaked Microsoft source code—all titles chosen for their popularity on peer-to-peer networks. When executed, a large message appears scolding, "Bad Pirate!"

—*SecurityFocus*, 3/18/04

BJ'S COMPROMISED?

A "possible compromise" in the computer systems used by BJ's Wholesale Club stores remains under investigation after the company learned that credit card information for some of its customers may have been stolen.

The Natick, Mass.-based wholesale consumer buying club said in a recent announcement that a "small fraction" of its 8 million members may have been affected by the data thefts from its stores. The incidents are being investigated by credit card companies and law enforcement agencies.

—*ComputerWorld*, 3/19/04

BUG PLANTING SEASON?

A Californian insurance claims manager was recently charged with planting an electronic bug on a computer owned by his former employers. Larry Lee Ropp, 46, was indicted on a single wiretapping charge over an allegation that he planted a keystroke logger on a PC used by a secretary to senior executives at Bristol West Insurance Group. Police arrested Ropp after he allegedly asked a former colleague to remove the bug.

—*The Register*, 3/24/04