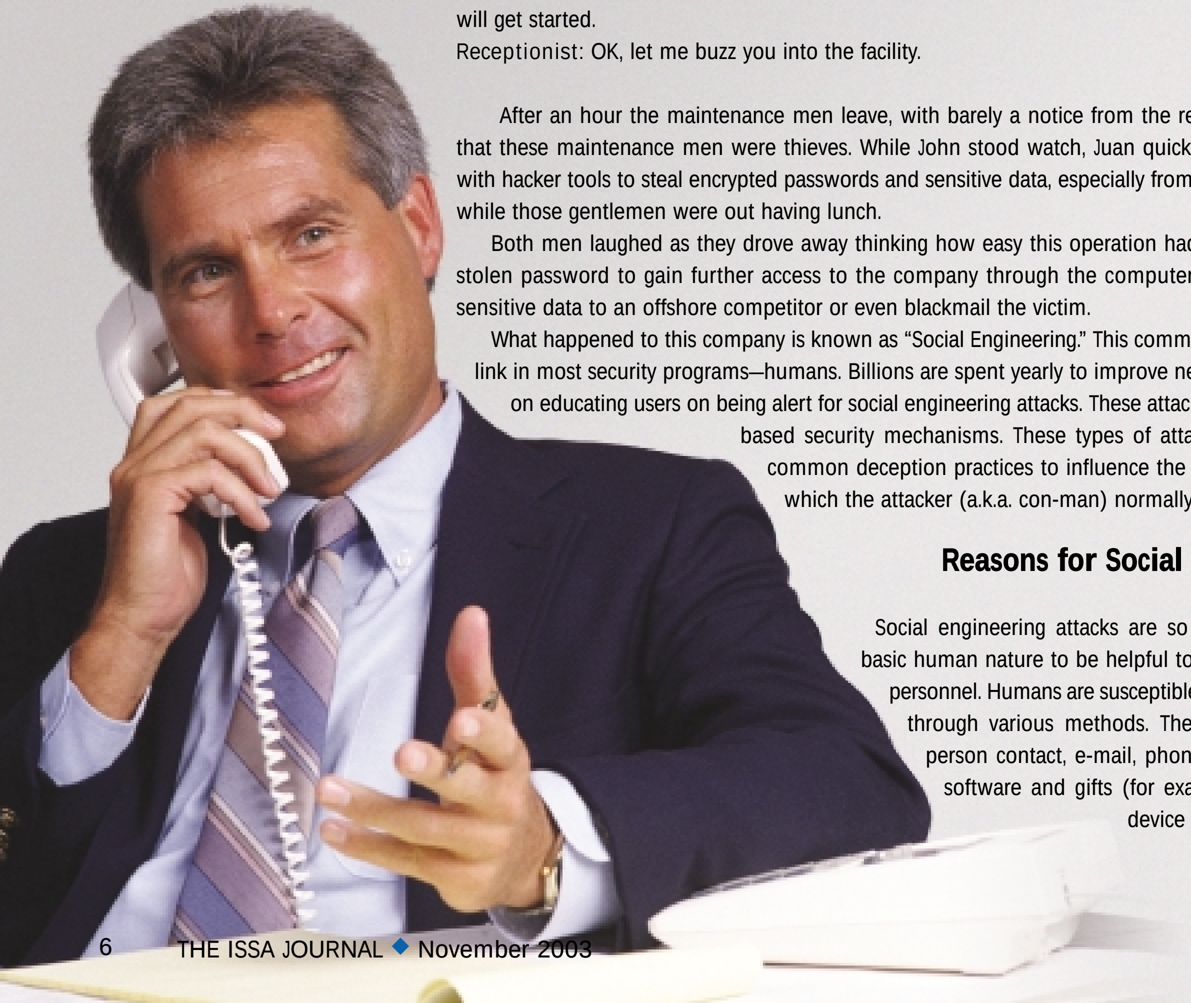
A HACKER WILL BE WITH YOU SHORTLY: SOCIAL ENGINEERING 101

By John Bumgarner

Maintenance Person: Hello, I am John from Acme Heating and Air and this is Juan. We are conducting an assessment of your ventilation system for any containments. This is part of a yearly inspection, which is covered under the building's maintenance contract.
Receptionist: OK, what do you need from us?
Maintenance Person: Nothing. The inspection should take around an hour. We have all the equipment so we will get started.
Receptionist: OK, let me buzz you into the facility.



