

FRONTLINE

SUMMER 2008

TIPS AND TECHNIQUES TO PROTECT YOUR INFORMATION

INSIDE

2 Security Savvy

Test your knowledge after reading this issue of FrontLine.

3 Special Tactics

Five security practices for work and home.

3 TopLine Management

PCI 6.6 requirement.

4 University of Missouri

Make IT safe – protect your password!

4 Horror Stories

Cybercrime headlines from around the world.

Security Sweets: Password Protection



According to a London survey, 21 percent of people would give up their password for a chocolate bar.

The survey was conducted by the organizers of Infosecurity Europe, an information security event. Posing as market researchers, they interviewed 576 office workers in London. This year's results were significantly lower than last year when 64 percent revealed their password. Either people are becoming more security-savvy or they're trying to watch their weight. Respondents were also asked about their use of passwords at work, and half said

they knew one or more of their coworkers' passwords. More than half of respondents used the same password for all of their accounts (home and work) and 43 percent of people rarely changed them. Those that used several passwords often wrote them down and hid them in a desk or in a document on their computer. Most people used familiar proper nouns like family names, pets and football teams as the basis for their password. In other words, they created them to be easy to remember, but also easy for a criminal to discover. All of these practices put your information in jeopardy.

The surveyors did not verify the authenticity of the passwords, so hopefully respondents were

[Continued on page 2]

Free Public WiFi?

Jennifer was recently in the airport traveling on business, and thought she'd use the time to do some work on her laptop. When she pulled up the network connections available to her, she saw one titled "Free Public WiFi." She thought perhaps the airport was offering this free network connection as a service to its customers.

The truth is, it's a scam. "Free Public WiFi" is likely not a legitimate network connection, but rather one that connects your computer to a stranger's computer. This one-to-one connection is termed an "unsecured computer-to-computer network," and it can mean trouble.

Most employees no longer work within the security of the office firewall all the time. With

more organizations striving to go green and travel less, more workers are working from home, remote offices or even coffee shops. Employees that travel pick up wireless connections at airports and hotels, along with computer viruses. It's important to know which wireless connections are safe to connect to and which you should avoid.

If you see "Free Public WiFi" as a network option, do not connect to it. A computer-to-computer network is controlled by another user's computer and connecting to it could allow an attacker to gain direct access to your computer. This makes it easier for the attacker to install viruses, peek at the sensitive data in your files or steal your organization's upcoming project ideas.

[Continued on page 3]

only giving away a fake password in return for free chocolate. Even if you don't get a Cadbury, it's an important opportunity to evaluate the strength of your passwords.

There are three ways to prove you're allowed access:

1. Something you know (login and password).
2. Something you have (access card or key).
3. Something you are (fingerprint or retina).

Some computers are installed with "biometric" scanners that require you to scan your finger, palm or even eye to recognize you as an authorized user of the machine. While this technology offers another layer of defense, it is not yet widely available. Since most organizations currently use only the first type of security to authenticate users, it is even more important to have a strong password.

A strong password includes:

- at least eight characters.
- at least one number.
- at least one special character, such as @ # ! & \$.
- a mix of upper case and lower case characters.

Security professionals have a way to measure the strength of passwords, which they express in terms of "bit strength." The greater the number of characters in a password, the more protection a password affords. If you create a password utilizing these tips, but it is only six characters in length, your bit

strength is 39 bits. Compare that to a password that is eight character in length and your bit strength increases to 52 bits; a big difference for only two more clicks of a finger. Just remember not to make your password so long that you need to write it down to remember it.

Not only is the length of your password important, but so is the randomness of the characters you choose. Avoid using the most common number, "1," the most common letters, "a," "e," "o" and "r," and passwords based on dictionary words, names, government-issued ID numbers or dates.

The best way to combine all of the above is to use a passphrase based on your favorite book, song, TV show or other phrase that will be easy for you to remember. Let's say your favorite book is *Harry Potter and the Sorcerer's Stone*. Take the first letter of each word, and you're left with HPatSS. Replace some of the letters with numbers and special characters that look similar to the letter, such as HP@t55. This passphrase serves as the base for each of your passwords.

To create a unique password for each of your Web accounts, tack on two distinguishing identifiers to the end of your passphrase. For example, your Amazon account password would be HP@t55Am and your MySpace password would be HP@t55MS. And there you have it—a strong password that you can remember every time. FL

SECURITY SAVVY

Test your knowledge after reading this issue of FrontLine.

