CLUB DIRECTOR

THE MAGAZINE OF THE NATIONAL CLUB ASSOCIATION

NOVEMBER / DECEMBER 2008 | WWW.NATIONALCLUB.ORG

Technology Trends

MOVING INTO THE FUTURE WITH MEMBER SERVICES

Social Engineering
Strategic IT Planning
Disaster Relief Act

Don’t Be Fooled
by Social Engineering

BY AMY RIGARD

The phone company technician arrived at the club one morning and announced that a service problem in the area was causing businesses to experience outages and poor voice quality. He was at the club to make sure they had the latest switch upgrade to prevent the problem from happening. The technician was dressed in a phone company uniform with a badge, and asked for access to the phone system closet. He went about his business in less than five minutes and reported that the switch was fine and would not be affected by the service problems. But, things aren’t always what they appear to be …

The natural human tendency is to trust. So it is no wonder that hackers have found clever ways to manipulate this trust. That’s right—hackers are no longer simply sitting behind their computers tapping into an IP address with an unsecured computer or network. They’ve found a much weaker link in the security chain—people and their natural willingness to accept someone at his or her word.

Through social engineering, or the art of manipulating people into performing actions or divulging confidential information, sensitive information could end up in the wrong hands. The term social engineering, in this sense, was developed by Kevin Mitnick, a former criminal hacker who served time in prison and now works as a consultant.

Clubs, while typically not considered a target by traditional hackers who were looking for financial data, are poised to become targets of social engineering. Carla Brinker, a manager at RSM McGladrey, a firm that provides technology consulting services to the private club industry, said clubs are being targeted because it’s known they typically have weaker network security. Plus, if a hacker can get in, they know there’s valuable information to steal: clubs hold a lot of individual net worth among the membership. “They think clubs are easy pickings, so they’re going to try,” Brinker said.

Mark Lipsitt, principal of The Lipsitt Group, echoed that sentiment. “Clubs have had it lucky for a while, but that is going to end,” he said. People who target clubs are looking for information they can sell, such as membership information, and they’re targeting the members, rather than the club as a whole. “When you look at the typical club’s security, they pay attention to the physical security of the network [from a hardware/software perspective], but they are often ignoring the people part,” he said. “The demographics of clubs make them prime targets. Plus, since clubs have not really experienced this problem in the past, the tendency [of social engineers] may be to believe security is a little lax.”

The general manager heard that a number of members had called recently to change their credit card numbers on file at the club. It seems that these members had been contacted by their credit card company and told that significant purchases of flat panel TVs, personal electronics and even a car had been charged to their cards. The account number used was the same account number that they had given the club to charge their dues and fees. The general manager felt it was more than a coincidence and warranted an investigation …

> "WITH PRETEXTING, PEOPLE HAVE DONE THEIR HOMEWORK AND ALREADY KNOW A LITTLE BIT OF INFORMATION — USUALLY ENOUGH TO GET PEOPLE TO LET THEIR GUARDS DOWN."

Preying on Trust

"Social engineering preys on people's emotions," Brinker said. She has seen it firsthand, as part of her job is to try to gain confidential information from clients to test their security.

Someone who is attempting social engineering will try to present a credible, authentic scenario, just as the example illustrates. On the phone, they sound like who they claim to be, and in person, they appear to be who they say they are and are there for the reasons they claim to be. If someone seems hesitant, a social engineer will try to make them feel guilty or place fear in them. "It almost always starts on trust, then guilt and fear, and sometimes curiosity and greed are other emotions that are preyed upon," Brinker said.

Among her numerous security tests, Brinker has impersonated a florist, a delivery driver, a janitor, and other vendors. "A uniform and a confident smile are often the only authentication people need," Brinker said, adding that is a troubling fact, considering that uniforms can be purchased on sites like eBay.While Brinker has been stopped many times, more frequently, she gains access into the business.

Suspecting foul play, the general manager hired a risk management expert to review the club's computer security. During the risk management company's network scan an unknown device was identified. A search of the equipment room located the device, which was a small router that was configured to allow unfettered outside access to the club's computer network. The computer equipment was housed in the same room as the telephone switch…

"Pretexting" is an element of social engineering that preys on trust by gathering small pieces of information from multiple people until a person collects enough information to gain the unauthorized access.

"With pretexting, people have done their homework and already know a little bit of information—usually enough to get people to let their guards down," said Scott Perry, business development manager for Flagship Networks, Inc., a systems integrator company that services the hospitality industry in N.Y., N.J. and Conn. This homework, or reconnaissance, could be done in a number of ways.

