

FRONTLINE

WINTER 2009

TIPS AND TECHNIQUES TO PROTECT YOUR INFORMATION

INSIDE

2 Security Savvy

Test your knowledge after reading this issue.

3 Special Tactics

Bad security is paved with good intentions.

3 Under the Microscope

Mobile phone fable.

4 University of Missouri

Don't let a computer virus get you down!

4 Horror Stories

Cybercrime headlines from around the world.

Financial Crisis Creating Insecurity?



A man approaches you at the office claiming to be a financial auditor. He sternly says he needs access to your boss's locked,

unoccupied office to retrieve an important back-up disk of files. You know that, in this fragile economy, your company is enduring financial strain. Do you let him in? Do you let him take the disk?

Anxiety over the financial crisis and fear of losing their jobs has made many employees more eager to please and thus more vulnerable to "social engineering." Social engineers manipu-

late people (not necessarily by using technology) to breach an organization's security.

To evaluate the security of their organization, some companies hire "penetration testers" to simulate the kinds of attacks a criminal might use. According to penetration testing company Errata Security, breaching a bank's physical security is a lot easier now in this struggling economy. Employees are reportedly too eager to cooperate with anyone claiming to be an auditor. In a recent penetration test of a mid-sized bank, Errata's chief technology officer David Maynor convinced employees that he was a federal auditor. He was allowed access to the branch manager's unoccupied office in order to "leave him a note." Maynor easily made off

[Continued on page 2]

Don't Acquire Bad Security

Many organizations are undergoing significant changes these days. In the midst of these adjustments, employee records, financial records and trade secrets may all need to be shared with new employees and/or moved to a new computer system. Whatever the degree of change within your own work environment, it's important to consider your role in keeping your organization's sensitive data safe even when change is in the wind and time is of the essence.

When organizations change course or through restructures, sales or mergers, good security practices need to be an integral part of the process. You may hear rumors of potential shifts within your organization that may directly effect you. Although this may be a frustrating time, it

is best not to increase the discomfort with office gossip. Imagine that you are having lunch with a coworker and you innocently mention a rumored merger. The information hasn't been made public, but a shareholder with your organization is sitting behind you and overhears the discussion. These rumors can spread like wildfire with lasting effects on your organization, and potentially you.

Similarly, do not post rumors about your organization on a social networking site, blog or microblog. It's not just bad policy, it could be cause for termination.

After the acquisition or merger, it's likely your data may need to be moved or shared. Now is a great time to take a look at your files and

[Continued on page 3]

with a back-up tape containing confidential account transaction data.

Another kind of social engineering attack known as “phishing” is done through e-mail. The United States Computer Emergency Readiness Team reported an increase in phishing scams related to the financial crisis. These scams frequently involve banks, savings and loans or mortgage lenders that recently failed or were acquired by other institutions.

JP Morgan Chase Bank posted several examples of these phishing messages on their Web site. To the right is an impressive example. It appears to be from Chase, it cites the correct date of Chase’s recent acquisition of Washington Mutual bank and even has the correct name of Chase’s chief marketing officer. This looks like a legitimate message, but you can tell that it is a phishing message because the sender asks you to click a link and update your personal and account information—something a real financial institution will never do.

Of course, social engineering scams do not just happen during times of crisis. Last year, a thief made off with over \$26 million worth of diamonds, and all he used to steal them was his charm. The thief stole 120,000 carats of diamonds from ABN Amro’s safety deposit boxes in Antwerp, Belgium. The thief posed as a successful businessman. He became a trusted trader, was given an electronic card to access the bank vault and then learned where the diamonds were held. Philip Claes, spokesman for the Diamond High Council in Antwerp said that the bank had been fitted with a security system costing more than \$1 million. Claes told the press that the lesson learned was: “despite all the efforts one makes in investing in security, when a human error is made nothing can help.” FL

From: Chase Online
 Sent: Friday, November 28, 2008 10:14 AM
 Subject: WaMu & Chase. Safe & Secure - Message id XLKLTRZBGW

WaMu customers: we're proud to welcome you to one of the nation's largest banks; as of September 25, 2008, all WaMu customer deposits are now deposits of JPMorgan Chase, one of the most stable banks in America.

What will change; Some aspects of the ONLINE SERVICES: Chase Online and WaMu Online

DEADLINE: December, 30, 2008
 What you need to do: Update your information by visiting Chase Online or WaMu Online. Log on to your account and you will be re-directed to the client information update screen.

If you have not signed up for online access, you can enroll easily by clicking “Enroll” at the bottom of the Login page.

Please do not reply to this message. For questions, please call Customer Service. We are available 24 hours a day, 7 days a week.

