

# FRONTLINE

FALL 2008

TIPS AND TECHNIQUES TO PROTECT YOUR INFORMATION

## INSIDE

### 2 Security Savvy

Test your knowledge after reading this issue.

### 3 Special Tactics

Protect your parents from fraud.

### 3 TopLine Management

Awareness trends from the 2008 CSI Computer Crime and Security Survey.

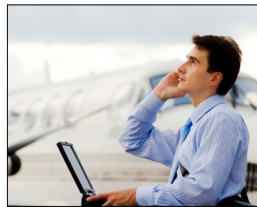
### 4 University of Missouri

New policy requires all employees to report security problems.

### 4 Horror Stories

Cybercrime headlines from around the world.

## Is the Data on Your Laptop Protected?



*Did you know that the laptop computer you lost could cost your company hundreds of thousands of dollars? Don't have a laptop, you say? Lost cellular phones, CDs and the pocket-sized portable storage drives you plug into your USB port might cost your organization just as much. The device itself is not costly; it's the data that is truly valuable.*

Consider all the information stored on your mobile devices. Does it contain addresses, birthdates, health insurance information or credit card numbers for your clients, customers or

employees? Respondents to the Computer Security Institute's 2008 Computer Crime and Security Survey said lost mobile devices containing this sort of personal information cost the organization an average of \$268,000 last year, spent on notifying people whose personal details were breached, paying fines and/or losing business because of bad press.

Do your laptop or other mobile devices contain information about your organization's finances, or details about new products or projects still in development? CSI Survey respondents reported that lost devices containing this sort of "proprietary information" cost those organizations an average of \$241,000 in lost business and other costs.

[Continued on page 2]

## Think Before You Speak, E-Mail, Blog

*Are you as careful with company secrets as you are with your own? During World War II, the armed forces created the adage "loose lips sink ships" to remind soldiers about the value of keeping military secrets safe. Although the war has long been over, similar principles apply today at your organization.*

When you are at the water cooler, a restaurant, on public transportation or even speaking to a coworker, it is important to be aware of who might be listening, and keep your lips sealed about future plans and sensitive information.

If you have knowledge about a possible layoff or merger that you wouldn't want the whole company to know of, or a new product you wouldn't want your competitors to know about,

then don't talk about it in casual conversation. This applies to the written word as well. Instant messages, out-of-office memos, social networking sites, blogs and personal Web sites are all places where you must guide your thoughts with personal censorship. Your organization may have its own policy about what is and what isn't appropriate for these messages as well.

Consider Alaska Governor Sarah Palin's e-mail mishap when her personal e-mail account was compromised. The hacker used the password recovery feature on her Yahoo e-mail to read her messages. Her security questions were birthday, zip code and "where did you meet your spouse?" The hacker simply performed a Google search to discover the answers. Once

[Continued on page 3]

So, whether you are traveling on business, taking work home with you or even just cleaning your desk, there are certain precautions you should take to protect your laptop computer, disks and cell phone, and the confidential information stored on them.

### Logging In

Some organizations require a password to log in to the computer. If your laptop is stolen, a thief wouldn't be able to log in to your machine if it is password-protected. For this reason, never write your password on a sticky note and attach it to your computer. More secure computers may contain thumbprint scanners. Scanners add another layer of protection because your fingerprint cannot be borrowed, lost or stolen.

### Encryption

Encryption is the process of transforming data to make it unreadable, unless you have the key to decipher the data and make it readable again. Encryption is like the cryptograms next to the crossword puzzle in the newspaper. A cryptogram is a puzzle in which each letter is replaced by a different letter or number, and you must decipher the code to solve the puzzle. The difference is an encrypted sentence is much harder to crack than a cryptogram.

You or your security administrator can encrypt either individual files (file encryption) or the entire device all at once (whole-disk encryption). Whole-disk encryption will also encrypt your metadata. Metadata is the data about the data, such as the date a file was created, file names, size of the file, etc.

Talk to your security department if you are unsure of how your data is being protected.

### Prevent Laptop Theft

- Before your travels, assess whether or not the information you carry on your laptop and other mobile devices is necessary. If not, ask your information technology department for advice on where it can be properly stored.
- When traveling with your laptop, be aware of your surroundings. There are a multitude of locations where travelers can misplace their devices, including taxis, airport security checkpoints, departure gates, restrooms, restaurants, lounges, stores or ticketing kiosks.
- Allow enough time to get where it is you are going. If you're too busy worrying about the time, you're more likely to lose track of your items.
- Know whom to contact if your work laptop is lost or stolen. Read your organization's policy or ask your information technology department to find out.
- Treat your laptop like you would a big wad of cash. You wouldn't leave that lying on a desk in your hotel room, would you? Use cable locks to protect your laptop from theft.
- Consider purchasing a laptop tracking service. If your laptop is stolen, the software is able to track the stolen computer and provide information to the authorities to get it back and apprehend the thief.

