The Ultimate Guide to **Social Engineering**

From CSO Magazine and CSOonline.com

CONTENTS

I. Definition

What is Social Engineering?

Social engineering is the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password. The goal is always to gain the trust of one or more of your employees.

Famous hacker Kevin Mitnick helped popularize the term "social engineering" in the '90s, but the simple idea itself (tricking someone into doing something or divulging sensitive information) has been around for ages.

What Social Engineers Want

The goal for many social engineers is to obtain personal information that can either directly lead them to financial or identity theft or prepare them for a more targeted attack. They also look for ways to install malware that gives them better access to personal data, computer systems or accounts, themselves. In other cases, social engineers are looking for information that leads to competitive advantage. Items that scammers find valuable include the following:

- Passwords
- Account numbers
- Keys
- Any personal information
- Access cards and identity badges
- Phone lists
- Details of your computer system
- The name of someone with access privileges
- Information about servers, networks, non-public URLs, intranet

How Social Engineers Work

There are an infinite number of social engineering exploits. A scammer may trick you into leaving a door open for him, visiting a fake Web page or downloading a document with malicious code, or he might insert a USB in your computer that gives him access to your corporate network. Typical ploys include the following:

Stealing passwords: In this common maneuver, the hacker uses information from a social networking profile to guess a victim's password reminder question. This technique was used to hack Twitter and break into Sarah Palin's e-mail.

Friending: In this scenario, a hacker gains the trust of an individual or group and then gets them to click on links or attachments that contain malware that introduces a threat, such as the ability to exploit a weakness in a corporate system. For example, says Netragard CTO Adriel Desautels, he might strike up an online conversation about fishing and then send a photo of a boat he's thinking of buying.

Impersonation/social network squatting: In this case, the hacker tweets you, friends you or otherwise contacts you online using the name of someone you know. Then he asks you to do him a favor, like sending him a spreadsheet or giving him data from "the office." "Anything you see on a computer system can be spoofed or manipulated or augmented by a hacker," says Desautels.

Posing as an insider: In many cases, the scammer poses as an IT help desk worker or contractor to extract information such as a passwords from an unknowing employee. "Roughly 90% of the people we've successfully exploited during [vulnerability assessments for clients] trusted us because they thought we worked for the same company as them," Desautels says.In one case, a Netragard worker posed as a contractor, befriended a group of the client's workers and set up a successful phishing scheme through which he gleaned employee credentials, eventually gaining entry to the entire corporate infrastructure.

State of the State

Social engineering attacks are widespread, frequent and cost organizations thousands of dollars annually, according to research from security firm Check Point Software Technologies. Its survey of 850 IT and security professionals located in the U.S., Canada, U.K., Germany, Australia and New Zealand found almost half (48%) had been victims of social engineering and had experienced 25 or more attacks in the past two years. Social engineering attacks cost victims an average of $25,000 - $100,000 per security incident, the report states.

"Socially-engineered attacks traditionally target people with an implied knowledge or access to sensitive information," according to a statement from Check Point on the survey. "Hackers today leverage a variety of techniques and social networking applications to gather personal and professional information about an individual in order to find the weakest link in the organization."

Among those surveyed, 86% recognize social engineering as a growing concern, with the majority of respondents (51%) citing financial gain as the primary motivation of attacks, followed by competitive advantage and revenge. The most common attack vectors for social engineering attacks were phishing emails, which accounted for 47% of incidents, followed by social networking sites at 39%.

New employees are the most susceptible to social engineering, according to the report, followed by contractors (44%), executive assistants (38%), human resources (33%), business leaders (32%) and IT personnel (23%).

However, almost one-third of organizations said they do not have a social engineering prevention and awareness program in place. Among those polled, 34% do not have any employee training or security policies in place to prevent social engineering techniques, although 19% have plans to implement one, according to Check Point.

II. Basic Tactics

There are four basic psychological tactics that social engineers use to gain trust and get what they want, according to Brian Brushwood, host of the Web video series, "Scam School."

Knowing these underlying principles of social engineering will enable employees to more easily recognize when they are being targeted by a scammer.

1. Social engineers convey confidence and control. According to Brushwood, one of the first steps to pulling off something deceptive is to act confident. For example, someone trying to get into a secure building might forge a badge or pretend to be from a service company. The key to getting in without being challenged is to simply act like you belong there and that you have nothing to hide. Conveying confidence with body posture puts others at ease.

"People running concert security often aren't even looking for badges," says Brushwood. "They are looking for posture. They can always tell who is a fan trying to sneak back and catch a glimpse of the star and who is working the event because they seem like they belong there."

Another way to gain the upper hand is to seem in charge through conversation, says Brushwood. "The person who asks the questions controls the conversation," he says. "When someone asks you a question, it immediately puts you on defense. You feel a social pressure to give a correct or appropriate response."

Takeaway: Advise employees not to become too comfortable with allowing outsiders into the building. Visitors (and service providers) should have credentials checked thoroughly—even if they are familiar faces.

2. Social engineers offer free gifts or favors. Reciprocation is another human impulse used by social engineers, according to Brushwood. "When people are given something, such as a favor or a gift, even if they actively dislike the person who did it, they feel the need to reciprocate," says Brushwood. Examples include a plate of cookies offered to a receptionist or an offer to hold the door for an employee.

The time delay between giving the gift and asking for a favor is important. "If you give a gift and then immediately ask for a favor, the odds are that somebody might perceive it as a bribe. If they perceive as a bribe, they react uncomfortably." Instead, a skilled con artist might give something to a gatekeeping employee early in the day and then come back later, claiming a mix-up, such as an item left behind after a meeting.

"Chances are, they will let you by as reciprocation for how you treated them earlier," says Brushwood.

Takeaway: Advise employees to be skeptical of anyone who tries to give them something. Depending on how big the stakes are, an experienced criminal may even spend weeks laying the groundwork to form a reciprocal relationship with staff that can result in access to sensitive or secure areas.

3. Social engineers use humor. People generally enjoy the company of those with a good sense of humor. The social engineer knows this all too well and uses it to gain information, get past a gatekeeper or even just get out of trouble. Brushwood has used humor to get out of speeding tickets many times. His trick is to show a funny license picture and then even finds a way to hand the officer a Monopoly "Get out of Jail Free" card as part of his side-of-the-road shtick.

