

FRONTLINE

SPRING 2009

TIPS AND TECHNIQUES TO PROTECT YOUR INFORMATION

INSIDE

2 Security Savvy

Test your knowledge after reading this issue.

3 Special Tactics

The soft human target.

3 Under the Microscope

Data mining.

4 University of Missouri

Getting the security you need!

4 Horror Stories

Cybercrime headlines from around the world.

Data, Do No Harm



The Obama administration has made it clear that, due to the rising costs of health care, the country will be implementing standardized electronic medical records, and plans to spend \$19

billion to accelerate the use of computerized medical records in doctors' offices.

In a speech outlining his economic recovery plan, President Obama said, "We will make the immediate investments necessary to ensure that within five years all of America's medical records are computerized." His hope is that

electronic medical records will prevent errors, create jobs, and save lives.

In order for medical records to be shared electronically between doctors, hospitals and insurance companies, a system must be in place to store them. One such system currently in use is Google Health, an online platform that stores medical data from patients' home-based devices, such as glucose meters and blood pressure monitors. Medical professionals may then access the readings from the Personal Health Records systems.

The downside of this data portability is that the security and privacy of millions of Americans may be at risk. Especially alarming is that the

[Continued on page 2]

Stupidity for All Times in Perpetuity

According to *The New York Times*, Vaughan Ettienne, a New York City police officer and champion body builder, is considered to be polite and thoughtful in person. However, his online persona portrays a different personality.

One day in 2006, Ettienne posted the description of his mood on MySpace as "devious." This description was one of 122 moods he could have selected. The "devious" setting depicts an angry, red face surrounded by flames. The next day, Ettienne and his partner chased an ex-convict, Gary Waters, who was riding on a stolen motorcycle, and arrested him for carrying a loaded gun. Once Waters was on trial in New York State's Supreme Court in Brooklyn, he claimed that Ettienne and his partner stopped him, beat him, and then planted a gun on him to

justify breaking three of his ribs. What seemed like a simple case of gun possession became a contest centering on the truth about Ettienne's personality. Was Ettienne a diligent cop who found a loaded gun on an ex-convict? Or did Ettienne make up a "devious" story in keeping with his ruthless online character?

"You have your Internet persona, and you have what you actually do on the street," said Ettienne. "What you say on the Internet is all bravado talk, like what you say in a locker room." Jurors learned that weeks before the trial, Ettienne had also posted this status on his Facebook page: "Vaughan is watching *Training Day* to brush-up on proper police procedure." *Training Day* is a film starring Denzel Washington as a narcotics detective who pillages the city

[Continued on page 3]

creators of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, the current law that safeguards patient privacy) didn't anticipate electronic health records systems; HIPAA offers little to assure patient privacy and security under the new electronic environment.

On the upside: Congress is gearing up to revise health care privacy laws so that they apply to electronic health records as well. One possible solution would allow patients to add additional controls to protect sensitive information such as records containing a patient's mental health status or chronic conditions. In addition, health care providers and insurers may be required to use encryption technology to protect personal health information.

As you imagine your personal, medical information flitting around cyberspace unprotected, you may gain an appreciation for how your customers and fellow employees feel when they place their sensitive information in *your* care. Whether you touch sensitive customer data, such as credit card numbers and health records, or your co-worker's sales projections for next month, someone is counting on you to safeguard the information that is critical to them. Are you protecting sensitive information in your workplace as you would like your own personal medical records to be protected?

A few tips may help you think about security in a new way:

1. Pay attention to the security awareness messages that your organization publishes. The training they provide will educate you on sound security practices being employed by hundreds of organizations today. Staying current keeps you and your organization a step ahead.
2. Know where to go for security guidance. Whether it's your help desk, security staff, company policies, supervisor, or security portal of your intranet, find out what's expected of you and how your organization provides answers to your information security questions and concerns. Take advantage of the resources offered.
3. Learn how to distinguish between information that requires protection and information that doesn't. If your company uses a data classification system, learn it and use it. If not, you probably already know intuitively how to classify your data. Start now by making a mental list of five documents that probably deserve extra protection. You're probably right.
4. Step up to the plate. It's not someone else's job to protect the information that you handle, and it's not an *additional* job for you. Security is simply the way things get done in the year 2009. You're expected to be security savvy!
5. Talk it up. If you observe co-workers making poor decisions that affect security, or security flaws built into the way you do things, speak up. The more you practice thinking about security, the better you'll get at protecting critical resources.
6. Stay on top of it. During times of change, roles in the workplace can shift rapidly. You may be taking on new work and handling unfamiliar tasks. When you do, be on the lookout for any new sensitive information that comes your way, and learn how to protect it. **FL**

SECURITY SAVVY

Test your knowledge after reading this issue.