FL

## SECURITY SAVVY

Test your knowledge after reading this issue.

1. How does encryption protect you?
  - a. Encryption protects you from phishing messages.
  - b. Encryption renders your data unreadable to attackers.
  - c. Encryption scans your computer for viruses.
  - d. All of the above.
2. Where is it okay to post sensitive work-related information?
  - a. Facebook or LinkedIn profile
  - b. Blog or microblog (like Twitter)
  - c. Personal e-mail message
  - d. None of the above
3. What is one tool you can use to protect the *physical* security of your laptop?
4. How does your organization protect sensitive information on your laptop?

1. b. Encryption renders your data unreadable to attackers.  
 2. d. None of the above. It is never okay to post sensitive business or personal information on the Web.  
 3. Use cable locks to provide physical security for your laptop.  
 4. Your organization may protect sensitive data with password protection, encryption or biometric scanners. Read your organization's policy or ask your IT department if you're not sure which method is used at your organization.

According to *Caring.com*, a Web site devoted to helping people care for their aging parents, "When it comes to scoping potential victims, experts say con artists tend to look for individuals who are home during the day to answer fraudulent telemarketing calls, retired people who are hoping for one more shot to increase their nest eggs and those who will be too proud to admit they were 'had' and report that they were victimized to the authorities." Despite these trends, there are steps you can take to help protect your parents from becoming victims.

### Phone Scams

Criminals may call your parents and entice them to spend their money on investment schemes, vacation clubs or sweepstakes. A stranger who calls to ask for your personal or financial information should be treated with caution. Register your parent's phone number with the national Do Not Call Registry at <https://www.donotcall.gov/default.aspx>. Take note that researchers conducting surveys are not bound by the Do Not Call Registry. Although there are legitimate surveyors, be cautious of "pretexters" who are out for your parent's personal information. A pretexter will lie about his or her identity or purpose to ask your parents personal questions. Once answered, the pretexter may use the sensitive information to commit identity theft, financial fraud or theft by calling your parent's financial institution or workplace pretending to be them.

### Identity Theft

If criminals do obtain your parent's information such as Social Security, bank or credit card account numbers, they can steal your parent's identity, including opening new accounts, making purchases on victims' credit cards or opening loans in their names. Encourage your parent's to keep an eye on their bank balances and credit ratings to look for suspicious activity. Visit [annualcreditreport.com](http://annualcreditreport.com) for a free copy from each credit bureau: Experian, Equifax and TransUnion. Advise your parents not to make any investments or estate planning changes without consulting their financial advisor first. If your parents require any household help, encourage them to run a credit check on hired personnel or hire them through an agency that will run one.

### Internet Fraud

Inform your parents not to open e-mails, download files or click on links from people they do not know. Criminals will target your parents with phishing scams (e-mails designed to trick people into revealing their personal information). Scams related to prescription drugs or health information are especially popular and effective among criminals. In order to prevent malware from infecting your parent's computer, check that their anti-virus software is installed and activated. Also, set their spam filters and Internet browsing security settings to the highest level to protect them from downloading malicious files. **FL**

### Think Before You Speak, E-Mail, Blog

the messages were accessed, the hacker discovered that, although none of the messages contained particularly incriminating information, Palin *had* discussed government business through her personal e-mail account. This is a good case study to learn from: be sure to create unique security questions, do not post your sensitive personal or business information and do not use your work e-mail as a personal e-mail.

Electronic eavesdropping is the latest trend in corporate espionage. There can be several harmful ramifications of sharing sensitive information on social networking sites, blogs and forums. There are people whose sole job

responsibility is to surf the Internet to spy on organizations and employees. Be selective about the people you add as your friends on social networking sites, and be cautious of revealing too much information about yourself and your organization too quickly.

Several company leaks occur from preventable human error. Be aware of shoulder surfing on public transportation where other passengers could read your confidential documents. Use a privacy screen on your laptop to prevent people from looking over your shoulder. Always remember to lock your laptop, even if stepping away from your computer for a minute. **FL**

[Continued from page 1]

Security is everyone's job, but are you properly training everyone to do that job?