"Police deal all day with the boo-hoo stories," he says. "But my approach is to be upbeat, to give them the impression that I am not worried and would rather hang out and make them laugh."

Takeaway: In a breach or criminal scenario, the social engineer might try and chat with an employee to get information out of him. One good example is the fake IT call, where the caller asks for an employee's password. It is much more likely that sensitive information will be volunteered if the conversation is fun, and puts the employee at ease.

4. Social engineers can always state a reason. Brushwood was recently inspired by the results of a recent Harvard study that found people are likely to concede to a request if the word "because" is used when asking. The study looked at groups of people waiting to use a copy machine in a library and how they responded when someone approached and asked to cut in line.

In the first group, the person would say, "Excuse me, I have five pages. May I use the Xerox machine because I'm in a rush?" In that group, 94% allowed the person to skip ahead in line. In another group, the line-cutter asked: "Excuse me, I have five pages. May I use the Xerox machine?" Only 60% said yes to this person. In a third group, the question was, "Excuse me, I have five pages. May I use the Xerox machine because I need to make copies?" Even though the reason was seemingly ridiculous, 93% still said yes to the line-cutter.

"Turns out, the magic word is because," says Brushwood. "Just like if you see someone marching around like they own the place, it's safe to assume they belong there. Likewise, if someone says 'because,' people assume they have some legitimate reason."

Brushwood points out that gaining people's cooperation requires just the perception of a reason, even if the reason is nonsense.

Takeaway: It's important to slow down and look and listen to what is happening and what is being said in a work environment. During a hectic day, it may seem easier to wave someone by or give up information when it is requested. But awareness and presence of mind are paramount to preventing a criminal from taking advantage of you.

III. Prevention

No organization is immune to the threat of social engineering. Consider a contest held at the DefCon security conference, in which contestants were challenged with obtaining information about target companies that could be used for

a hypothetical attack. Of 140 phone calls made to employees at target companies, almost all coughed up information; only five employees did not. And 90% of targeted employees opened up a URL sent to them by contestants—even though they really didn't know the person who had sent it. The numbers reveal the scope of the social engineering problem for all organizations.

With that in mind, here are some ways to minimize your organization's risk.

Raise Staff Awareness

It is widely agreed that the single most effective way to battle social engineers is staff awareness. A security-aware culture is possible in any organization as long as it is the standard by which everyone operates, and concepts are consistently reinforced. Here are some ways to build a culture of security. Audry Agle, CISSP, CBCP, MBA and an independent consultant in the San Diego area, offers seven ideas to help you raise staff awareness of the dangers of social engineering.

Appeal to personal lives: Get people interested in security by arming them with techniques to secure their own personal information. Offer Lunch-N-Learn sessions where staff can get tips for what needs to be shredded or locked up at home, how to manage personal passwords, how to secure home-based wireless networks, etc.

Make the message visible: Put posters up at fax machines, shred bins and coffee rooms. Make them eye-catching but simple so that anyone walking by can read and interpret them without breaking stride. Change your messages at least once per month so there is always something new. If you don't have a graphic artist on staff, hire a college student to do the artwork, or use one of the security awareness vendors for ready-made ones.

Provide treats: You'd be surprised how far a donut goes to get attention. Have an occasional celebration where Security thanks the staff for doing their part.

Use their desk: If you have a clean desk policy, perform random desk checks after hours. Reward those who have no sensitive material out by leaving a small treat like a piece of candy or pack of gum and a "Thanks for Doing your Part" note, or enter them in a monthly drawing for a prize.

Bring it to their computer screen: If you have a company newsletter, include a security article in each edition and provide information on the latest incidents, particularly in your industry. Supplement your newsletter with a monthly email to all staff, with a short message about a timely and relevant topic—PDA safety, emergency preparedness or a reminder of who to call for suspicious incidents. Provide a Security page on your employee intranet that lists the security policies, important contact information, links, etc.

Require training: Training programs will be more effective if you include interactive exercises, contests, games or give-aways. Try to keep it short, and test comprehension.

Walk the walk: A high-impact technique is for senior leadership members to display their own penchant for security. Advertise internally when someone does something that thwarts a potential attack, or comes up with a control that bolsters the security of your organization in a cost-effective manner.

Remember that your employees can make or break your security program, Agle says, so keep them engaged in the process by soliciting feedback and suggestions.

Stop, Think, Connect

A coalition of government, industry and non-profit organizations have developed a campaign that aims to make people think before they engage in potentially risky activity online. The message—"Stop. Think. Connect."—is intended to be easily understood and implemented, a la other popular safety slogans such as, "Click it or Ticket" and "Stop, Look and Listen." The campaign is the result of a mandate from President Barack Obama's Cyberspace Policy Review, which called for the creation of a national public awareness campaign focused on cyber security.

"It is a simple, actionable message that applies to everyone as we connect to the Internet from an array of devices, including laptops, personal computers, smartphones and gaming consoles," says NCSA Executive Director Michael Kaiser.

Learn and Teach Basic Lessons

In his book *Social Engineering: The Art of Human Hacking*, Chris Hadnagy tells three memorable stories of vulnerability assessment tests that he's conducted for companies, to gauge their exposure level. Each story points to what organizations can learn from these results.

THE CASE OF THE OVERCONFIDENT CEO

Lesson Learned 1: No information, regardless of its personal or emotional nature, is off limits for a social engineer seeking to do harm.

Lesson Learned 2: It is often the person who thinks he is most secure who poses the biggest vulnerability. Some experts believe executives are the easiest social engineering targets.

Hadnagy was once hired as an SE auditor to attempt to access the servers of a printing company whose processes and vendors were proprietary and of interest to competitors. The CEO told Hadnagy that hacking him would be next to impossible because he "guarded his secrets with his life."

"He was the guy who was never going to fall for this," says Hadnagy. "He was thinking someone would probably call and ask for his password, and he was ready for an approach like that."

After some information gathering, Hadnagy found the locations of servers, IP addresses, email addresses, phone numbers, physical addresses, mail servers, employee names and titles and much more. Through Facebook, he was also able to get other personal details about the CEO, such as his favorite restaurant and sports team.But the real prize came when Hadnagy learned the CEO was involved

in cancer fundraising, due to a family member's succesfull battle with cancer.

