Global Information Assurance Certification Paper

Social Engineering: Information Bandits

Mandy Page

GIAC Security Essentials Certification (GSEC)

Practical Version 1.4c

Option 1

Submitted 11/23/04

Table of Contents

Abstract

Information Bandits use many techniques to get confidential information. This paper will discuss the techniques of impersonating, dumpster diving, eavesdropping, bribing, stealing, tailgating, shoulder surfing, namedropping, phishing and reverse social engineering. Then we'll look at ways to avoid being a victim of these social engineering techniques.

Introduction

Information Bandits are people who try to obtain confidential information using social skills. They use social engineering to get small pieces of information using different techniques. Social engineering is the practice of conning people into revealing sensitive data on a computer system. Once all the pieces are collected the Information Bandit can then put them together like a puzzle. They now have the information needed to gain unauthorized access to a valued system or information and can use this for malicious behavior.

Impersonating

Impersonation is the act of assuming the character or personality of another person. Information Bandits use impersonating for fraudulent reasons. They will pose as somebody who most people would trust easily. They may call an employee and pose as IT support. Using their social engineering techniques the Information Bandit will try to get the employee's password, user id, or other confidential information. They may use the excuse that they need this information for testing a new application or they need to resolve a current system problem. This catches the victim off guard and makes the situation seem urgent. The sense of urgency can make people more vulnerable and they are more likely to give the information out.

Some IT departments have done tests to prove to management how easy it is to get information from employees. Here is an example of how one support analyst proved to his department heads that their company was vulnerable. In this example, the support person even contacts a member of management to see how they will handle his request for her password and user ID.

> I called Kelly and said, "Hi, this is Peter Livingston from the computer department, have you noticed your computer slowing down recently?"
>
> "Who are you?"
>
> "Oh, I'm Mark's assistant. He asked me to check with everyone regarding the recent slowdown of our filing system. Did you notice anything slowing down?"

"Well, it did seem rather slow the other day."

"OK, hang on, I'm going to log onto your terminal, now your user name is kblake?" I gave the person's name with first initial before the last name.

"No, it's kblakey."

"Ah, thanks. Sorry I'm still new here, OK. Hang on, oh, what's your password?"

"sam89," she replied.

"Thanks, now Kelly, would you please come to the security session meeting you were scheduled for. You just allowed a total stranger access to the system."[1]

There are ways to avoid being a victim of an Information Bandit who is trying to use impersonating. Here are some good tips on how to avoid becoming a victim:

- First, never give your password to anybody. An experienced IT department should be able to fix problems without an end user's password.
- If you feel uncomfortable giving out information that is requested, end the phone call. Ask the person for their name, title, and phone number so you can call them back. Then, research this information and call them back if you can prove they have given you legitimate information.
- Report any unusual call to your IT department. They will log it and continue any research that is needed.

Dumpster Diving

"Dumpster-diving is the practice of searching through a company's trash bins to find any sensitive information that might have been discarded."[2] The Information Bandit can use dumpster diving to gain confidential information. They are looking for user ids, passwords, network diagrams, account numbers, policy numbers, and other confidential information that is thrown in the trash. This can be on a piece of paper, floppy disk, CD, or anything else containing confidential information. The information they find can be just another piece to the puzzle and gets them one step closer to getting the unauthorized access they want.

Information Bandits have used dumpster diving to break into corporate systems. Here is a highly publicized incident of Information Bandits using dumpster diving to break into the systems of some major corporations.

[1] Richardson, pg 1.
[2] Troxel, pg 1.

> In a front-page article in the Wall Street Journal in late 1999, a cracker ring, dubbed the Phonemasters, was alleged to have penetrated systems at AT&T, MCI WorldCom, Sprint, Equifax, TRW, and the databases of Lexis-Nexis and Dun & Bradstreet using mostly Dumpster diving and social engineering techniques. Online coverage of the Phonemasters labeled it the "biggest bust of a cracker ring in the history of network computing." The sheer extent of the penetration of public network infrastructures achieved by the Phonemasters supports this claim quite strongly.[3]

Dumpster diving is an easy way for Information Bandits to get confidential information. There are ways to outwit the dumpster diver. Here are some good tips:

- Do not dispose of confidential information in the garbage. This includes; network diagrams, policy or account holder information, password lists, employee information, hard drives, and floppy disks, CDs or any other confidential item.