1. **How might you learn more about security?**
 - a. Help desk / security staff
 - b. Company policies / intranet security portal
 - c. Supervisor
 - d. All of the above
2. **True or False:** When you're online, you're anonymous.
3. **Which of the following may you safely post to your social networking site?**
 - a. Your payment card information for shopping convenience.
 - b. Your office and/or home address so that colleagues will know how to contact you.
 - c. Photos or discussions that would shock your boss.
 - d. None of the above.
4. **Which of the following is good security practice to follow to prevent a data breach?**
 - a. Organize, classify and secure your organization's sensitive information.
 - b. Turn off your anti-virus software so that your computer runs faster.
 - c. Read your organization's security policies and best practices.
 - d. Think about where your sensitive data is stored, and how you use and protect it.

1. d. All of the above.
 2. False.
 3. d. None of the above.
 4. a., c., and d. Never turn off your anti-virus software.

SPECIAL TACTICS

The Soft Human Target

The private medical records of Grady Memorial Hospital patients were made public on the Internet, not due to hackers, but because of human error. In July 2008, 45 patients' medical records were placed onto an unsecured site, open to the public, where they remained for a few weeks. The information included doctor's notes, the names and ages of the patients, their medical conditions, diagnoses, and medical procedures.

The error occurred because the Atlanta, Georgia hospital outsourced the job of transcribing the notes to a local firm, which outsourced the work to a Nevada contractor, who in turn outsourced the work to a firm in India. The error was discovered when a doctor at Grady Memorial Hospital performed a search of his own name on Google, and found the sensitive information of his patients posted on the Internet.

A data breach is the unintentional release of information to an insecure environment. While even the most secure organization can fall victim to a data breach due to intentional attack, the least secure organizations will almost certainly become breach victims. Breaches can be the result of keeping more sensitive information than needed for too long, providing more access than needed to too many employees, or not encrypting data.

The 2008 Data Breach Investigations Supplemental Report released from Verizon's

Business Investigation Response team, is a compilation of four years of data breaches from more than 500 cases. The report disclosed that many attacks are relatively cheap, automated, and anonymous for the criminals, because they are able to prey on employees who are not thinking about security:

"In the face of hardened networks and systems, criminals often set their sights on softer human targets." –Verizon's report.

Consider the following cases in which employees were not willfully deceitful; they simply weren't thinking about security:

- Several employees were granted resources and access privileges which they didn't need for their job, and ended up causing a breach by misusing those privileges without regard to the security ramifications.
- Employees forgot to enact proper security. The team's advice is, "Check, recheck, and check again."
- Viruses and other malicious code were more frequent when employees use their company e-mail for business *and* personal use.

It can be just one employee, with access to one spreadsheet of customer information, who neglects good security practices, can inadvertently cause a data breach. Don't let that employee be you. Make security intentional. **FL**

Stupidity for All Times in Perpetuity

he is supposed to serve and protect. Based on the defense lawyer's testimony, jurors decided that Etienne was trying to emulate the Washington character in the film.

"I'm not going to say it was the best of things to do in retrospect," said Etienne. "As the lawyer Ron Kuby says, stupidity on the Internet is there for everyone to see for all times in perpetuity." Officer Etienne said he has never been disciplined for brutality and is now being careful to mask his identity on the Web. "It paints a picture of a person who could be overly aggressive. You put that together, it's reasonable doubt in anybody's mind." Waters, on parole for a burglary conviction when

he was arrested, beat the most serious charge—the felony possession of a 9 mm Beretta and a bagful of ammunition. He was convicted on the charge of resisting arrest, a misdemeanor.

Etienne's case is just one recent example of how fun posts on your social networking sites can come back to haunt your personal life, career and relationships. An easy way to test whether or not you should add a photo or post a comment to your social networking site is to ask yourself if you'd be comfortable with your supervisor seeing the information. If the answer is no, don't add it. "For all times in perpetuity" is a long time. **FL**

DATA MINING



One evening, Brittany came across a fun survey that promised to calculate her "Attraction Fraction"—how welcoming she is to romantic advances.

The survey didn't ask for any information that could really identify her—only her zip code—so she figured it was safe to play along. One question asked her to choose from a list of four possible vacation destinations around the world. She selected a tiny tropical island off the coast of South America. About three months later, Brittany was shocked to find in her home mailbox a sales brochure for the very same island. It couldn't have been because of the survey, she thought; I didn't tell them anything about myself!