Armed with the information, he was ready to strike. He called the CEO and posed as a fundraiser from a cancer charity the CEO had dealt with in the past. He informed him they were offering a prize drawing in exchange for donations—and the prizes included tickets to a game played by his favorite sports team, as well as gift certificates to several restaurants, including his favorite spot.

The CEO bit, and agreed to let Hadnagy send him a PDF with more information on the fund drive. He even managed to get the CEO to tell him which version of Adobe reader he was running. Soon after he sent the PDF, the CEO opened it, installing a shell that allowed Hadnagy to access his machine.

When Hadnagy and his partner reported back to the company about their success with breaching the CEO's computer, the CEO was understandably angry, says Hadnagy.

"He felt it was unfair we used something like that, but this is how the world works," he says. "A malicious hacker would not think twice about using that information against him."

THE THEME PARK SCANDAL

Lesson learned 3: Security policy is only as good as its enforcement.

Lesson learned 4: Criminals will often play to an employee's desire to be helpful.

The target in this next case study was a theme park client that was concerned about the potential compromise of its ticketing system, as the computers used to check in patrons also contained links to servers, client information and financial records.

Hadnagy started his test by calling the park, posing as a software salesperson. He was offering a new type of PDF-reading software that he wanted the park to try through a trial offer. He asked what version they were currently using, obtained the information easily and was ready for step two.

The next phase required on-site social engineering, and Hadnagy used his family to ensure success. Heading up to one of the ticket windows with his wife and child in tow, he asked one of the employees if they might use their computer to open a file from his email that contained a PDF attachment for a coupon that would give them discount admission.

"The whole thing could have gone south if she said no," explains Hadnagy. "But looking like a dad, with a kid anxious to get into the park, pulls at the heart strings."

The employee agreed, and the park's computer system was quickly compromised by Hadnagy's bad PDF. Within minutes, Hadnagy's partner was texting him to let him know he was "in" and gathering information for their report. Hadnagy points out that while the park's employee policy states they should not open attachments from unknown sources (even a customer needing help), there were no rules in place to actually enforce it. "People are willing to go to great lengths to help others out," says Hadnagy.

THE HACKER IS HACKED

Lesson learned 5: Social engineering can be part of an organization's defense strategy.

Lesson learned 6: Criminals will often go for the low-hanging fruit. Anyone can be a target if security is low.

A third example shows how social engineering is used for defensive purposes. Hadnagy profiles "John," a penetration tester hired to conduct a standard network penetration test for a client. He ran a scan using Metasploit, which revealed an open VNC (virtual network computing) server, a server that allows control of other machines on the network.

He was documenting the find with the VNC session open when, suddenly in the background, a mouse began to move across the screen. John knew it was a red flag because at the time of day this was happening, no user would be connected to the network for a legitimate reason. He suspected an intruder was on the network.

Taking a chance, John opened Notepad and began chatting with the intruder, posing as a new and unskilled hacker. "He thought, 'How can I get more information from this guy and be more valuable to my client?'" says Hadnagy. "John played to the guy's ego by trying to pretend he was a newbie who wanted to learn more from a master hacker."

John asked the hacker several questions, pretending to be eager to learn some tricks of the hacking trade. By the time the chat was over, he had the intruder's email, contact information and even a picture of him. He reported the information back to his client, and the problem of easy access to the system was also fixed.

Hadnagy also points out that John learned through his conversation with the hacker that the hacker had not really been targeting the company; he had just been out looking around for something easy to compromise and found the open system quite easily.

Secure the Weakest Link: The End User

While technology has changed, the most influential factor in security has not: The employee. As Winn Schwartau, founder of The Security Awareness Company says, "The weakest link in all of this stuff is the person at the keyboard." As a result, security managers are up against a combination of ignorance, apathy and arrogance when it comes to individual awareness.

Here are two teachable moments that Schwartau has encountered in his decades of conducting security awareness training. Social engineering, he says, has new players and forms, but the underlying techniques usually remain the same.

NEVER PROVIDE PERSONAL INFORMATION—TO ANYONE

Teachable moment: Part of awareness training needs to include specific instructions not to give out personal infor-

mation to any person or department. "Let them know: Our department will never ask you for these kinds of details," says Schwartau. "The proper procedure when launching a new system is to issue new credentials. You never ask for existing credentials."

We had been hired by a large financial services firm in New York to do security awareness training. We wanted to do an assessment of their awareness level, so we created a social engineering test.

It was not the traditional "call someone on the phone and try to social engineer them." We took their letterhead and wrote a letter and sent it through regular mail to about 30% of the employees, so approximately 1,200 people. The letter said essentially: "Hi, we're from corporate information security. The reason you are receiving this letter is because we know social engineering occurs at work, and we are going to upgrade our systems." We then went into some detailed technical babble about how we were going to migrate this database to this and a lot of stuff the average person is just not going to understand.

It went on to say, "We know you're concerned about security, and that is the reason for this letter. We don't want you to communicate any of this information over anything but mail, because that is the only secure way to do this. We need your personal details on the following things so we can transfer them into the system and verify them for accuracy because we've been having trouble with databases in this transition."

We told recipients: "Please do not email or fax this information. Use ONLY the self-addressed, stamped envelope," which we addressed to an address that was not the company's address. We told them we had done that because we did not want anyone at work intercepting this in the office. We also told them we had set up a special, secure P.O. Box that only the security department had access to.

After it was sent out, we received about a 28% response. It was a very simple social engineering test, and more than a quarter of the people targeted fell for it.

We've done this in other places with phishing emails. In one place, we sent an incredibly enticing email offering free stuff. We did that AFTER extensive training and certification of the entire organization, which was in excess of 95% passing the awareness assessments. But the response to the phishing email, even after the training, was 40%.

No matter how many tests, assessments and other measures you put into place, it's not going to work against human nature. We can help it with training, and measure an incremental increase in awareness, but you will never achieve 100% success.

IF THEY ASK FOR CREDENTIALS, THEY ARE NOT TRUSTWORTHY

Teachable moment: Like the security department at work, a legitimate financial institution will never ask you for credentials through email. They will have you call the number on back of your card, or visit the homepage you always go to. Never, ever trust anyone who comes to you asking for credentials, says Schwartau. That is not how it's done.

I got this email recently from what looked like Bank of America. I bank with Bank of America, and I do about 98% of my banking online. The email was from SiteKey, their site verification system, which is actually a pretty good system. It said "Hey, this is from SiteKey, and this is really urgent because you just transferred some money, and we need to verify that."