After an hour the maintenance men leave, with barely a notice from the receptionist. She does not realize that these maintenance men were thieves. While John stood watch, Juan quickly used floppies and USB drives with hacker tools to steal encrypted passwords and sensitive data, especially from the CEO's and CFO's computers while those gentlemen were out having lunch.

Both men laughed as they drove away thinking how easy this operation had gone. They could now use the stolen password to gain further access to the company through the computer network and they can sell the sensitive data to an offshore competitor or even blackmail the victim.

What happened to this company is known as "Social Engineering." This common tactic focuses on the weakest link in most security programs—humans. Billions are spent yearly to improve network security, but little is spent on educating users on being alert for social engineering attacks. These attacks essentially bypass technology-based security mechanisms. These types of attacks are nothing new; they use common deception practices to influence the victim to provide information to which the attacker (a.k.a. con-man) normally would not have access.

Reasons for Social Engineering

Social engineering attacks are so successful because they target basic human nature to be helpful to someone like the maintenance personnel. Humans are susceptible to persuasion and manipulation through various methods. These methods include person-to-person contact, e-mail, phone conversations, snail mail, free software and gifts (for example, a statue with a listening device or micro-camera). The listening device may seem extreme, but it is possible when the attacker is being funded to conduct the operation.

Social engineers typically fall into three categories. These include internal, external and trusted. Internal threats come from employees, who can manipulate other employees to obtain sensitive information or passwords to critical systems. External threats include competitors, hackers or professional criminals. Trusted threats come from individuals who have regular access to your organization. These individuals include consultants, sales representatives and contractors.

Social Engineering Methods

The steps used by social engineers to study a target are similar to those used by spies working for intelligence agencies. These steps are (1) information gathering, (2) target selection, and (3) target interdiction. The social engineer starts by gathering as much information about the organization as available. Information comes in a variety of forms, which include: (1) white (a.k.a. open source), (2) gray (such as conference materials) and (3) black (such as internal documents). Open source information can be obtained from the Internet, especially from the company's web site or by performing key word searches for the company name or e-mail addresses (@targetcompany.com). Company's dumpsters can provide information like telephone numbers, employee rosters and even passwords. If a specific item is being targeted, then the attacker may gather gray and/or black information. Gray information is usually obtained from conferences where members of the organization are making presentations on items of interest. Gray information could include white papers and briefing slides. Black information is the most difficult to obtain prior to the mission, because the data is normally internal to the organization. Black information is not intended for public disclosure and is usually sensitive in nature.

Once the attacker has gathered all the information, the data is analyzed to determine the best location to interdict before moving to the high-payoff target (for example, new soft drink recipe). The best avenues to gain further access include the organization's help desk, technical support, the receptionist and other company personnel. The attacker now needs to establish short-term trust with one of these parties to gain additional information. Some of the techniques used to establish this trust include: (1) playing the role of an end-user with the help desk, (2) playing the role of a technician with the receptionist, (3) playing the role of an authority with the technical support group, or (4) sending e-mail to select end-users with links to download a new application that could benefit their work. The latter requires more work because the attacker must create a false Web site with information about the application, which may include fake press releases, news articles and white papers.

Social Engineering Categories

Social engineering attacks fall into one of four categories. These categories include: (1) ego attack, (2) sympathy attack, (3) intimidation attack and (4) technical attack.

The "ego attack" targets someone who is frustrated with their current job position. The attacker appeals to the victim's vanity and makes the person feel knowledgeable about the subject the attacker is interested in. The attacker normally pretends to be a law enforcement officer, which makes the victim feel honored in helping. The victim usually never realizes what has happened, even after the attack is over.

The "sympathy attack" normally plays on the empathy and sympathy of the victim. The attacker pretends to be a fellow employee, contractor or vendor who needs some type of information urgently. The attacker usually suggests that he will lose his job or get into trouble if the victim does not provide assistance. Sympathy attacks are very successful because the attacker can "shop around" until he finds someone that will assist him.

The "intimidation attack" normally uses authority to coerce the victim into cooperating with the attacker. The attacker usually pretends to be someone of influence like the CEO or law enforcement official. If the attacker portrays a law enforcement official, he will inform the victim that they are conducting a secret investigation and that it should not be discussed with anyone. Victims who attempt to resist are normally threatened with criminal charges or termination.

