

FRONTLINE

SPRING 2008

TIPS AND TECHNIQUES TO PROTECT YOUR INFORMATION

INSIDE

2 Proof Positive

What percentage of your IT security budget is spent on awareness training?

3 Special Tactics

Crazy toaster: your gadgets can't be trusted.

3 Under the Microscope

Whaling attacks.

4 University of Missouri

Attack of the zombie bots!

4 Horror Stories

Cybercrime headlines from around the world.

Phishing the Social Network Oceans



Phishing scams are becoming increasingly popular within social networks. Phishing is a criminal's attempt to obtain your personal information such as usernames, passwords, credit card number, etc. via electronic communication. The term is a spoof on "fishing" because criminals are increasingly using sophisticated lures to catch your financial information. Social networking sites like MySpace, Facebook and LinkedIn are the future of phishing scams.

BAIT

Criminals are beginning to target social networking sites with phishing scams, as evidenced by a recent example involving Facebook posts containing fake links that could steal your information. The messages appear to be posted from your friends, which makes you more trusting of clicking on the attached link. The message reads "lol i can't believe these pics got posted.... it's going to be BADD when her boyfriend sees these," followed by what looks like a Facebook link.

HOOK

The link leads to a fake Facebook login page
[Continued on page 2]

Your Messages' History Trail

Detroit's Mayor Kwame Kilpatrick may be convicted of lying under oath, and if he is found guilty of perjury, he will be sentenced to up to 15 years in prison, be forced to resign as mayor and be disbarred because of text messages he sent using his city-issued pager back in 2002.

Most of us don't discuss our sordid affairs or criminal activities on our organization's equipment. But it is important to keep in mind that you could be releasing personally identifiable information (PII) about you or your organization via text or other modes of communication.

In January, the *Detroit Free Press* revealed the existence of more than 14,000 romantic text messages exchanged between Kilpatrick and his chief of staff, Christine Beatty. The

text messages reveal graphic details of Beatty and Kilpatrick's extramarital affair, their use of city funds to arrange romantic getaways and their conspiracy to fire Detroit Police Chief Gary Brown.

The attorneys for the city have tried to keep the text messages hidden on the basis that they were personal and private communications. However, a city directive (ironically re-authorized by Kilpatrick in his first term as mayor) states that all electronic communication sent on city equipment, including Kilpatrick's city-issued pager, should be "used in an honest, ethical and legal manner." The directive also cautions that such communication "is not considered to be personal or private."

A whistleblower suit was filed against the
[Continued on page 3]

hosted on a Chinese .cn domain. The fake URL is <http://www.facebook.com/profile.php.id.371233.cn/>. 371233 is a phony profile number and .cn indicates a Chinese domain. A real Facebook link would not have the .cn. The fake page does actually log you into Facebook, but it also records a copy of your username and password. The fake link then adds the same post to your friends' walls, so it spreads very quickly.

Social network phishing occurred as far back as June 2006 when the Orkut worm spread to 700,000 users in 24 hours! The worm is known as MW.Orc and it spread through Orkut, a social networking site run by Google (also the number one most-visited site in Brazil). The worm spread by disguising itself as a JPEG file and posting a link in other users' scrapbooks.

CATCH

The criminals who used MW.Orc stole banking details, usernames and passwords by installing a malicious executable file onto users' computers. The worm also made the users' computers part of a botnet—a network of infected computers controlled by criminals. Google released a fix to prevent further exploits from MW.Orc, but a new worm, Scrapkut, is infecting Orkut users. Scrapkut dupes people into clicking what looks like a YouTube video and then downloads code onto the user's computer. So far the worm seems to be harmless, but who knows what the future holds for the next wave of viruses?

Because financial institutions are working hard to secure your financial information, criminals are targeting sites like Facebook to make money in new ways. You may think that a criminal obtaining your username and password to your social networking site is no big deal, but there are good reasons to be concerned

and cautious. Although you should have a separate username for your social networking site, your e-mail account, your bank Web site and other accounts, many people use the same username and password for all. This makes it even easier for criminals to access your e-mails and account info. Some people even store personal information such as their maiden name or their credit card number on their social networking site. Obviously you should avoid posting such personal information.

SAFE SWIMMING

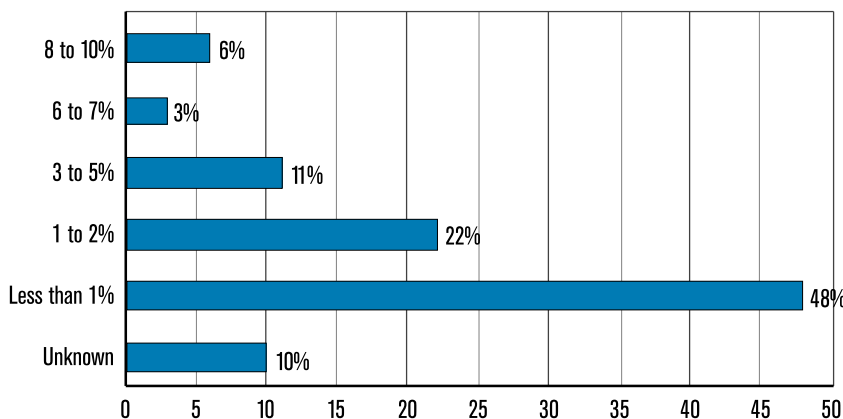
To protect yourself from phishing scams on social networks, there are actions you can take to secure your information:

1. Visit the real social network site to change your password.
2. If you use the same username and password for any other Web sites, change your password at those sites as well and make them different from each other.
3. Post as little personal information as possible. With some networking sites you may even want to go as far as fibbing your true name, but this is a violation of Facebook's terms of use.
4. Only add your real friends, never a stranger.
5. When possible, set your social networking site to "private." This assures that only people you have added as your friends can view your full profile.
6. Play the Anti-Phishing Phil game to educate yourself on what links are phishing scams and which are safe to visit, plus it's fun! http://cups.cs.cmu.edu/antiphishing_phil/quiz/index.html. There is also a Portuguese version of the game at (<http://seguranca.sapo.pt/phishingze/>).
7. Ask your IT department to submit suspicious links to PhishTank, <http://www.phishtank.com>. FL

Proof Positive: What percentage of your IT security budget is spent on awareness training?

Percentage of IT Security Budget Spent on Awareness Training

By Percent of Respondents



CSI 2007 Computer Crime and Security Survey
Source: Computer Security Institute

2007: 475 Respondents

The 2007 CSI Computer Crime and Security Survey asked respondents the percentage of their IT security budget that was spent on awareness training. Almost half spent less than 1 percent on awareness programs, perhaps because of the low cost of implementing them. It may be that real dollars aren't being put behind security awareness training.

SPECIAL TACTICS

Crazy Toaster: Your Gadgets Can't Be Trusted

According to Dror Shalev, a hacker and security expert, any kitchen appliance can be used to attack your computer; and he proved just that with his Crazy Toaster.

Shalev's point of the Crazy Toaster is to convey that you can't trust anything when it comes to the world of the Internet. We plug iPods, MP3 players, USB drives, cameras, cell phones and so many other gadgets back and forth into our home, work, friend's and complete stranger's computers. We often don't realize the ramifications of these actions. Think back to the holiday season when it was discovered that digital photo frames not only carried your pictures, but also a virus that downloaded itself onto your computer when you plugged it in.

Shalev felt challenged by a Google security expert's statement that there was no need to be afraid of a toaster at home. But Shalev disagreed and created the Crazy Toaster to prove that we should be less trusting of our home appliances and external devices.

To prove his point, Shalev set about creating a toaster that could hack into a computer. Shalev developed software and networked it with the toaster so when plugged in, the software would be activated on the victim's computer. The same software can be networked

with any home appliance to steal your personal information. With wireless capabilities, a hacker doesn't need to connect the appliance to the PC.

The idea of a Crazy Toaster invading our computers may not be as crazy as it seems. The Disneyland Resort recently teamed up with Microsoft to create the Innoventions Dream Home complete with technologies of the future. The home will include such features as lights and thermostats that automatically adjust when a person walks into the room. Mirrors and closets could identify clothes and suggest matching outfits and colors, or track what is in the wash or at the dry cleaners. The countertop would be able to identify groceries and provide recipes. Residents could even load photos, music or e-mails into a cell phone just by placing it on the surface of a desk!

In the future, Shalev cautions people to only purchase appliances or external devices from branded companies. The important lesson is to be cautious of where you are plugging in your external devices, as you may be transferring viruses without even being aware of your actions. Check to see what external devices you are allowed to use at work. If external devices are allowed, run an anti-virus check on both the computer and the external device before you plug it in. **FL**

Your Messages' History Trail

city by two former police officers, including Brown, who investigated the mayor's misconduct in office. The jury found Kilpatrick guilty, but the case cost the city over \$500,000 in legal expenses.

The ramifications were many. Beatty resigned as chief of staff and Kilpatrick resigned from the Florida A&M University Foundation board because of the scandal. Beatty, a law student, may have difficulty obtaining her license after lying in court. Beatty and her husband divorced in 2006.

RECORDS RETENTION

What is most astonishing about this case is the number of years the city was able to go back to obtain Kilpatrick's text messages. Many employees believe their text messages, instant messages or even e-mail messages

are private. However, if your organization owns the equipment, your conversations may be lawfully stored and could come back to haunt you. Read your organization's records retention policy to see how long your information is kept on file or in backups. Records retention policies vary widely by industry, state and nation.

Don't expect that your communication messages are private and not being stored. More than likely, they are being recorded, and what you say about other people or your organization could be made public. Messages can also be taken out of context, so be cautious of what you say and write. It may seem innocent to you but others may find it inappropriate.