Now, I knew it was a scam because I'm a professional paranoid. But I'm looking through the email, the addresses, and they are all correct! The logos, the site key information; all correct. All I could think was, "How they heck are they pulling this off?"

So then I look under the links; I do a mouse-over to look under and see what is going on. It's still all correct. I clicked a couple of links to see how far I could go and took some screen shots for training purposes. I still could not figure it out.

Finally, after quite a while, I realized it: The reason I could not figure it out is because I was on my laptop with a 13-inch screen with low resolution. Underneath the links, the addresses, it said 'Bank of Americil.com.' I knew better from the get go. But how many people are going to fall for something like that?

Teachable Moments

John Sileo, an identity theft expert who trains on repelling social engineering, knows from first-hand experience what it's like to be a victim. Sileo has had his identity stolen—twice. And both instances resulted in catastrophic consequences. The first crime took place when Sileo's information was obtained from someone who had gained access to it out of the trash (yes, dumpster diving still works). She bought a house using his financial information and eventually declared bankruptcy.

"That was mild," said Sileo, who then got hit again when his business partner used his information to embezzle money from clients. Sileo spent several years, and was bankrupt, fighting criminal charges.

Now that he has emerged from these problems, he spends his time assisting organizations to train employees on what social engineering and identity theft techniques look like. "I'm trying to inspire employees to care about privacy," he said. "If they don't care about it at a human level, they are not going to care about the company's privacy policy or IT security. You've got to get it at a primal personal level." Here are two of Sileo's memorable social engineering scenarios he's heard during his years as a security lecturer.

Doctor Who?

Not long after Dr. Yamitori shared her username on a handout at a medical conference, she received an invitation to become friends with Dr. Xavier on a social networking site built for the medical community. Dr. Yamitori had shared her impressions of the conference on the site, and Dr. Xavier had been taking note. Over the course of the next month, the two never communicated directly via the network; rather, they received regular updates and comments posted by the other doctors in the network.

On Friday afternoon at 2:00 PM, Dr. Xavier (Dr. X) posted a comment directly to Dr. Yamitori (Dr. Y). Dr. X

explained that he was in the process of researching software packages for his office and, knowing from the conference that Dr. Y ran an efficient operation, wanted to find out what software she used to manage her patient files.

Dr. Y happened to be at her computer and responded immediately to the query. Because both were part of a doctor's network, and concluding that the questions were innocuous, Dr. Y shared that she used Patient Relation 10.0 and was very happy with it. Dr. X thanked her, asked no further questions, and concluded the thread somewhat abruptly.

At 2:06 P.M., Dr. Y's assistant sent an internal instant message to her, saying that Dr. Xavier was on hold and had a quick follow-up question to their online chat. When Dr. Y picked up, Dr. X apologized for any trouble he was causing, but said he had one last question and thought it was a good excuse to meet in person. Dr. X then asked Dr. Y if she would mind sharing the name of the software technician from Patient Relation Software who had installed the package for her so that he could ask some technical questions. Dr. Y gladly told him that her contact at the software company was Kenneth, and gave him Kenneth's phone number.

On Monday morning, before most doctors are in their offices, Dr. X's accomplice called Dr. Y's office and reached the receptionist, Priscilla. He told her that his name was Terry, that he was from Patient Relation Software, and that he was filling in for Kenneth, who was out sick. After flattering her ("Dr. Y says you're the real brains of the operation"), Terry explained that he needed to make a critical security update (version 10.1) to Dr. Y's software system. If it didn't happen right away, he added, her system could be the one that allowed hackers access into patient files. Immediately, Priscilla felt personally responsible.

Because Kenneth was out sick, Terry explained, he didn't have the username and password to dial in to Dr. Y's server and make the changes. He told Priscilla that as soon as the changes were made, he would call her back and let her know so that she could change her password. It was critical, he said, to change it as soon as he called in order to maintain security. In fact, he added, he would just send her a message on the social networking site, if she told him her username. She shared that as well, thereby giving him access to all of her friends who filled a similar role at other medical offices.

Knowing that Patient Relation was in fact the software package her office used to track patient records, that they were currently using version 10.0, that Kenneth was the name of their regular technician, and that she didn't want to be responsible for a data breach, Priscilla never suspected she was being socially engineered into revealing highly sensitive information. She gave Terry her password and, thus, full access to more than 17,500 private patient records, including their Social Security numbers, insurance data, medical histories, and even blood types.

Takeaway: "It used to be about who we trust. Now it's about how we trust," said Sileo, who gives his clients a three-step process to instill in employees in order to repel a social engineering attack.

The hogwash reflex: Training includes having employees develop a catchword or phrase that will go off in their head when someone requests information. "You immediately have a trigger event," he said "A word that pops into your head that reminds you that you may be at risk."

Ask the right questions: Teach employees to ask "Can I call you back at XYZ Software to verify you are who you say you are?" If they get an excuse, they should know immediately it's a red flag to do more research without giving up information."

Stop. And think through the options: Instead of being hurried through an event and acting on a panic reflex, take it slow and consider what you need to do in order to maintain privacy.

The Hurt Locker

There is a lot of theft from women's lockers at work-out facilities. What happens is a woman goes to work out, puts her cell phone and wallet into a locker and puts on a combination lock. Somebody who has recorded it with a mini-camera standing behind her knows the combination. They get into it, open up the cell phone, click a few keys, close it up and put the cell phone back in the locker. Grab the wallet or purse, close the locker, lock it and leave.

The woman comes back from working out, gets into her clothes, grabs the cell phone, goes for the wallet: It's missing. They usually think first they've left it in the car or out front. As they are walking out, the person who stole the wallet is there. They ring their phone. They say "This is Whatever Bank and we have reason to believe someone is trying to cash-out your account. Has your purse been stolen recently?"

The person is immediately in a panic and willing to do whatever it takes to make herself safe. The bank person on the other end, who is not actually a bank person, says, "Hey, we are here to protect you. That's what we do. But In order to shut down access to the account, I need to verify your Social Security number."

It may sound stupid on the outside looking in for someone to give up their social security number, but when you are in a panic, 90% or so of people will give that information away. And then the person will also say, "OK, we can shut down the card, too. What is your PIN?" Because they are rushing through it, because they are in fear, they don't give it a second thought.