- Use locked recycle bins to dispose of confidential papers. These papers should be shredded or destroyed when removed from the recycle bin.

- Empty recycle bins frequently. This way if somebody does break into a locked recycle bin, most of the information will already be destroyed.

- Make sure all storage media is totally wiped clean of information before disposing of them. You should cut up or destroy floppy disk, CDs, or tapes before throwing them away. Hard drives should be cleaned off with a wipe program. The program will write over all data with zeros or random patterns. You cannot completely erase data by deleting it or reformatting the drive.

Tailgating

Tailgating is when an unauthorized person follows an authorized person into a secured building. When the tailgater enters the secured building they are able to get valuable information. They can walk around and get names and phone numbers of employees so they can call the employee and use the impersonating, social engineering skill. They can steal computers, PDAs, storage media, paper or anything else that has confidential information on it. The Information Bandits may be able to get into rooms that hold servers, and other valuable network equipment.

The biggest advantage the tailgaters have is human nature. It is human nature to hold the door when somebody is coming in the door behind you. Some

[3] McClure & Scambray, pg 1.

employees may know better to hold the door for a stranger, but they will make an exception to the rule if they have seen the person in the building before. What they don't realize, is the employee may have been terminated, or quit their job recently and they are not authorized to be in the building anymore. This person may be a disgruntled employee, who is there to cause harm to the computer systems or employees of the company.

Tailgating can be extremely harmful to a company. The best ways to prevent tailgaters from entering buildings can be expensive, but stopping the tailgater may be well worth the money spent. Preventing a tailgater will make it harder for the Information Bandit to steal confidential information. Here are some tips for stopping a tailgater:

- Make sure employees have proper training on how harmful tailgating can be. Put in place strict rules against tailgating.
- Employees should wear ID cards or badges at all times when in the secured building
- Have security guards at all visitor entrances. All visitors should check in with the security guards and should be escorted through the building.
- Have employees enter through card reader/revolving doors. This will prevent tailgating because only one person can enter the door at a time.
- Exterior and interior doors that are usually secured should never be propped open.

Name Dropping

Name dropping is when a person gives the impression that they are associated with someone important. Information Bandits use name dropping to intimidate people so they can get important information from them. Most employees are going to jump at the opportunity to assist somebody important, such as somebody high up in management. Once that important person's name is associated with the request, some employees are not going to question the request. They are more concerned with pleasing this important person.

Let's look at a hypothetical scenario. If the CEO of a company wants a list of all the servers in their company, why shouldn't they get this information? They run the company and should have access to any information they want. More than likely, the CEO will not contact a systems employee directly to gain access to this information. They will have the personal assistant or someone contact the individual. This makes it easy for the name dropper to obtain information if the employee does not double check that the individual is associated with the CEO.

Name dropping is an easy way for Information Bandits to obtain important and confidential information. There are ways to outwit name droppers. Here are some tips:

- Teach employees to stop and think before acting on a request from somebody they don't know. Their judgment should not be clouded by a sense of urgency.

- Make phone calls to verify the requestor's story. If they are name dropping somebody in management, then there should be a secretary or an assistant that you can contact.

- Ask the person for a number at which they can contacted. Contact them once you have verified their story.

Bribing

Bribing is the act of offering money or other incentives to influence that person's views or conduct. Information Bandits use bribing to obtain confidential company or customer information. They can gain access to customer's credit card information, bank account numbers, information regarding the company's systems, and other confidential information using bribing.