Sincerely,
 Carter Franke
 Chief Marketing Officer

©2008 JPMorgan Chase & Co

SECURITY SAVVY

Test your knowledge after reading this issue.

1. **The IRS demands to enter your boss’ office to retrieve a back up disk. Would you:**
 - a. Enter your boss’ office to retrieve the disk yourself and hand it over to the man.
 - b. Contact your boss to validate the legitimacy of the request.
 - c. Give the man the key to your boss’ office and tell him to take what he needs for the audit.
2. **True or False:** It’s okay to open a phishing message if it is addressed to you personally.
3. **Which of the following is a good security practice to follow?**
 - a. Hold the door open for strangers behind you when entering your office building.
 - b. Turn off your anti-virus software to speed up your computer and get more work done.
 - c. Save sensitive information onto a USB stick to work on the files at home.
 - d. Create a strong password.
4. **You receive an e-mail message from your bank offering to refinance your mortgage. The sender wants you to click a link to learn how much money you’d save. Would you:**
 - a. Click the link to see what they are offering.
 - b. Call the number provided within the e-mail to learn more.
 - c. Call the number of your bank that you are familiar with instead of the one listed in the e-mail.
 - d. E-mail the sender to learn more.

1. b. Several criminals try to pose as legitimate business contractors. Always ask your boss or calling the agency at a number you are already familiar with to verify their legitimacy.
 2. False: Even if a message is addressed to you, it could be a phishing message. See above for an example.
 3. d. Create a strong password. The other examples are bad security practices.
 4. c. A phone number listed in an e-mail could be a phone scam. Call a number you are familiar with to verify if the e-mail is legitimate.

SPECIAL TACTICS

Bad Security is Paved With Good Intentions

When making your New Year's resolutions, why not add "Practice better security" to your list? Do you save business files onto a CD or USB stick and take your work home so you can burn the midnight oil and finish that important project? Do you turn off the anti-virus software on your computer so it runs more quickly? Do you leave your personal e-mail or phone number on your outgoing voicemail message so you're always available?

Despite your good intentions, these are risky security practices. If you're not careful you might actually be a risk to your organization's security! Obviously, deceitful insiders may cause trouble, but the well-meaning insider can be just as damaging to an organization.

Your organization has established rules about the safe use of technology. Learn what those rules are and practice some of these security tips:

- Your CDs and USB flash drives (USB sticks) may seem harmless, but they might actually be security concerns. Portable storage devices like these are often lost...and you never know who might find them. It's best not to save confidential files—such as customer databases, financial records, research on products still in development—to a removable storage device. Some of this information could be a boon to competitors. Other information is protected by law; it could cost your

organization millions in fines or lost business if this information is lost or stolen. If you must store files on portable storage devices, ask your information security department about some of the latest, most sophisticated USB sticks on the market. Some can be "encrypted" so that thieves cannot read the files without a password. Others can even destroy the data on the drive after it's been lost!

- Never turn off your anti-virus software. These tools are in place to protect your data and should be activated at all times, even if they occasionally make e-mailing and file downloads take a little longer.
- Avoid "tailgating"—assisting an unauthorized employee through a secured entrance. Although you may think it is the polite thing to do, letting an unidentified stranger into your organization's office is bad security practice. You never know who you could be letting into your organization. Instead, simply make your apologies and direct them to the proper place for visitors to check in.
- Your computer isn't the only security concern. Your voicemail is also susceptible to attacks. Change your password frequently, delete messages after you have listened to them and never leave sensitive information in voicemail boxes. You never know who may be listening. **FL**

Don't Acquire Bad Security

folders. Work files do not belong on your home computer or on a USB stick. Instead, those files should remain protected on your office computer.

Where are your work files saved: your desktop, laptop, or a shared server? Take a moment to consider the ramifications of the loss or theft of your laptop. Such a disaster could not only cause a data breach, but imagine all of the work to recreate. In most cases, if there is sensitive information stored on your laptop, and it is stolen, there are reports to complete, managers' questions to answer. Your privacy and legal department may even have some of their own. Instead, be sure to create backups

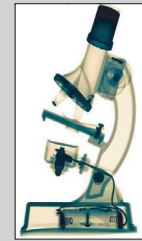
that you store in a securely locked location, or save your files to a shared server.

Now is also a good time to review your organization's policies. Do you know the current disaster recovery plan in case of an emergency? Or what off-site storage facility now maintains your organization's backup files? Will you need to transfer your customer data or sales leads into a new computer program? How does this new program secure that information? These are just some of the questions you should begin to ask yourself during this time of transition. It's a long road, but security can actually be improved, one step at a time. **FL**

[Continued from page 1]

UNDER THE MICROSCOPE

MOBILE PHONE FABLE



On Nov. 20, executives at Verizon Wireless officially apologized to Barack Obama after a number of Verizon employees accessed and viewed an inactive account for Obama's former personal cell phone. Although the phone account was no longer active, these employees face disciplinary action, and the incident highlights the importance of mobile phone security.