Takeaway: It goes back to point three of Sileo's three steps. Take control of that interaction, he says. "Stop and ask yourself, "'Should I call the bank myself? Should I contact them to let them know what is happening?" If you just slow down and take control, that gets rid of the majority of social engineering."

IV. Social Engineers in Action

Pickup Lines

Social networking sites, corporate offices and anywhere on the Web are all common places for scammers to ply their trade, with the intent of stealing identities, hijacking accounts, infiltrating corporate systems and making money. Here are some of the most prevalent social engineering tactics, targeting social network users, office workers and Web users.

ON SOCIAL NETWORKS

"I'm traveling in London and I've lost my wallet. Can you wire some money?"

How it works: The scammer poses as a "friend" on Facebook or another social networking site, sends a message claiming to be stuck in a foreign city with no money (due to a robbery, lost wallet or other problem) and asks the recipient to wire money. Users need to be wary that because criminals can hack accounts and pose as a "friend," they cannot always be 100% certain of the identities of the people with whom they interact.

"Someone has a secret crush on you! Download this application to find who!"

How it works: Facebook has thousands of applications users can download, but not all are safe. Some may install adware that launches pop-up ads, while others expose personal information to third-parties. Users need to be judicious about which applications they use.

"Check out this link!"

How it works: An email or other message—sometimes seeming to originate from a friend—encourages users to click on a link that lands them on a bogus site and asks them for personal information, such as their password or account number. The site may look authentic, but it is actually designed to capture such information for the scammers' gain. An example is a Twitter spam campaign that asked recipients, "Did you see this video of you?" The link led to a fake Twitter Web site that asked for the user's password.

IN THE OFFICE

"This is Chris from tech services. I've been notified of an infection on your computer."

How it works: Posing as technical support people, scammers call business users, tell them their PCs are infected and then offer to help them get rid of it. Playing on the user's vulnerability and fear, the scammer purposefully ratchets up the technical difficulty of the "fix," and as the user grows more nervous, they offer to fix it themselves—which of course requires the user to reveal his or her password. The strategy exploits people's discomfort with technology.

"Hi, I'm the rep from Acme, and I'm here to see Nancy." How it works: Scammers pose as a legitimate visitor (a client, sales rep, service technician, etc.) and use their knowledge of the company—even a shirt bearing an authentic logo—to gain the confidence of the receptionist. Criminals can take weeks and even months to get to know an organization before even coming in the door. Knowing who to ask for, how to act and how to dress is often all it takes for unauthorized access a facility. An example is a 2007 diamond heist at the ABN Amro Bank in Antwerp, Belgium, where an elderly man, pretending to be a successful businessman, offered the female staff chocolates and eventually gained their trust with regular visits. Ultimately, the bank lost 120,000 carats of diamonds because the man was ultimately able to gain off-hours access to the bank's vault.

"Can you hold the door for me? I don't have my key/access card on me."

How it works: Fraudsters wait outside one of the facility's entryways—the front door or the smoking area, for instance—and pose as a fellow office mate. Workers hold the door open, allowing them to gain access, never thinking to ask for a badge proving they have permission to enter. Even when credentials are required, criminals are getting better at using high-end photography to print authentic-looking badges.

PHISHING LURES

"You have not paid for the item you recently won on eBay. Please click here to pay."

How it works: Users receive emails impersonating companies like eBay, claiming they have not yet paid for a winning bid. When they click on the provided link, it leads to a phishing site. The ploy plays to people's concerns about a negative impact on their eBay score. Rather than clicking on this type of email, experts recommend that users go directly to the Web site of the business involved by typing the URL into the browser bar.

"You've been let go. Click here to register for severance pay."

How it works: Criminals take advantage of economic uncertainty and increased digitization by sending an email to employees with a malicious link that appears to relay news that requires a quick response, such as, "We are sending out W-2 forms electronically this year."

TARGETED ATTACKS

Social engineering tactics are becoming increasingly specific, with criminals targeting individual people and dedicating more time to gaining personal information, with hopes of a larger payoff. Here are five of these more involved—and more lucrative—types of scams.

"This is Microsoft support —we want to help."

How it works: Scammers pose as a Microsoft tech support person and claim to be calling all licensed Windows users whose PCs are generating an abnormal number of errors due to a software bug. Victims are instructed to go to the event log, which can be particularly alarming to inexperienced users because, in fact, most Windows event logs do record many small errors. Many people at this point will be ready to do whatever the alleged support person instructs, which in this case is to go to a remote access service, Teamviewer.com, that gives the scammer control of the machine.

From there, the criminal installs malware that will grant him or her continual access to the PC.

"Donate to the hurricane recovery efforts!"

How it works: Shortly after a major earthquake, tsunami or other disaster, fake Web sites pop up, targeting people concerned about loved ones in the affected region and claiming to have specialized resources, such as government databases and rescue effort information, to help find victims. The sites collect names and contact information and use it to solicit charitable donations. The caller takes advantage of the victim's heightened emotions to obtain his or her credit card number. With all this information—name, address, a relative's name and a credit card—they are armed to commit identity theft. In some cases, criminals launch secondary attacks, such as posing as a bank representative, asking for the victim's Social Security number to verify the charity donation's legitimacy.

"About your job application…"

How it works: Social engineers are targeting headhunters and businesses by embedding malware in email responses to job postings. According to a warning from the FBI, more than $150,000 was stolen from a U.S. business via unauthorized wire transfer. The attacker responded to a job opening posted on an employment Web site, and through the malware, obtained the online banking credentials of the person authorized to conduct financial transactions within the company. By changing the account settings, the criminal redirected the sending of wire transfers to his own accounts. Many organizations now require job seekers to fill out an online form rather than accept resumes and cover letters in attachment.

"@Twitterguy, what do you think about what Obama said on #cybersecurity? http://shar.es/HNGAt "

How it works: Social engineers are observing Twitter trends to launch attacks. One example is the hijacking of legitimate hashtags with the purpose of embedding malicious links into the tag. Once tweeted, the malware redirects users to a phishing Web page with nefarious intent, whether it's stealing Twitter account information or launching even more malware. Scammers are also targeting individuals by learning about their interests and then sending a legitimate-sounding tweet that invites them to click through to what turns out to be a phishing site.

"Get more Twitter followers!"