Over 500 security professionals responded to the 2008 CSI Computer Crime and Security Survey that asked what steps they have taken to secure their organizations. When asked what percentage of the security budget was allocated to "awareness training"—education for all employees about best security practices—42 percent of respondents said they spent less than 1 percent of their security dollars on awareness programs. Thirteen percent of respondents aren't even sure how much of the security budget is spent on awareness training.

The survey also asked about measures organizations had adopted to gauge the effectiveness of their security awareness training programs. Four out of five respondent organizations do train employees about security risks and appropriate handling of sensitive data. However, 32 percent of respondent organizations do not measure the effect this training has on the organization. Those that do evaluate awareness training measure the volume and type of incidents (18 percent), volume and type of help desk issues (17 percent), staff reports of experience (23 percent), social engineering testing (14 percent) and mandatory written/digital test (36 percent).

Security is everyone's job. The return on investment of awareness training outweighs the costs when you factor in the monetary losses of proprietary information due to breaches of customer and employee confidential data.

The full 2008 CSI survey results will soon be available at [GoCSI.com](http://GoCSI.com). Visit [GoCSI.com](http://GoCSI.com) to download your free copy.

# New Policy Requires All Employees to Report Security Problems

IT Security issues are the responsibility of everyone. You can help protect the University and its resources by complying with the mandatory reporting requirement. University employees are required to report all suspected information security incidents and weaknesses. Issues should be reported to your departmental IT person and/or the Division of IT as appropriate.

Examples of information security incidents and weaknesses include:

- A known or suspected compromise of a computer system, application, or database
- E-mail containing confidential information sent to the wrong recipient(s)
- Known uses of insecure (weak) passwords or sharing of passwords
- Unauthorized or old accounts within a computing system or database
- Physical theft or loss of computer or storage device
- Missing reports or printouts that are known to contain confidential information

Read additional examples and details in the mandatory reporting requirement. ([http://www.umssystem.edu/ums/departments/is/infosec/hr\\_mandatory\\_reporting.shtml](http://www.umssystem.edu/ums/departments/is/infosec/hr_mandatory_reporting.shtml)).

These issues should be reported to [abuse@missouri.edu](mailto:abuse@missouri.edu) or by calling the appropriate help desk below:

- MU/UM employees should call the Division of IT help desk at (573) 882-5000
- UMHC employees should call the ITS help desk at (573) 884-4357

All reports will be handled in a timely and professional manner.

More information about other commonly reported issues can be found below. If you have any questions please contact [isam@missouri.edu](mailto:isam@missouri.edu).

Report all threats to persons or property immediately by calling the MU Police Department at (573) 882-7201 or Emergency Services at 911.

## Horror Stories

If you find yourself wondering why today's managers and security departments are concerned about employee security behaviors, take a look at today's headlines. These selected stories from around the globe make it clear that there are lots of good reasons to be careful.

### **SOCIAL ENGINEERING CRACKED PALIN'S E-MAIL**

Details describing how someone hacked into Sarah Palin's Yahoo Mail account emerged on Thursday, and it appears to have been done with little more than social engineering, the process of acquiring personal information through social manipulation.

—CNET News, 9/18

### **SCAMMERS REPLACE CREDIT CARD READERS IN IRISH STORES**

Fraudsters in northeast Ireland posing as authorized bank service personnel replaced credit card readers in retailers' stores with their own, capturing data that can be used to empty bank accounts and make purchases. As many as 10,000 credit and debit cards may have been compromised by the time authorities became aware of the scam late last week, said Jennie Chamberlaine, marketing manager for the Irish Payment Services Organization, on Monday.

—IDG News Service, 8/18

### **FEDS ARREST HACKERS OF TJX, OTHER RETAILERS IN HUGE CONSPIRACY BUST**

Eleven perpetrators allegedly involved in the hacking of nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers have been charged with engineering the largest hacking and identity theft conspiracy ever prosecuted by the Department of Justice. The case links several high-profile data breaches of the last two years—including TJX Companies, BJ's Wholesale Club, Barnes & Noble and Dave & Buster's—to a single group of conspirators.

—DarkReading, 8/5

### **DEATH NOTICES REMOVED FROM COUNTY WEB SITE**

Privacy concerns and identity theft fears prompted Maricopa County Recorder Helen Purcell to halt public viewing of death certificates on the agency's Web site. "There is so much personal information on them: a mother's maiden name, what they died from," Purcell said, adding that her office has been fielding complaints for years about the office's practice of posting death-certificate images. The office quietly took them down last month.

—The Arizona Republic, 9/10