1. How many characters create a strong password?
 - a. At least 6 characters
 - b. At least 8 characters
 - c. The longer, the better
2. When entering your credit card information to make an online purchase, what Web address is an indicator that the data is being sent over a secure channel?
 - a. www.
 - b. http://
 - c. https://
 - d. url.com
3. Which wireless network is most likely to be a scam?
 - a. Hotel Lobby: Unsecured wireless network
 - b. Jane's Coffee Shop: Security-enabled wireless network
 - c. Free Public WiFi: Computer-to-computer network
4. What are the most common letters to avoid when creating a strong password?
5. What are the three ways to prove you are allowed access to data?

1. b. Your password should be at least 8 characters. If it's too long you may be tempted to write it down.
 2. c. Remember https:// where "s" stands for "secure channel."
 3. c. Free Public WiFi is an unsecured computer-to-computer network that you should not connect to.
 4. The most common letters to avoid when creating a password are "a," "e," "o," "r," and "1."
 5. 1. Something you know. 2. Something you have. 3. Something you are.

SPECIAL TACTICS

Five Security Practices for Work and Home

1. Protect your personal information

A criminal that has your personal information can access your financial accounts, credit records and other assets. Anyone can be a victim of identity theft.

- ❑ Do not open e-mail messages from people you don't know. Instead, use your preview pane to see whether the message is from a legitimate source.
- ❑ Never respond to solicitations for your personal or financial information.
- ❑ When shopping online, one indicator that a merchant has taken steps to secure a Web site is the URL that begins with "https://". This URL signifies that your credit card data is being sent across a secure channel to protect your data.

2. Be a good cyber citizen

- ❑ Secure your Web browser, like Internet Explorer or Firefox, by increasing your online security. Check "Tools" then "Options" to find your security features.
- ❑ When posting on social networking sites, bulletin boards, chat rooms, instant messages or even e-mail messages, act the same way you would act in front of your grandmother: polite, considerate and without malice.
- ❑ Read the terms of agreement before checking that little box when you register for a new account. Although most people never read the terms, it's not a bad idea to

do so to see how your personal information will be stored, who will be accessing it and how it will be used.

3. Keep a clean desk

Having a clean desk not only looks more professional, it also protects you from nosy neighbors and untrustworthy passers-by.

- ❑ Always put paperwork in folders stored in a locked drawer and never leave out papers containing confidential information.
- ❑ Never write your password on sticky notes, or other papers lying on your desk.
- ❑ Keep the keys to your locked drawers and computer in a secure place—not in an unlocked drawer.

4. Guard printers and fax machines

When printing or faxing confidential or sensitive documents, it is best practice to wait at the machine until the entire document is printed or the fax has gone through. Do not leave papers behind because you never know who will be the next person to pick them up.

5. Lock it up

A lost laptop or other mobile device is the number one cause of data breaches for organizations. Keep your laptop physically locked as well as locking your computer screen every time you step away from it. The same goes for your backups. Keep them securely locked away instead of sitting on your desk. **FL**

Free Public WiFi?

Wireless security isn't just a concern at the airport. A home user is also responsible for securing a wireless network with a password so that only responsible parties can access the connection. If you obtain wireless access with a router and your connection isn't password-protected, any one of your WiFi-enabled neighbors can access it. If you live in a highly populated city, there can be a lot of intruders leeching off your bandwidth, thus making your computer run slower.

An unauthorized user could abuse your home connection by hacking into your computer to distribute illegal material such as pirated software, or worse yet, to spread a virus. Since the criminal is part of your network, communication between him and the Internet will appear to be coming from you. According to

most Internet service providers, the fine print will hold *you* responsible for any illegal activities the criminal engages in while using your wireless connection.

The network is like a backdoor into your computer that allows a hacker to search for your personal information, sniff out your passwords and even gain access to your corporate network. He or she can piggyback onto it and gain unauthorized access to your organization's resources which could lead to an embarrassing security breach. A simple way to help minimize your risk is to change the default password on your wireless router. Also, read the manual that came with your router to learn about wireless security protocols that can add further protection to your network. **FL**

As of June 30, all businesses that store, process or transmit cardholder data must secure their public-facing Web sites against Internet attacks. Requirement 6.6 of the Payment Card Industry (PCI) Security Standards Council has made it clear that credit card companies will only do business with vendors who comply to these security standards. The requirement was created to prevent losses and breaches of clients' personal information. If a compromise does occur, the organization will be found non-compliant if protective measures were not taken to secure the Web site.