Data mining is the practice of searching large amounts of computerized data to find useful patterns or trends. For example, when you sign up for a free Microsoft Hotmail e-mail account, you are asked to submit your name, age, gender and zip code, but that's not all Microsoft learns about you. The company also tracks such things as the time of day you access your inbox, and how much money people within your zip code earn. This information may then be sold to businesses that will e-mail you advertisements because you fit their profile of a potential buyer.

In the novel *The Numerati*, author Stephan Baker writes, "Even if you hold back your name, it's a cinch to find you. A Carnegie Mellon University study recently showed that simply by disclosing gender, birth date, and postal zip code, 87 percent of people in the United States could be pinpointed by name." Although not every Web site you visit will engage in data mining, you need to know that it is possible.

Getting the Security YOU Need!

Flip on the news on any given night and you're likely to see a story about Internet security. Who has your information? What email scams are going around? What are the latest computer viruses to be concerned about? These things are an everyday problem threatening to make your life miserable! What can you do about it? Becoming informed is your best defense for keeping your information safe. The Division of Information Technology's Information Security and Account Management (ISAM) team is here to help. We offer a wide range of training customized to meet your needs.

Whether you'd like to educate yourself or ensure that those around you know what to look for, we can help. Worried that your co-workers are clicking and downloading things they shouldn't? Let ISAM come in and help educate your co-workers with a 30-minute presentation on phishing scams, key logging and how to keep your system up to date with anti-virus software. Do you know what social engineering is and why you should worry about it? Our training will teach you how to prevent this in your department, show you what signs to look for and teach you the right questions to ask.

Our training sessions are designed to get you the information that you need. The information provided in the training can be used not only for your job but will also give you tips to use at home. We offer both on-line and in-person group training. On-line training can be done individually or department wide. In-person training is for groups with 5 people or more and can be customized for your department's needs. No matter which venue works best for you, each will touch on many subjects to help you and your department stay secure.

Remember, education is the key to security. Let ISAM help you learn how to keep your information safe! Contact isam@missouri.edu for more information or to sign-up for on-line or group training today!

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.

CONSTRUCTION SIGNS WARN OF ZOMBIES

Austin drivers making their morning commute were in for a surprise when two electronic road signs on a busy stretch of road were taken over by hackers. The signs near the intersec-

tion of Lamar and Martin Luther King boulevards usually warn drivers about upcoming construction, but Monday morning they warned of "zombies ahead."

—Austin News, 1/28

BOTNET RINGLEADER GETS 4 YEARS IN PRISON FOR STEALING DATA

The first person to be charged under federal wiretap statutes for using a botnet to steal data and commit fraud was sentenced to four years in prison this week. John Schiefer, a 27-year-old Los Angeles resident, was also ordered to pay \$2,500 in fines.

—Computerworld, 3/6

'SMISHING' FISHES FOR PERSONAL DATA OVER CELL PHONE

When we think of phishing attacks, in which scammers try to lure sensitive information out of Internet users, we think of fake official-looking e-mails and Web sites. But you don't even need to be online to get phished. A phishing attack making the rounds tries to dupe cell phone users into revealing their personal data over the phone. It uses SMS messages, which makes it a "SMiShing" attempt.

—CNET News, 2/24

NYPD WORKER BUSTED IN MASS COP-ID THEFT

A civilian official of the New York Police Department's pension fund has been charged with taking computer data that could be used to steal the identities of 80,000 current and retired cops, sources said. Anthony Bonelli allegedly got into a secret backup-data warehouse on Staten Island last month and walked out with eight tapes packed with Social Security numbers, direct-deposit information for bank accounts, and other sensitive material.

—New York Post, 3/4

JOB SEEKERS TARGETED BY IDENTITY THIEVES

Job seekers beware. Identity thieves are looking to steal personal information from those searching for employment. Fake job ads are up 345% over the past three years, according to the U.K. Association for Payment Clearing Services, and the Identity Theft Resource Center (ITRC) warns that would-be workers should be careful about providing personal information to purported employers.

—InformationWeek, 3/5

WEB MAVEN GIVES CONVICTED BOTMASTER KEYS TO NEW KINGDOM

For the past four or five months, Mahalo.com has entrusted its site to a security consultant who stole hundreds of thousands of bank passwords with a massive botnet, which he sometimes administered from his former employer's premises. For most of that time, serial entrepreneur and Mahalo CEO Jason Calacanis was in the dark because no one at the company had bothered to Google the employee.

—The Register, 3/5