The final attack is the "technical attack." The attacker usually has no direct interpersonal contact with the potential victims. The attacker uses forged e-mail, phony Web sites or other items (for example, software CDs) to establish contact with the victim. In forged e-mail attacks the attacker usually portrays himself as a system administrator or support person. Phony Web sites can be used to lure a victim to download new screen savers or utilities. The attacker can even embed JavaScript in the Web page's source code, which can upload documents or install software on the victim's system.

All these attacks are normally successful in gaining additional access or information from their intended victims. One of the easiest methods to penetrate an organization's security is being hired as part of the janitorial staff. Janitors normally have full access to the facility after hours and can go undetected for months or even years. I personally used this method several times to obtain access to client's facilities as part of "Red Team" exercises. Another attack method that works is creating a phony mobile destruction service, where you shred papers and hard drives for companies. All it takes to be successful is being cheaper than their current service and have shred bins that look official. Once the bins are in place you just have to send someone to collect all the sensitive documents in the receptacle.

Measures to Counteract Social Engineering Attacks

Social engineering attacks are the single greatest threat to enterprise security and the hardest to prevent. Organizations can take measures to mitigate these attacks, but nothing can prevent them totally.

The first measure is to establish policies concerning methods used by social engineers to gain access. These policies should cover items like the physical access to buildings, access to server room, access to wiring closets and password resets for users. Policies should also include end-users' role in enforcing these policies and penalties for non-compliance.

The second measure is to create an awareness program that focuses on social engineering attacks. This program could include the creation of cartoon posters with themes about password resets, physical access and wearing badges when in the building. The posters can be placed in the break areas or company bulletin boards. A bi-monthly security newsletter should also be part of the awareness program. The newsletter can focus on a variety of security topics to include social engineering.

The third measure is to establish an education program that outlines company policies and procedures. Education is the primary defense against social engineering attacks. Employees should be required to attend the training annually and acknowledge they understand the policies by signing a compliance document. Establish role-playing exercises to emphasize the threat posed by social engineering attacks and how these attacks succeed. An example of such an exercise is:

Social Engineer: Hi, this is John Brown from graphics. How are you doing today?
Help Desk: I'm doing fine, how are you doing?
Social Engineer: I am doing OK. I worked late last night on some new graphics for the company's Web site and got very little sleep. This lack of sleep has caused me to forget my password this morning. I need to have it reset so that I can complete these graphics by my deadline this afternoon. Could you reset it for me?
Help Desk: I am sorry that you had to work late. I would be happy to reset it. Your userid is jbrown correct?
Social Engineer: Yes, that is correct.
Help Desk: OK, I have reset your password to password. You will be prompted to reset it on first login. Do you need anything else?
Social Engineer: No, thanks for the reset. I hope that you have a great day. 'Bye.

The fourth measure is to test your program's readiness periodically. Testing this program unannounced is the best method to assess its effectiveness. Testing measures could include sending e-mail messages to a select target group that installs a new background to their desktop. The background could state, "Your system has been compromised by the Acme Product's Security Team as part of a compliance test. Please read the Acme Product's policy on accessing unknown e-mails." Another way is to send bogus compact disks with information about testing a new application and a chance to win a prize (a car, trip, etc.). When the victim inserts the disk into their computer the autorun feature executes an application that creates a folder on the desktop named "Compromised Security!" Inside the folder are copies of items from the victim's "My Documents" folder and the company security policy on installing unauthorized software. Other methods include calling the help desk posing as an end user and trying to get a password reset or having someone pose as a maintenance person that needs access to the data center.

The fifth measure is to establish incident teams, which can respond to security incidents when they occur. Members of this team are like emergency responders and only respond when called. Team members should be trained to stop and contain the incident quickly without causing additional damage and while maintaining evidence for legal actions later. This team should also be tested periodically to ensure their procedures and methods work under stress.

Conclusion

Organizations should be on the lookout for social engineering attacks because they have destructive consequences when successful. By increasing user awareness about such attacks, organizations can limit the success and damage posed by the attacks.

John Bumgarner, M.A., CISSP, GCIH, IAM, SSCP, is the founder and president of Cyber Watch Inc., which offers strategic, operational and tactical security consulting to a variety of clients. Previously John worked with several U.S. government agencies, including the United States Special Operation Command, Central Intelligence Agency, National Security Agency, Defense Intelligence Agency, and others. He has written articles for Security Management Magazine *and has spoken at several conferences on information security topics. John recently developed a product called PassGuard™ used to protect passwords and sensitive accounts from hackers.*