

# SECURITY Smart™ NEWSLETTER

SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

## Avoiding Social Engineering Scams

**WHAT THE AVERAGE PERSON** might call a con is known in the security world as social engineering. Social engineering means tricking a victim into divulging sensitive information – especially computer passwords – or otherwise providing access to someone who shouldn't have it. What do social engineers want? Ultimately, the goal is usually money. Bank account numbers and personal identification numbers are good targets, but sometimes a social engineer will ask for less obviously valuable information.

Most of the time the trick involves posing as someone else in order to gain the victim's trust.

Social engineering made the newspapers a lot in the mid-1990s, most famously when the FBI chased down a famous computer hacker named Kevin Mitnick. While the term may not show up in the headlines as often these days, that doesn't mean these tactics have been laid to rest.

Today there are more ways than ever for con artists to pull off their tricks.

Perhaps the simplest, classic social engineering tactic is to call a victim and pretend to be from tech support, asking



the target to “confirm” their network login. However, some scams get much more elaborate. Criminals will even take time to borrow your company's “hold” music on the phone and use it later to fool you in a phone conversation. They also use phone-number spoofing to

make a different number show up on the target's caller ID.

Other forms of trickery take advantage of your curiosity. Common e-mail lines include: “Someone has a secret crush on you! Download this application to find who it is!” and “Did you see this video of you? Check out this link!” Of course, the links take the unsuspecting victim to sites that can download viruses and other nasty stuff onto your computer.

What's the best defense against all social engineering scams? Caution! Always verify the identity of anyone who asks for your “help” in getting access to a building or network.

And remember, there is almost never a legitimate reason to provide your password when someone else calls or emails you.

# Cut Out the Middle Man

Could your network be open to an unwelcome visitor when you're online?

**The Internet is a marvel, but it's also vulnerable to threats.** One of the well-known tactics that could affect your surfing security is a "man-in-the-middle" attack.

The name defines it: Someone is hacking into your network, inserting his computer between yours and the server you want to reach to connect to a website. The man in the middle now sees whatever information you are communicating with that website.

If you're using your home computer, for example, the interloper could see your passwords, unencrypted credit card numbers or any financial data you transmit to your bank. If you're on a networked computer from work, the man in the middle potentially could access shared files, your corporate mail server or other databases.

This exploit is a risk for secure sockets layer (SSL), a protocol that's in place when you interact with a website that sends and receives sensitive data. If a little yellow padlock icon shows up in your tool bar, or if the website's URL begins with "https", you are conducting a

transaction over an SSL. (Do you shop online? You most likely use SSL.)

When someone launches a man-in-the-middle attack, he could piggyback onto a request you make to your bank, for example, invisibly making another request. Your transaction might go through just fine, but the middleman's might too, directing your money to someone else. He could also create a login screen that looks legitimate and asks you to input your password so he can record that before sending you to the actual site you are trying to reach.

Security experts believe this type of attack has been uncommon so far, when it comes to capturing information from SSL sessions. "The attack is hard to use and the attacker will need to have detailed knowledge of the application he is attacking," says Frank Breedijk, a certified information systems security professional at Netherlands-based Shuberg Philis. But as it has been discussed openly in security forums and is widely known, more hackers will continue to try to use it.

How can you protect yourself against a man-in-the-middle attack?

- 1 Be wary of using a peer-to-peer or ad hoc connection or one advertised as "Free Public Wi-Fi" in a place like an airport, coffee shop or library. It's simple for a hacker to set up his own laptop with a "free wi-fi" name and sit in the room waiting for the unsuspecting other patrons to log in. A legitimate store network should have the correct wireless server name posted behind the counter (where the sign can't be tampered with).
- 2 Upgrade to the most recent version of your Web browser.
- 3 Look for "green glow" in the URL line—the site name repeated on a green background just before the page URL—which indicates higher security in most situations.
- 4 As always, never answer unsolicited e-mails that request sensitive information.
- 5 Ask your IT staff how to optimize the settings on your PC for security.

## Before Checking In, Check It Out

New research finds variations in hotels' security and safety levels.