For example, a person could frequent a place where club employees are found—such as a bus stop or nearby coffee shop—to eavesdrop on conversations, trying to gather information that would help them gain access, such as names of key staff, routine maintenance schedules or upcoming club events. Or, a club could unknowingly hire someone who is working as a "plant" or informant, who secures information over a period of time for the person who carries out the attack. A more common scenario involves someone simply gaining building/grounds access to the club. Once inside, the person could eavesdrop on conversations, install electronic surveillance, or leave a flash drive equipped with technology to gather sensitive data, in hopes that someone curious enough would plug it into their computer and unintentionally install it.

Pretexting occurs via the telephone as well—often by someone trying to learn club information such as staff names, work schedules and passwords or account numbers for the club. By first gathering information about where the club has its bank account—such as watching the mail for statements—someone pretending to be from the bank could call and ask for the account number or password to verify the club's information. Many times, these perpetrators are skilled actors at impersonation and intimidation and can use both information and their authoritative demeanor to access information.

Viruses, Worms and Trojans—Oh My!

With names that sound dangerous, malicious or just plain unpleasant, how does one understand the difference between these various threats that can cause serious damage to your computer and files?

The following list includes definitions of some of the common threats for computers:

Virus. A computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user. A virus must meet two criteria: 1) It must execute itself. Often, the virus places its own code in the path of execution of another program. 2) It must replicate itself. For example, it may replace other executable files with a copy of the virus-infected file.

Worm. Worms are programs that replicate themselves from system to system without the use of a host file. This is in contrast to viruses, which require the spreading of an infected host file. Although worms generally exist inside of other files, often Word or Excel documents, there is a difference between how worms and viruses use the host file.

Trojan horse. The term Trojan horse comes from a Greek fable, in which the Greeks presented a giant wooden horse to the Trojans as a peace offering. However, a nasty surprise awaited the Trojans as Greek soldiers sprung out of the hollow horse and captured Troy. Similarly, a Trojan horse program presents itself as a useful computer program, while it actually causes havoc and damage to your computer.

Increasingly, Trojan horses are the first stage of an attack, and their primary purpose is to stay hidden while downloading and installing a stronger threat such as a bot. Trojan horses cannot spread by themselves and are often delivered to a victim through an e-mail message where it masquerades as an image or joke, or by a malicious Web site, which installs the Trojan horse on a computer through vulnerabilities in Web browser software.

Spyware. Spyware is a general term used for programs that covertly monitor activity on your computer, gathering personal information, such as usernames, passwords, account numbers, files, and even driver's license or social security numbers. Some spyware focuses on monitoring a person's Internet behavior, including places you visit and things you do on the Web, the e-mails you write and receive, as well as your instant messaging conversations. After gathering this information, the spyware then transmits that information to another computer, usually for advertising purposes.

Spyware is similar to a Trojan horse in that users unknowingly install the product when they install something else.

Malware. Malware is a category of malicious code that includes viruses, worms and Trojan horses. Destructive malware will utilize popular communication tools to spread, including worms sent through e-mail and instant messages, Trojan horses dropped from Web sites, and virus-infected files downloaded from peer-to-peer connections. Malware will also seek to exploit existing vulnerabilities on systems making their entry quiet and easy.

Bots and Botnets. A bot is a type of malware that allows an attacker to take control over an affected computer and use that computer to send out phishing e-mails or malicious code. Bots are usually part of a network of affected machines, known as a botnet, which is typically made up of victim machines that stretch across the globe.

Since a bot-infected computer does the bidding of its master, many people refer to these victim machines as zombies. The cybercriminals that control these bots are called botherders or botmasters. Some botnets might have a few hundred or couple thousand computers, but others have tens and even hundreds of thousands of zombies at their disposal. Many of these computers are infected without their owners' knowledge. Some possible warning signs could be mysterious messages, a slower computer or more frequent crashes.

Phishing. Phishing involves using SPAM, malicious Web sites, e-mail messages and instant messages to trick people into divulging sensitive information, such as bank and credit card accounts. Phishers, pretending to be legitimate companies, may use e-mail to request personal information and direct recipients to respond through malicious Web sites. They tend to use emotional language or scare tactics or urgent requests to entice recipients to respond. The phish sites can look remarkably like legitimate sites because they tend to use the copyrighted images from legitimate sites. Requests for confidential information via e-mail or instant message tend to not be legitimate.

Firewall. A firewall provides a line of defense between computers that share information to control the flow of information back and forth between a computer and a Web server. A firewall examines all traffic routed between the computer and the Internet to see if it meets certain criteria. If it does, it is allowed in. If it doesn't, it is stopped. Protecting your computer from intrusion, the firewall keeps your machine from getting burned by destruc-tive intrusions that could result in data loss or file corruption.

