January 2007

Intelligent Technical Solutions

Innovations

Quotes

"We can let circumstances rule us or we can take charge and rule our lives from within." *Earl Nightingale*

"If you want to make peace, don't talk to your friends. Talk to your enemies." *Moshe Dayan*

"Avoiding danger is no safer in the long run than outright exposure. Life is a daring adventure or nothing at all." *Helen Keller*

"Be master of your petty annoyances and conserve your energies for the big, worthwhile things. It isn't the mountain ahead that wears you out, it's the grain of sand in your shoe." *Robert Service*

How to shield your network from clever hackers

You've got antivirus software and firewalls guarding your computers and routers. You religiously download security updates. You've done everything you can think of to stay secure. But your network is still at risk.

Why? Because an employee could unwittingly give away the castle's keys.

The biggest threat to a computer is not a hardware or software problem. It's social engineering.

What it boils down to is this: Someone will attempt to gain an employee's trust. Information can be elicited from that employee that puts everything at risk.

Social engineering relies on the fact that most people are nice. They want to be helpful. There's a natural inclination to lend a hand when someone has a problem.

These efforts can be conducted over the telephone, via e-mail, or through instant messaging. Larger organizations are especially at risk, because employees do not know one another, but small businesses can be victimized too. Anonymity is important to the hacker. But the little fish at a company can also be "gamed."

So let's look at four different social engineering situations -- and the ways to thwart them.

1. The caller isn't working on your network. One of your newer employees gets a call from a computer repair technician. "My name is Joe Smith," says the technician. "Your company's network is having problems, and I'm working on it. I need you to type in some commands."

On the face of it, this is silly. Any legitimate repair

(Continued on page 2)

Microsoft Releases Internet Explorer 7

Significant Security Improvements, New Features

Microsoft has released Internet Explorer 7, the newest version of their web browser. The program, which has been in the works for nearly five years offers many significant improvements and is a worthy upgrade.

"Internet Explorer 7.0 is the best browser Microsoft has ever produced," wrote Mike Wendland of the Detroit Free Press.

Users running their Windows Updates have been offered the upgrade option beginning last week. The new version does require Windows XP Service Pack 2, so if you haven't kept up with Windows updates, you may need to install these updates before being offered the option to download IE7. The Windows Update service will handle everything for you.

Few problems have been reported with the upgrade, although there are some known incompatilbilities with the Yahoo Toolbar. The most current version of the toolbar works fine, but older versions do not.

For those still a bit squeamish about upgrading, there is an excellent uninstall utility that can restore your

(Continued on page 4)

I | T | S

INTELLIGENT TECHNICAL SOLUTIONS

Clever hackers. . .

(Continued from page 1)

tech is going to have access to the network, if that's what he needs. How else could he fix the thing?

The caller is playing on your employee's natural desire to be helpful. The employee is unlikely to understand the commands he is asked to enter. They may expose the structure of the network, or open a security hole.

The caller then asks the employee to enter commands that identify his desktop computer. "Aha," he says. "That's the machine that has been causing the problems. I'll need your username and password."

Once the caller has collected this information, you could have an identity theft problem. He has a route into your system and he knows how your network is structured. If you have a database of customers and their credit card numbers, he may download it. Or he could get into your payroll system. There, he'll find Social Security numbers.

What to do? Train your employees to never, ever give out information to such callers. Computer repair personnel already have access to the network. If they don't, there's probably a good reason. And they should already have a password with system privileges. They don't need an individual employee's password.

At the very least, employees should check with a supervisor before disclosing sensitive information.

2. That e-mail isn't from Joe. One of your employees gets an e-mail. It's from her friend Joe. It has an attachment. Without giving it much thought, she opens the attachment. It's something unappealing, so she deletes the e-mail and forgets it.

Unfortunately, that attachment includes a Trojan horse. Your antivirus software should whack it. But maybe you haven't kept the antivirus software up-to-date. The Trojan could use a backdoor port in Windows to download more dangerous programs.

These programs could find their way around your network, digging for credit card and Social Security numbers.

Employees should never open attachments they were not expecting. Legitimate return addresses are easily stolen by worms. The fact that the e-mail bore Joe's return address is meaningless. If your employee wasn't expecting something from Joe, she should have checked with him before opening it.

3. When the hackers go "phishing," don't take the bait. An employee gets an e-mail message that her eBay (or PayPal, Citibank, America Online, etc.) account has a problem. She's told that she must go to a certain page for more information. The spam includes a link.

When she clicks the link, a page with the company's logo opens. It explains that her account will lapse unless she re-authorizes it. It then asks for her username and password.

Or it may ask for a credit card number, or perhaps a Social Security number. Sometimes, it requests her mother's maiden name (often used as a hint to get a password restored).

Your average crook isn't a Rhodes Scholar, so, early on, these schemes were unsophisticated. The "phishing" pages were poorly designed and often contained bad English. And their Web addresses clearly had nothing to do with the companies they supposedly represented.

More recently, the pages have been much better designed. And the pages often contain the logos of eBay or other companies. You'll find links to the company's real pages. It's easy to be suckered.

So remember this: eBay isn't going to ask for a password. Neither will AOL or any other legitimate company. Delete all spam, including these pitches.

What, you may ask, does an eBay password have to do with my business? Just this: People often use the same password for everything. So the eBay password may also give access to your network, a bank account and other confidential areas.