If you travel frequently for business or pleasure, you've likely noticed a wide disparity when it comes to hotel quality. Towel fluffiness and breakfast buffet offerings are obvious differentiators, but have you ever considered the quality of a hotel's safety and security features?

A new hotel management research study from Cornell University's Center for Hospitality Research finds that safety and security equipment in U.S. hotels varies dramatically by size, location and overall hotel class. The report defines safety as meaning protection of a guest's person, while security additionally involves protection of a guest's property. The safety features that earned a hotel high marks included sprinklers and smoke-free rooms; desirable security features were electronic locks, interior corridors and an in-room safe. Safety materials, a safety video and security cameras also contributed points to the hotels' scores.

The study concludes that gaps in security and safety equipment are most evident in small hotels, or those with fewer than 50 rooms, as well as budget-priced and relatively old hotels. Luxury and upscale hotels, airport and urban hotels, large properties, and new hotels generally provided key safety and security features. So if you're given the choice of staying at the C'mon Inn to save a few bucks, consider the security issues (how familiar you are with the area, and so on) before making your decision.

### Have a Nice Stay

While you're on the road, follow these tips for a safe hotel experience:

- ✓ When you make your reservation, ask if the guest-room doors have deadbolts. Request a room on the third floor: high enough for security but still accessible by fire ladder.
- ✓ At the hotel, use valet parking, or park close to the lobby in a well-lit area.
- ✓ If the clerk mentions your room number aloud at check-in, request another room.
- ✓ Use the in-room safe for valuables.
- ✓ Don't use your name when answering the room phone.
- ✓ Don't open your door to anyone without verifying with the front desk.

# Trash Talk

Time to throw out your old computer? Cell phone? Data storage devices? Woo-hoo! Getting the new gear is exciting. The retired equipment, however, can easily become an albatross. You can't simply toss your stuff in the trash, because in addition to the potential toxicity of their various components, there are the potential hazards of your personal or corporate data falling into the wrong hands. But what to do—besides hide the albatross in an upstairs closet and hope someone else will take care of it? (No snickering: The Environmental Protection Agency reports that approximately 235 million units of electronic products had accumulated in storage as of 2007. The Institute of Scrap Recycling Industries expects that number to reach 400 million by the end of the decade!)

## Be Free

Before you free yourself of that old gear, make sure the gear is free of you. Get all your personal and work info out of electronic memory. Here's the catch: You have to do more than delete.

### How to cleanse your computer

It's important to delete all the data you can, but most of it still lives out of sight on the hard drive. That's why you need to take one of these steps:

- ▶ Erase data using a magnetic method. So-called "degaussing" devices are expensive and are usually operated by disposal services. This method is particularly good for removable media such as tapes, disks and thumb drives.
- ▶ Run a program to overwrite the entire hard drive. Free versions for personal use are available online (check out [www.killdisk.com](http://www.killdisk.com)).
- ▶ Physically remove and destroy the hard drive by perforating or shattering it. Obviously you can't reuse or resell it afterward.

Any of these methods should be repeated more than once.

### How to cleanse your phone

Mobile phones are simpler to erase than computers. Here's what you can do:

- ▶ Refer to your owner's manual. (You remember where you put it, right?)
- ▶ Contact your service provider or manufacturer for instructions.
- ▶ Find erasing instructions online. Check out [www.recellular.com](http://www.recellular.com) to get started, or go to [www.wirelessrecycling.com](http://www.wirelessrecycling.com) and look for phone data eraser.

## Letting Go

Now that your equipment has forgotten everything it ever knew about you, it's time to say goodbye. There are three routes to unburdening yourself of old electronics:

- ▶ Donate to charity or schools.
- ▶ Sell to other individuals or businesses.
- ▶ Send to a recycling facility.

## Be Responsible

It might seem more secure to destroy e-relics than to go through the erasing rigmarole, but the ingredients that make electronics so powerful can be poisonous when they are spewed into the air or seep into the water table.

E-waste is the fastest-growing component of the municipal waste stream worldwide, according to the National Resources Defense Council. Lead, cadmium, mercury, chromium and polyvinyl chlorides are some of the worst pollutants. That's why it's important to find a reputable recycler to handle your cast-off electronics. The Telecommunications Industry Association exhorts you to get written certification of data removal from your recycler. Whether it's a municipal collection center or a commercial enterprise, ask questions to be sure they are cleansing your data appropriately and disassembling and recycling the hardware, not just shipping it out to a landfill in China.