How it works: Another Twitter-oriented ploy is to send a tweet that promises it can increase your followers if you click on a link. The link takes the user to a Web service that asks for their Twitter credentials. Of course, no legitimate third party would request this information, which should be users' first clue that they are being scammed.

True stories

Hiding in Plain Sight

In February 2009, Chris Nickerson, founder of Colorado-based security consultancy Lares, conducted an on-site vulnerability test for a retail company with a large call center. With some prep work, Nickerson says the team was able to gain access to the company's network and database quite easily. Here is an account of how he did that.

"I started off by gaining information on the target. There was a large horserace going on in the area, and in the town where the company was located, it was the big thing to go to this horse race. Everyone in the city and around it left the office to go to it. That was a perfect time for me to come in and say I have an appointment.

I said I had to meet with someone we'll call Nancy. I knew Nancy wasn't going to be in the office because on her MySpace profile it said she was getting ready to go to the race. Then her Twitter profile said she was getting dressed to go to the event. So I knew she wasn't in the office.

Before I went to the office, I went to a thrift shop and got a Cisco shirt for $4. Then I went in and said "Hi. I'm the new rep from Cisco. I'm here to see Nancy." The front desk attendant in this situation said, "She's not at her desk." I said "Yeah. I know. I've been texting back and forth with her. She told me she is in a meeting and the meeting is going over."

This was right around lunch time, and I said, "Since I'm waiting, is there anywhere around here where I can go get some food?" I knew full well that after surveying the area, the closest thing was about five miles away because they were sort of out in the sticks.

The receptionist said "Four or fives miles down the road there is a McDonalds. But we have a nice cafeteria here. If you want, you can just eat in there." Being allowed to go to the cafeteria gave me full access to the facility because the only thing that was guarded was the door. The cafeteria led right into the rest of the building.

So I went into the cafeteria and ate. While I was there, I did USB key drops. I put files on them with names like "Payroll" or "Strategy 2009." The USBs had rootkits on them. Many contained an autorun rootkit. Others had Hacksaw, which is a little piece of tech that you can use with a U3 drive. You plug it into a machine and, if the machine has auto-run on the CD-ROM running it, it will just start dumping all the passwords, usernames, all that. It will also put a hook into the machine to start emailing that information out to an email account that you give it to contact. So, even after I left, I could still be filtering information. It only takes about 30 seconds to enable itself.

When I do this kind of exercise, I put USBs in areas that people are in where they might forget something: The bathroom, for instance, on the sink. Another good area is near the coffee machine —areas where people naturally put things down where they might not remember to pick it back up. I've never done USB key drops without success.

Meanwhile, I had another one of my guys go in through the smoking door in the back. He hung out, waited, had some cigarettes with people who came out to smoke on break, and when they were done, the door opened and he just cruised in. Yet another exercise to prove it really doesn't

take much to get inside.

Eventually, once he was in, I had him come and get me in the cafeteria. That was so it appeared on the security tapes as though someone was coming to get me out of the cafeteria to escort me to whatever meeting I was going to attend. We went through and found inside of this giant 100,000-square-foot cube farm a few seats that were wide open and just sat down.

There was no one around us. So, we started pulling keys. We used things like Ophcrack to start cracking Windows passwords and dump them into Linux. We started putting our machines on the networks so we could start doing pen testing and hacking active servers in the environment. We put up things like WRT 54G routers: the little blue Linksys wireless units. We took those, stuck them under a cube, put Unix on them and opened WRT. That made it so I had a wireless access point I could hit not only from the parking lot, but it also beacons and calls home so I had a Unix box that sits inside their network.

A short time later, a full team of people came in. A lot of the work that was done at this facility was shift work, and it was shift change time. Because we did our homework right, we were at the two of three cubes that were vacant so there were no conflicts or questions.

Everyone sat down around us. I announced myself as the Cisco engineer who was working on the phone system. Many of them responded with jokes and said things like, "Honey, please don't fix it. I don't want to take any calls today."

One thing I have learned is that cookies are the keys to everyone's heart. When I'm doing the type of exercise where I'm posing as a tech, or a VAR, I like to bring cookies. I did for this exercise, and I started passing out cookies to everyone in the area. We were all laughing, having a great time. Meanwhile, we were in the middle of hacking their entire network.

In the end, what we exposed for the client was the vulnerability of their physical access, and we showed them some of the blended techniques we used to get in. We were able to demonstrate how, with social engineering, we were able to hack the SQL Server and dump the whole database of everybody's account information. This kind of breach could have cost them multiple billions of dollars. And we had access to all of it because of these vulnerabilities. We wore button cams and hat cams so they could watch how it was done.

Companies need to run a general social engineering awareness campaign. You need to tell employees what to look for and how to look for it. Companies need to teach employees that it's not that the company doesn't trust the people within the organization; it's that there are people out there trying to do this every day. It is just a good awareness technique to do it.

If someone is coming to work on your environment, you should probably know who they are. If you think of your company like your home, you do things differently. You are not going to just let someone walk into your house. That is the kind of philosophy companies need to inject into the corporate culture."

Inside a Scammer's Mind

CSO got to experience a vulnerability assessment first-hand when Chris Nickerson, founder of Colorado-based security consultancy Lares, agreed to take a look at one of the buildings in our area. He pointed out areas of weakness that a criminal might look for when sizing up a facility's potential for a breach.

One of the first things Nickerson did was point out that the building's generator was both uncaged and unlocked. He even went up to the generator and opened the doors. About 10 minutes later, we were approached by a man who introduced himself as the facilities manager.

"Hi, how are you doing?" Nickerson said casually, as he walked up to the approaching man.

"I understand you were looking at the generator and opening the doors on it. I got a security call," the facilities manager said, clearly concerned.

"Actually we are doing a security assessment and pointing out things around the building," said Nickerson

"OK, and who do you work for?" the man asked.

Nickerson said we worked for CSO, and the manager seemed satisfied with that answer.

"Alright, very good," he said, as he left us to continue our assessment.

"I have absolutely no credentials on me that verify that," noted Nickerson. "So we were just allowed to fully access the building, poke at stuff, and now we have a point of verification that is trust. Now we can go in and be even worse with the camera because we already have a pre-verified point, and we know security has been called on us for opening generators. They are now actually going to help us into the building knowing full well what we are doing, even though they have no reason to believe us."