If it isn't something you wouldn't want your boss to see, don't send it! **FL**

UNDER THE MICROSCOPE

WHALING ATTACKS



Criminals are targeting executives and wealthy end users in phishing scams known as whaling attacks. The fake e-mail messages are more convincing

than ever before. The message has a sense of urgency and a link for the victim to click now to take action. This combination makes it easy for even the tech-savviest end user to click the link.

The links lead to a virus that is downloaded onto the users' computer and steals his or her sensitive information. Since the victims are usually an authority within the organization, this can be especially damaging to the organization, clients, the victim and co-workers.

In June 2007, MessageLabs stopped more than 500 e-mail messages that contained an attachment from a reputable company. The download actually contained an .exe file that, when opened, collected sensitive data from the recipient's computer. Each e-mail was addressed to the recipient and included his or her name and job title, which made the scam message look reputable. The criminals had collected this personal information through social networking sites by targeting senior executives, or their friends and family. The criminals hoped to hack into the family computer in order to obtain the senior executive's work information.

Whaling attacks should not just be a concern to the targeted victims. Think of all of the client lists, financial records and personal information saved onto a high-level executive's computer and the potential consequences of that information leaking to a competitor. Successful whaling attacks affect the entire organization.

Attack of the Zombie Bots!

Almost everyone has heard of computer viruses and the dangers they pose. However, there's a new threat in computer security—botnets. It's important to protect yourself against this threat or you may find that your computer is sending spam or worse without you even knowing it!

First there are a few terms you should become familiar with. "Bot" is a term for a computer that has been infected by a virus that allows it to be controlled remotely. The systems that are infected are also called "zombies", because the hacker has remote control over the infected computer. After breaking into several computers and taking control of several "bots" a hacker becomes a "bot herder". Botnets are networks composed of millions of infected computers.

Bot infections are often spread via regular computer viruses. They usually enter your system through a security vulnerability and create a secure connection channel to communicate with the bot herder. Then, they wait for commands from their master. It's often hard to tell if you have been infected—many computers may experience slower performance but little or no effect that is noticeable to the end user. However, the system is still being controlled by the bot herder.

The bot herder can use these systems to do many things—most of which are illegal. Bots can be programmed to send spam or attack Web sites in order to knock the site off the Internet. They can serve pop-up ads, download new content or programs to the infected machine, log keystrokes and steal passwords—basically, anything the bot herder wants to do. Usually, the goal is to control computers and computing resources. This activity will appear to be coming from your computer and you may have to spend time and money to prove that it wasn't you!

There are some simple ways to protect your system from unwittingly becoming a bot:

- **Don't click on attachments in e-mail.** Many bots are created when a user clicks on an e-mail attachment and inadvertently infects their system.
- **Don't click on instant messages (IM) from unknown sources.** IM programs are increasingly being used to spread bot infections.
- **Run anti-virus software and keep it updated.** Symantec AntiVirus is available at no charge to University faculty, staff and students. It can be obtained at the Division of IT [Software Distribution Site](#).
- **Keep your operating system up-to-date.** Bot programs often use vulnerabilities in operating systems to find their way onto your computer. If you're ever afraid that your computer may be infected, you should take it to a reputable computer technician for repair. University faculty, staff and students can utilize the repair services at [Tiger Tech](#).

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.

LAPTOP STOLEN: PERSONAL DATA ON 300,000 HEALTH INSURANCE CLIENTS

Horizon Blue Cross Blue Shield of New Jersey has notified its members that an employee laptop computer containing personal information—including Social Security numbers—for about 300,000 individuals was stolen in early January. The health care insurer has sent letters to thousands of its members alerting them about the theft. On its Web site, the company says a "security feature was initiated" on Jan. 28 that "destroys all the data on the stolen computer."

—InformationWeek, 1/30

EUROPE STILL TOP SOURCE OF SPAM

European spam networks have pumped out more unsolicited e-mail than those in the United States for the third month in a row, according to security vendor Symantec. Symantec called this a "significant shift" in spam trends as, historically, compromised U.S. computers have been used to send spam, and many spammers have been U.S.-based.

—CNET.com, 2/6

SHIP'S ANCHOR CUT MIDEAST INTERNET CABLE

A telecommunications company on Friday blamed a ship anchor for cutting one of three severed undersea cables that snarled Internet traffic throughout the Middle East last week. FLAG Telecom's FALCON cable spanning Dubai and Oman was snapped Feb. 1 by an abandoned six-ton ship anchor, the company said, and will be repaired by Sunday.

—CNN.com, 2/8

FORMER CHINESE PROFESSOR TO SUE GOOGLE AND YAHOO

A former Chinese university professor who was dismissed after he founded a democratic opposition party, plans to sue Yahoo and Google in the United States for blocking his name from search results in China. Guo Quan, an expert on classical Chinese literature and the 1937 Nanjing massacre of Chinese civilians by Japanese troops, last week issued an open letter pledging to bring a lawsuit against Google after he discovered that his name had been excised in searches of its Google.cn portal in China.

—CNET.com, 2/13