### DID YOU KNOW?

Discarded TVs, computers, peripherals (including printers, scanners and faxes), mice, keyboards and cell phones totaled about **2.5 million tons** in 2007.

Source: U.S. Environmental Protection Agency

## Recycling Resources

Time to put your computer or mobile phone out to pasture? Check these sources to find out how to do it right:

- ▶ To compare data wiping programs: [www.howtowipeyourdrive.com](http://www.howtowipeyourdrive.com)
- ▶ To find charities that accept donated electronics: [www.ebay.com/rethink](http://www.ebay.com/rethink)
- ▶ To locate an electronics recycler near you: [www.epa.gov/ecycling](http://www.epa.gov/ecycling)
- ▶ To locate recyclers that have pledged to handle materials responsibly: [www.e-stewards.org](http://www.e-stewards.org)
- ▶ To learn what questions you should ask your recycler/disposal company: [www.ecyclingcentral.com/faqs](http://www.ecyclingcentral.com/faqs)

# Keep employees—and your company—safe.

From the editors of CSO magazine, *Security Smart* is a quarterly newsletter ready for distribution to your employees—saving you precious time on employee education! The compelling content combines personal and organizational safety tips, so it is applicable to many facets of employees' lives. Using our editorial and design expertise the newsletter has an easy to read design with multiple entry points so you are assured that your intended audience of employees—your organization's most valuable assets—will read and retain the information. Sign up today to start having this newsletter distributed as a key tool in raising security awareness within your organization.

**To meet the security education needs of organizations of all sizes, *Security Smart* is available in a variety of formats and programs.**

## ELECTRONIC DISTRIBUTION PROGRAMS

### PDF Distribution

Via single e-mail to an individual, then distributed internally

- 1-500 employees \$995/year
- 501-1,500 employees \$1,255/year
- 1,501-5,000 employees \$1,675/year
- 5,001-10,000 employees \$2,395/year
- 10,001+ employees \$3,145/year

\$ \_\_\_\_\_

### Web-hosted fee

Link provided to a unique website that hosts the newsletter in PDF format

- Add \$500/year to PDF distribution subscription fee

\$ \_\_\_\_\_

## PRINT DISTRIBUTION PROGRAMS

### Printed (bulk ship)

- 1-500 employees \$2,249/year
- 501-1,500 employees \$2,649/year
- 1,501-5,000 employees \$7,495/year
- 5,001-10,000 employees \$14,995/year
- 10,001+ employees call for pricing

\$ \_\_\_\_\_

### Printed (drop ship)

- Add \$45/1,000 copies/U.S. location to print subscription fee

\$ \_\_\_\_\_

## CUSTOMIZATION OPTIONS

### Custom Branding (flat fee)

Electronic or print distribution

- Add \$695/logo and 50-60 characters of text

\$ \_\_\_\_\_

### Promotional Code

\_\_\_\_\_

### TOTAL

\$ \_\_\_\_\_

## Sign me up!

To order, fill out this form and fax or e-mail to Security Smart at 508.879.6063 or [cso\\_marketing@cxo.com](mailto:cso_marketing@cxo.com), or call 888.455.4646 with any questions.

### Billing Address

Company Name \_\_\_\_\_

Street Address \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ Zip \_\_\_\_\_

Telephone Number \_\_\_\_\_

Contact Name \_\_\_\_\_

Signature \_\_\_\_\_

### E-Mail Address (if electronic distribution)

\_\_\_\_\_

### Shipping Address (if print distribution)

Company Name \_\_\_\_\_

Attention \_\_\_\_\_

Street Address \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ Zip \_\_\_\_\_

Telephone Number \_\_\_\_\_

### Payment Method

- Charge my credit Card

Visa  Mastercard  American Express

Name on Card \_\_\_\_\_

Card Number \_\_\_\_\_

Expiration Date \_\_\_\_\_

Authorized Signature \_\_\_\_\_

Invoice Me

P.O. Number \_\_\_\_\_