Nickerson said during his team's assessments, questions from client staff come up all the time. This is a common occurrence, and his skill at the fine art of BS is obvious.

"People are usually good about asking what you are doing," he said. "But once you give them a viable excuse, they let you go. As long as you do your intelligence right, you will never get caught. People don't like confrontation."

We spent about 20 more minutes photographing the building and poking around. The facilities manager checked back on us before we left and asked for more details of our project.

"I just want to be clear that people are watching, and I am getting calls," the facilities manager told Nickerson.

However, at that point, we had already collected enough information about the building to make any criminal's mouth water.

As we were heading out, we saw the manager at the generator, taking stock of its unlocked state.

"Hey you know what? I think we've already secured the

building," Nickerson laughed. "See? Security assessments change facilities."

The staff at the building we examined does get credit for being observant. While Nickerson said none of the interrogation we dealt with during our time there would have deterred him in the slightest from getting his job done, we weren't completely unnoticed.

Pranking the Superbowl

Comedian Sir John Hargrave is known for his comedy Web site, Zug, as well as his comic stunts. One of his highest profile stunts—at the 2007 Superbowl—involved some key tenets of social engineering. The stunt involved Hargrave and his team distributing thousands of "party packs," containing light-up necklaces, to spectators in specific seats at Dolphin Stadium in Miami. The party packs contained instructions for attendees to turn on their necklaces when Prince's half-time show began. When lit, the lights would display a message advertising Hargrave's Web site.

To orchestrate the stunt, the team wore shirts that Hargrave ordered with embroidered logos and carried fake laminated badges to pass themselves off as event workers. Hargrave had a genuine press pass, but the only legitimate credentials the rest of his group had were game tickets.

Of course, this was the Super Bowl, so security from local, state and federal agencies was on full alert, employing blackhawk helicopters, bomb-sniffing dogs and gamma-ray scanners. Nonetheless, Hargrave and crew were able to drive two delivery vans through the stadium's high-security delivery gate, obtain Homeland Security background checks on-site and store the boxes in the stadium garage overnight.

On game day, Hargrave used his press pass to gain early access to the stadium and move all 100 boxes to the targeted sections. When his team joined him, they distributed the boxes to each row of seats, just in time for half-time. While there is no documentation that the necklaces successfully broadcast Hargrave's message, there is little reason to doubt Hargrave's claim of breaching the stadium's security using social engineering tactics.

Key to the prank's success, Hargrave says, was looking official; while his crew wore their logoed shirts, Hargrave himself wore a suit and a Bluetooth headset. "If you look the part, people give you credit you don't deserve," he told CSO Magazine in an interview [http://www.csoonline.com/article/221349/zug.com-prince-of-pranks]. "Security's trained to look for someone "suspicious." The group also practiced for hours the day before the stunt until they felt they could pull off a business-like demeanor.

Second, Hargrave says, was initiating conversations with stadium staffers, asking for help. "People want to help, and once they do, they don't want to suspect they just helped someone they should have been suspicious of," he says.

Social Network Scams of Yesterday and Today

Lady Gaga and Wikileaks

The highly classified government information that was exposed on Wikileaks in 2010 could not have been obtained without successful social engineering, says Chris Hadnagy, author of Social Engineering: The Art of Human Hacking (Wiley, 2010). U.S. Army soldier Bradley Manning—accused of passing classified information to Julian Assange, founder of Wikileaks—was serving as a support battalion in Iraq. Manning obtained the material through his access to the Secret Internet Protocol Router Network used by the U.S. Department of Defense and Department of State to transmit classified information.

Former hacker Adrian Lamo—who reported Manning to authorities—told officials that Manning said he had downloaded material from SIPRNet onto CD-RWs. He allegedly managed to fool colleagues into thinking he was listening to music, rather than stealing classified information.

"I would come in with music on a CD-RW labeled with something like, 'Lady Gaga' ... erase the music... then write a compressed split file," Manning wrote in an online chat with Lamo. "No one suspected a thing. (I) listened and lip-synched to Lady Gaga's Telephone while 'exfiltrating' possibly the largest data spillage in American history."

"He played on the trust of the people inspecting him going in and out," noted Hadnagy. "And he had to keep his cool. I imagine if you are downloading classified government information that could get you a court martial, you have got to have nerves of steel."

Following the leak, social engineers began sending out messages asking, "Do you want to read the Wikileaks file? Here it is," says Hadnagy. "The attachment or link was a pdf, a really slick pdf. The Javascript they wrote would search the computer, find the version of Adobe reader running on the machine, and then launch the exploit for that version." Although the malware took some time to load, the ruse worked because victims were expecting a sizable document, Hadnagy says.

Getting to Know You Through Google

Google made headlines at the beginning of 2010 by revealing some of its services had been breached by Chinese hackers, who, according to Google officials, wanted to access the Gmail accounts of Chinese human rights activists. Several other companies were also targeted, including Yahoo, Adobe Systems and Symantec.

The hackers' success depended, in part, on carrying out a lengthy reconnaissance of Google employees. By using information they found in several places, including social networks, they were able to send what looked like legitimate messages to employees that appeared to be coming from a contact or friend. Employees then clicked on links contained within the trusted message, and spyware was installed on the machine.

"These attackers really went all out," says Hadnagy. "It must have taken a considerable amount of time to do this kind of information gathering and reconnaissance to get to the point where they could interact with targeted employees in a way that would allow them to elicit this kind of information"

Hadnagy says the incident highlights the security dilemma posed by social networks, which are now considered a vital part of the marketing strategy for many organizations. "So many companies use social media to transmit their marketing message to the world. But in another sense, they outline their whole company structure. And if a social engineer wants to use that, it's out there and easily accessible. That is what these Chinese hackers used, and it's what made this attack successful."

Hey Amazon, Where's My Order?

Businesses that use Amazon.com to sell their products were the target of a late-2010 scam. The ploy was discovered by researchers with GFI Software, who warned Amazon that cyber thieves were generating fake receipts in an attempt to report lost orders, with the goal of obtaining refunds or valuable products.

"The free program available online allows scammers to create an HTML 'receipt' for phantom Amazon.com purchases. By capturing a screenshot of the fake receipt, these cyber criminals are able to email unsuspecting sellers claiming they are missing items," says Christopher Boyd, senior threat researcher for GFI Software, in a post.

"Get the dislike button!" "Win a free iPad!"