To prevent threats from damaging threats such as viruses and malware, antivirus software and firewalls need to be installed on computers throughout the club. This helps protect the computer network. In addition, clubs should focus on educating staff about the possible threats they face from other sources, such as social engineering.

SOURCE: SYMANTEC

A simple telephone call to the phone company confirmed the general manager's suspicions: the technician was a fraud. No service problems had been reported by local businesses and no legitimate service technicians were dispatched to the club. The club and it members were victims of a social engineer! Police were called to investigate the crime.

Phishing for Information

Gathering sensitive data via e-mail, or phishing, is another common tactic used by someone trying to gain unauthorized access. Reconnaissance work can be done to learn the names of friends or associates, so an e-mail with a link to install damaging software can appear to come from someone you know. Likewise, hackers can send an e-mail from what appears to be a valid company e-mail address from someone with whom you regularly conduct business, stating your account has been compromised and prompting you to enter your account number and other identifying information to resolve the issue. Lipsitt cautions that no financial institution of any kind would ask for account information via e-mail, so always be suspicious of those types of e-mails.

While private clubs traditionally have not been targeted for social engineering schemes, enough businesses have fallen victim to create an awareness of this activity. This is especially important because clubs keep personal information on their members, such as e-mail addresses, phone numbers and physical addresses, credit card and Social Security numbers, which in the wrong hands, would be a major problem.

Fighting Back

Brinker said the key to preventing a social engineering attack is education. While it may be difficult for some to »»

WHILE PRIVATE CLUBS TRADITIONALLY HAVE NOT BEEN TARGETED FOR SOCIAL ENGINEERING SCHEMES, ENOUGH BUSINESSES HAVE FALLEN VICTIM TO CREATE AN AWARENESS OF THIS ACTIVITY.

draw the line between trust and exceptional customer service, it is a fine line that needs to be painted clearly. "You need to know to whom you're speaking when giving out sensitive information," she said. "Authentication is the hardest part. Photo IDs cannot be relied on, as those can easily be printed from a home computer." To authenticate a potentially unauthorized person, Brinker recommends asking someone else at the club if they are expecting that person or calling the company the person is supposedly representing, to verify the visit.

Lipsitt said the first thing to do if a club's security—network or human— is breached is to announce it to the membership. "That goes against the grain of what clubs would want to do because it would be embarrassing and potentially damaging to their reputation," he said. "But it must be done because it would be even more embarrassing for members to find out from a source other than the club." The club should present its members with information on what they know has been compromised and the steps they are taking to resolve the problem.

Lipsitt also recommends that clubs be more diligent when choosing the software they purchase, ensuring that it allows credit card numbers to be encrypted and is PCI-compliant.

Because phishing is an area where clubs could potentially be susceptible, and people typically have no training on what to do with various e-mails, policies need to be created and enforced. Lipsitt said the message to people used to be to never open an attachment in an e-mail from someone they don't know. Now, he said, the message is to not open an e-mail attachment from someone you weren't expecting it from. Rather, call the sender and ask if they did, indeed send it because viruses and other harmful things can be attached in seemingly innocuous items like Word documents or Excel spreadsheets. While this is not necessary with every e-mail received, it is best to use caution if an e-mail raises any amount of suspicion.

Brinker said that most people who are trying to gain unauthorized access are targeting financial information. If access has been gained to something that can be changed, such as passwords, change them right away. If it's something that can't be changed, it needs to be monitored.

Perry said most clubs don't have policies in their manuals about Internet use for personal activities and recommends creating a strong policy and reiterating it to employees. Staff also should be told never to give information to vendors, visitors and callers without verifying the person and purpose of the request.

Perry also emphasized the importance of maintaining the support on the technology products clubs have in place to secure their computer networks. Some clubs have an IT person on staff, and some may outsource this responsibility. Outsourced companies typically use remote management and have someone watching the club's network constantly, while most clubs only have one person on staff to serve this function. Often, controllers are responsible for overseeing IT, but it is not their main function.

"The odds are that an attack won't be targeted at a club's network," said Lipsitt. "But everyone is potentially under attack from social engineering."

As schemes become more elaborate and begin to infiltrate the club industry, it is important to take the necessary precautions to protect the club networks and members from any threats of an invasion of privacy. Knowledge of the specific threats—whether social engineering, phishing, viruses or technical dangers—is the first step. ■

Amy Rigard is NCA's assistant editor.