Organizations must find and fix vulnerabilities on the Web site that accepts credit card transactions. If the organization is unable to perform this work in-house, they may consider hiring a third-party company that specializes in Web application vulnerability assessment or scanning. If the organization is not protected, neither are their clients.

Another option is to purchase specialized Web security tools. One such tool is a Web Application Firewall (WAF) which acts as a barrier between the organization's Web site and the client's computer. The council provides a list of acceptable devices and how they should be deployed and configured.

Whether you hire a third-party or install a new tool, be careful as to whom or what you select. It is the organization's responsibility to prove that the tools, people or firms employed to fix vulnerabilities are qualified and can pass an auditor's or bank's inspection.

The council is giving organizations the choice to implement one of the two requirements based on budget constraints, but proper implementation of both provides the best defense.

[Continued from page 1]

Make IT Safe – Protect Your Password!

To help protect University resources (and your personal information), practice secure behavior and treat your password like your personal signature. Follow these three tips to help protect your password.

- 1. Never share a password or personal identification number (e-mail, voice mail, or otherwise).** There are almost always other ways of granting access to data and systems if there is a legitimate need to do so. If you need to grant access to others but are unsure of how to do so, check with the Division of IT Help Desk or your Departmental IT Professional. **The Division of IT will never ask for your password. If you receive an e-mail asking for your University password, it is a scam. Never send your password via e-mail.**
- 2. Don't write your password down** – doing so increases the chances of someone finding it and accessing your account or the network. This includes storing passwords in cellular phones, on sticky notes taped to your monitor or slipped under your keyboard. These are common places where people keep their passwords written down and also common places where people would look to find yours.
- 3. Change your password on a regular basis.** Faculty/staff can use the Password Manager. (<http://doit.missouri.edu/password-manager>) Students can use MyZou. (<http://myzou.missouri.edu>)

The University has very specific password requirements to protect its data. To ensure complexity, all passwords must have eight to 26 characters and include at least one character from at least three of the following:

- Lowercase letters: a - z
- Uppercase letters: A - Z
- Digits: 0 - 9
- Special characters: ? , _ - ~ + = \$!

A password cannot:

- Be a word found in the dictionary
- Be the same as your PawPrint
- Contain MU-related terms (tiger, Truman, Jesse, etc.)
- Contain spaces or symbols other than the special characters above
- Contain personal or directory information (Social Security number, employee ID, etc.)

Practicing these three security tips can help protect the confidentiality of your password, which can protect the University resources you access.

Do your part – help the Division of IT **Make IT Safe!**

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.

STANFORD EMPLOYEES' DATA ON STOLEN LAPTOP

Stanford University has notified tens of thousands of past and current Stanford University employees that their personal information-including their dates of birth, Social Security numbers and home addresses-was on the hard drive of a stolen university laptop. A Stanford spokesman said Saturday that the stolen computer contained personal information on people hired by the university before Sept. 28, 2007, which could be as many as 72,000 people.

–San Francisco Chronicle, 6/8

LOST CAMERAS 'PHONE HOME' TO CATCH THIEVES

Alison DeLauzon thought the snapshots and home videos of her infant son were gone for good when she lost her digital camera while on vacation in Florida. Then a funny thing happened: her camera "phoned home." Equipped with a special memory card with wireless Internet capability, DeLauzon's camera had not only automatically sent her holiday pictures to her computer, but had even uploaded photos of the miscreants who swiped her equipment bag after she accidentally left it behind at a restaurant.

–Reuters.com, 6/6

ARMY HOSPITAL BREACH MAY BE RESULT OF P2P LEAK

Peer-to-peer (P2P) applications may have been the culprit in a security breach that has exposed the personal information of more than 1,000 patients at Walter Reed Hospital, according to early reports. Names, Social Security numbers, birth dates and other information was exposed through a single computer file, hospital officials said Monday. The file did not include information such as medical records, or the diagnosis or prognosis for patients, they said in an Associated Press report.

–The Register, 6/3

GEORGIA PATIENTS' RECORDS EXPOSED ON WEB FOR WEEKS

A company hired by the state of Georgia to administer health benefits for low-income patients is sending letters to notify tens of thousands of residents that their private records were exposed on the Internet for nearly seven weeks before the error was caught and corrected, a company representative said Thursday.

–CNET News, 4/11