It is uncertain whether or not all the Verizon Wireless employees had authorized access to Obama's inactive account records. Fortunately, the employees could not have accessed any text messages or voice mail.

Though you cannot control what your phone provider does with your phone records, you can ask your phone provider some questions about how they secure and destroy your account information and phone records.

Also, you can look out for the security of your phone itself. Inside your mobile phone is a "SIM card," which is where information such as your contacts, your calendar, your text messages and your photos are stored. Sometimes when you get a new phone you can take your SIM card from your old phone and put it right into the new one. If, however, you cannot reuse your SIM card, erase all the data before returning it to your phone service provider. It is also a good idea to return your old phone to the retailer—don't throw it in the trash where just anyone can find it.

Don't Let a Computer Virus Get You Down!

One way to keep your computer healthy is to use anti-virus software. By keeping your computer virus free you're not only protecting your system – you're also protecting all the computers that share your network.

Anti-virus programs scan for and automatically remove worms, viruses and trojan horses. These various computer programs can be very damaging to your computer. Anti-virus programs work by comparing computer files against a file containing known virus components (called the virus definition file). The virus definition file is updated regularly because new viruses are created every day.

Your department's IT Professional has most likely installed anti-virus and scheduled updates for your University system. If you are unsure or have questions about the settings, please contact them.

For your personal systems, the Division of Information Technology provides, free of charge, Symantec Endpoint Protection software for Windows, Norton's for Mac. This software is available for download via the [IT Software Distribution Site](https://elms05.e-academy.com/missouri/) (<https://elms05.e-academy.com/missouri/>) for all faculty, staff and students. Although many new computers come with a version of anti-virus software, the version is usually only a trial and will expire. The user must remember that once the trial version is expired their system is vulnerable for attacks and viruses.

So don't let a computer virus get you down, use anti-virus software and make sure to keep it current. Your computer will thank you.

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.

FACEBOOK HIT BY NIGERIAN 419 SCAM

Normally, 419 scams are easy to spot and involve e-mail requests for money from supposedly rich individuals in countries such as Nigeria, from which the fraud gets its name. The latest Facebook attack is much craftier, however, because it hijacks the identities of real people known to Facebook members, asking for money under an apparently plausible guise.

–NetworkWorld, 11/10

OBAMA, MCCAIN WEB SITES HIT BY HACKERS

The campaign computer systems of President-elect Barack Obama and Republican Presidential candidate John McCain were targeted in a malicious phishing attack launched by foreign hackers, Newsweek reports. The Newsweek report on the phishing attacks came just two days after the 2008 U.S. Presidential election, in which Obama won the Presidential race in a sweeping victory at the polls Nov. 4.

–The Register, 11/7

MCDONALDS SURVEY SCAM: SUPER-SIZE FRAUD

Phishing fraudsters are attempting to scam the credulous into handing over their credit card details on the basis of a supposed offer from McDonalds. The scam relies on spam e-mails to trick burger scoffers into answering a fictitious satisfaction survey that offers a non-existent reward of \$75. After completing the quiz prospective marks are asked to hand over their banking details in order to receive their reward.

–The Register, 12/1

'HUGE INCREASE' IN WORM ATTACKS PLAGUES UNPATCHED WINDOWS PCS

A computer worm that exploits a Windows bug Microsoft Corp. patched more than two months ago continues to wreak havoc, a security company said today, as it boosted its overall threat ranking and warned users to patch their PCs.

–ComputerWorld, 1/12

CHECKFREE CUSTOMERS REDIRECTED TO UKRAINE SITE

Customers of CheckFree.com, an online bill paying site, were quietly redirected to servers in Ukraine early Tuesday morning, according to several reports. Representatives of CheckFree told WashingtonPost.com that customers were redirected to a blank log-in page that attempted to install malware on the visiting PC.

–CNET News, 12/4

INSIDERS NEW THREATS IN DOWN ECONOMY

Rene Rebollo was strapped for cash. One day, while working in his office at the Pasadena branch of Countrywide Home Loan, he noticed one computer in the building whose USB port hadn't been disabled by the company's IT department. Then, according to FBI affidavits, Rebollo got an idea. Every Sunday night for approximately two years, Rebollo went over to that workstation and downloaded confidential data on as many as 20,000 Countrywide customers to a small USB drive that he could carry out of the office in his pocket.

–DarkReading, 12/4