4. You must protect your company. A good security system will protect you technologically and socially.

Your employees are there to do a job. They're probably overburdened, so they'll resist worrying about security. But you must train them never to give out sensitive information, unless they are certain of the caller's identity, and never to open an attachment they were not expecting. (Do you think passwords are safe? In a London study, passersby were asked at random to give up their passwords in exchange for a candy bar. Seventy percent complied!)

(Continued on page 4)

The Lighter Side

Things toddlers eat....

Panicking when his toddler swallowed a small magnet, George, rushed him to the emergency room.

"He'll be fine," the doctor promised. "The magnet should pass through his system in a day or two."

"How will I be sure?" he pressed.

"Well, the doctor suggested, "you could stick him on the refrigerator. When he falls off, you'll know."

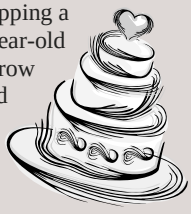
Grief and suffering

A dietitian was addressing a large audience in Chicago:

"The material we put into our stomachs is enough to have killed us. Red meat is awful. Soft drinks erode your stomach lining. Chinese food has MSG. And vegetables can be disastrous.

"But one thing is the most dangerous of all and we all have eaten it or will eat it. What food causes the most grief and suffering for years after eating it?"

Without skipping a beat, a 75-year-old in the front row stood up and said, "Wedding cake."



Resilience, bouncing back

The power to bounce back from disaster is called resilience. By actual definition, it is "the human ability to adapt in the face of tragedy, trauma ... and ongoing significant life stressers."

At one time, it was thought that some people were born with resilience, and others were not. That wasn't true.

Researchers at Wayne State University say we are all born with a tendency to be resilient. Most people are stronger than they give themselves credit for.

You don't have to get caught in a hurricane or suffer a tragedy to develop resilience. With work, family, trying to get enough sleep, whatever your situation, it comes from the belief than you can and will create positive outcomes.

Email: how personal is too personal?

When you get an email and the sender just starts writing, do you feel a little neglected? Shouldn't it be a little more personalized? But then, do you begin with "Dear Sir," Dear Mr. Jones," "Joe," or something else?

In a business email, say the etiquette experts, it's best to address people the same way you do when speaking with them in person.

If your first-name status feels a little tenuous, go with the more formal salutation.

Signing your email

Your email "signature" can offer your correspondent some important information, sometimes not obvious from the email headers.

Because the name of the sender is not always clear from the email address, always include your full name at the bottom of a message. Some companies use abbreviations or codes in the sender's address that may mean little to the recipient.

Put your email address after your signature. If it's a business address, include the company name and your title in the signature. (Some email programs allow you to set up automatic signatures.)

"I'm so proud of him! He just deleted his first 'Nigerian Money Scam' e-mail."

I | T | S
INTELLIGENT TECHNICAL SOLUTIONS

January 2007

7500 W. Lake Mead Blvd. #9-196
Las Vegas, NV 89128

(702) 869-3636
(888) 969-3636 toll free

www.itsasap.com

"We make all of your computer problems go away without the cost of a full-time I.T. staff"

Ask us about our fixed price service agreements — Computer support at a flat monthly fee you can budget for just like rent!

Hackers. . .

(Continued from page 2)

But even the best-trained employees can be suckered. The desire to be helpful can lead them down the garden path. Assume your system eventually will be invaded; keep critical information walled off from most employees. Only those with a real need should have access to databases or payroll information.

Even if a worm gets into your system, it can be thwarted. If you religiously update your antivirus software and Windows, worms can be knocked out or blocked. Be sure the firewall in your router has been activated and properly configured.

Worm and virus technology is rapidly growing in sophistication. Coupled with social engineering problems, the threat to your company is very real. You must stay alert.

Reprinted courtesy of Microsoft Corporation.

Internet Explorer 7. . .

(Continued from page 1)

previous web browser in a flash.

So what's new?

Security: Security is the name of the game these days, and the Internet Explorer has historically had a terrible security record. IE7 was designed with security as the first, second, and third priority. Running an entirely new architecture, IE7 disables virtually all ActiveX controls by default, which will stop spyware programs in their tracks. There is also protection against "phishing" (further described on page 4) where a web site masquerades as something else (i.e. pretending to be Bank of America to get you to enter your password).

Cool Stuff: The program has been redesigned to be simpler to use, but perhaps the biggest innovation is "tabbed browsing". You can view multiple web sites in the same browser window and switch between them through tabs at the top of the window. This eliminates multiple Internet Explorer windows open simultaneously.

An additional feature is support for RSS feeds. RSS allows you to "subscribe" to a web site's news and information. As the headlines change the browser will update itself automatically. This functionality has been around for a while on sites such as My Yahoo, but it is now available directly in the browser.

For those workstations that we manage, we will begin rolling out the Internet Explorer 7 update slowly over the upcoming weeks. If you have any questions please give us a call!

Spam By The Numbers

$11,000,000
The amount awarded to EarthLink in a spam lawsuit against a bulk mailer.
Source: The Register

TWO
The number of spammers EarthLink claims it is responsible for sending to jail since it began pursuing legal action. *Source: The Register*

$12,800,000
The amount still owed to AOL by a convicted spammer, David Hawke.
Source: MSNBC

$600,000
The estimated monthly earnings at the peak of Hawke's spam operations. That's a cool $7.2 million a year!
Source: MSNBC