There is a new deceptive tactic every day on Facebook that attempts to con users into clicking on malicious links, or filling out scam surveys. "Even the savviest user will sometimes click," Hadnagy says. Common results include malware installation or a survey that either generates commission money for the scammer or asks you for personal information that is stored in a database and used for identity theft. While the tricks may change from month to month, the end game is likely always going to remain, said Hadnagy. Expect to see ongoing social engineering scams on Facebook.

Careful Who You Friend

The Facebook Pwn tool is a good example of where social engineering is headed, particularly scammers' growing use of information obtained via social networking sites.

Here's how it works: In 2011, a group of security researchers based in Egypt created a tool, described as a "Facebook profile dumper," intended to educate users about how easy it is to be scammed on Facebook. The cross-platform, Java-based tool, which they released for general use, automates the collection of hidden Facebook profile data that is otherwise only accessible to friends in a user's network. According to the description released by the developers, the tool sends friend requests to a list of Facebook profiles, and once a victim accepts, it dumps all their information, photos and friend list to a local folder.

In a typical scenario described by the researchers, the scammer gathers information from a user profile by creating a new account. Then, using a "friending plugin," the criminal can add all the victim's friends, which ensures the scammer shares some common friends with the victim. Next, a cloning plugin asks the scammer to choose one of the victim's friends. The plugin clones the display picture and the display name of the chosen friend and sets it to the authenticated account.

Afterward, a friend request is sent to the victim's account. As soon as the victim accepts, the dumper starts to save all accessible HTML pages (info, images, tags, etc.) for offline examining. "After a few minutes, the victim may unfriend the fake account after he/she figures out it's a fake, but probably it's too late," the researchers explain in their post.

The scammer now has access to a host of information with which to execute a number of very targeted social engineering attacks. The more personal details criminals have at their disposal, the more convincing their attack can be. For example, a victim is more likely to open a malicious email attachment used in a spear-phishing attempt if it looks legitimate.

The researchers said the main goals for releasing the tool is user awareness for what is already happening in the world. "This tool should make the people aware of the implications of their actions online," Saafan told CSO in an email. "Accepting friend requests for even the smallest period of time without manually verifying that the friend is actually who he claims to be, is an example of wrong actions that we wanted to demonstrate."

Saafan also said he hopes to bring attention to what he considers to be Facebook's flawed user verification process. "I think Facebook should have a more strict policy for verifying that people are who they claim to be, and filter out fake or impersonating accounts," Saafan wrote.

Mobile Scams. Now that mobile devices have become a key part of our lives, social engineering is an attack method of choice to gain access to a person's smartphone or tablet. Information security expert Lenny Zeltser, senior faculty member with SANS Institute and an incident handler at the Internet Storm Center shares three examples of current cons being used by criminals to get inside your mobile device.

Malicious apps that look like legitimate apps. Scammers are taking advantage of popular mobile apps by developing malicious apps that look just like them. One example is an Android app that caused virtual "steam" to appear on mobile device's screen. "You could move your finger to scrape the virtual steam off," Zeltser explains. "People love this sort of thing."

Many people were conned into purchasing the malicious app instead of the authentic one because it was dif-

ficult to distinguish between the two of them. In some cases, Zeltser says, the malicious version activated an SMS message requesting premium services, for which the victim was charged. The attacker, meanwhile, was able to delete all return SMS messages acknowledging the charges, so the victims had no idea they were being billed. "In this scenario, the victim had no indication that the phone was sending messages or receiving any kind of notification of the charges—they would just get a large phone bill," Zeltser says.

According to Zeltser, Google removed over 50 malicious apps from the Android Market in Spring 2011 that were variants of the DroidDream trojan but looked like legitimate applications, with names like Super Guitar Solo.

"The advice we're giving people outside of the mobile world is, don't install applications that come from untrusted sources," says Zeltser. "That same advice applies now to mobile." Users cannot rely on an app's ratings because many people might not even realize they are using malicious apps.

Malicious mobile apps that come from ads. Malicious ads are being embedded in legitimate mobile apps. In one case, victims were invited to click on a link asking them to install an application to optimize battery consumption. "In the desktop world, we are seeing malicious ads as an incredible infection vector because they allow the attacker to present potentially malicious code into the browser of hundreds of thousands of victims. Now we are seeing this happen in a mobile environment too, to where ads are being placed in legitimate applications," Zeltser says.

Apps that claim to be intended for "security." Another new mobile attack vector is a ZeuS malware variant. When users visit a banking site from an infected PC, they are prompted to download an authentication or security component onto their mobile device in order to complete the login process, says Zeltser. "The attackers realize that users are using two-factor authentication," he explains. "In many cases, that second factor is implemented as a one-time password sent to the user's phone by the banking provider. Attackers were thinking: 'How can we get access to those credentials?' Their answer is: 'Attack the user's phone.'"

Once the PC is infected, victims log onto their bank account and are told to download an application onto their phone in order to receive security messages, such as login credentials. But it is actually a malicious application from the same entity that is controlling the user's PC. Now they have access to not only the user's regular banking logon credentials, but also the second authentication factor sent to the victim via SMS. In many cases, says Zeltser, people thought they simply were installing security applications, or in some cases, a security certificate.

"When people think something is done for security, they forget all logic and reason," he says. "They just blindly do it."

Forget fly-fishing; let's go spearfishing!

The criminal art of spearphishing—email spoofing that aims to get the recipient to click on a bad link or attachment—has been around for years. But that doesn't mean it's become any less effective. According to figures from the U.S. Computer Emergency Readiness Team (US-CERT), phishing attacks accounted for 53% of all security incidents in 2010.

What has changed is that more phishing attempts are direct, targeted efforts aimed at specific individuals within an organization. In fact, after the breach of an email database maintained by marketing firm Epsilon, security experts warned that banking customers should worry about a wave of spearphishing attacks utilizing the information gained from the break-in.

The days when phishers would blast out hundreds of generic messages in hopes of a few hits are ending. Criminals now realize a message with specialized, social engineering content that is directed at one person or a small group of people can be much more successful. After all, it typically only takes one machine to compromise an entire network.

"We now see more of the scenarios involving just two or three emails targeting the executive team, which spoofs the legal team and contains a malware attachment that talks about pending litigation," says Jim Hansen of the security awareness consultancy PhishMe.