If employees are underpaid or if they are not loyal to the company, then they are easy targets for Information Bandits. These employees are more apt to take a bribe in exchange for them giving the Information Bandit confidential information. They may see an opportunity to make fast money and not care about the consequences to them or the company. Many companies are starting to outsource to different countries because it is cheaper. Here is an example of how this turned out to be a big mistake for one company:

> Staffs at call centers in India are being bribed by organized crime and industrial spies to them help hack into the computer systems of British firms.
>
> In at least two recent cases, local IT staff working on the sub-continent for UK institutions were involved in what industry sources say were 'security issues' in what is described as the tiniest fraction of a far larger problem.
>
> In one case, sensitive financial information and credit card details were apparently illegally taken from a leading British financial institution.
> A spokesman for the National Outsourcing Association (NOA) in Britain said: 'This shows that there are some things that you really should not send overseas. For organized criminals, this is a godsend.[4]

[4] Warren, pg 1

Employees should know that taking bribes is unethical and most possibly illegal. Taking bribes in exchange for customer information is illegal. It is common sense that if somebody is bribing you for company information, then it is probably confidential and you should not give it out. Here are some tips to avoid bribing;

- Be sure to do background checks on employees before hiring them. This will help weed out the bad seeds.
- Create a policy against employees receiving gifts from vendors. A more detailed policy against bribery would also be a good idea.
- Make sure employees are fairly paid based on industry standards. If an employee feels that they are getting cheated out of pay then they are more likely to accept bribes.
- New employees should go through an ethics class which should include information regarding bribery.

Eavesdropping

Eavesdropping is listening secretly to the private conversation of others. It can also include viewing information that is intended for others. Information Bandits can intercept email as a form of eavesdropping. They will eavesdrop to get confidential information. It is possible for an Information Bandit to eavesdrop by wiretapping, using radio, using auxiliary ports on terminals, or by simply listening in to a conversation that is being held out in the open. Here is an example of how a small business stole business from its competitor by eavesdropping on a cellular phone;

> Even small businesses may find themselves the target of electronic eavesdropping. A company that serviced machinery discovered they were losing business to a competitor. An investigation revealed that their competitor was intercepting their service dispatch orders (communicated to the maintenance personnel via cellular phone). The competitor would then dispatch their own personnel and beat the original maintenance crew to the scene, thus getting several of the jobs.[5]

Eavesdropping can be very harmful to a company if they do not take the appropriate cautions. The company should train employees on how to avoid eavesdroppers. Here are some tips:

[5] Vanderploeg, pg 1

- Do not hold confidential conversations in public places such as restrooms, restaurants, conferences, and break areas. These types of conversations should be held in a private or secure room.

- Do not send confidential information over email unless it is encrypted. Encryption can help prevent unauthorized access to confidential information.

- Do not discuss confidential information over cellular or cordless phones. The radio signals transmitted and received by these devices can be easily intercepted, compromised, and exploited.

Phishing

> Phishing is a technique used to gain personal information for purposes of identity theft or obtaining confidential information, using fraudulent e-mail messages that appear to come from legitimate businesses. These authentic-looking messages are designed to fool recipients into divulging personal data such as account numbers, and passwords, credit card numbers, and Social Security numbers.[6]

Phishing has been a technique used over the telephone by Information Bandits for years. Recently, they started using spam or pop ups as their main way of phishing. At this time, phishing is mainly used for identity theft. How much longer before Information Bandits use it to obtain user names and passwords for company systems?

Here is an example of a spoofed email regarding a Paypal account;

> Dear PayPal Member,
>
> As part of our continuing commitment to protect your account and to reduce the instance of fraud on our website, we are undertaking a period review of our member accounts.
>
> You are requested to visit our site, login to your account and we will verify the information you have entered.
>
> Click Here
>
> This is required for us to continue to offer you a safe and risk free Environment to send and receive money online and maintain the experience.
> Thank you,

[6] Kay, pg 1

Accounts Management

As outlined in our User Agreement, PayPal will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Thank you for using PayPal

Do not reply to this email.[7]

Phishing is an easy way for Information Bandits to obtain confidential information from an unsuspecting victim. This activity is illegal and every instance of a phishing attempt should be reported. Here are some tips to avoid becoming a victim of phishing:

- Do not respond to any suspicious email requesting account information, asking you to login to a site, or requesting any type of confidential information. Do not click on any links within this email because it may take you to a spoofed site.
- Personally contact a company if they are requesting confidential information from you. Make sure to use a phone number that you know is genuine. You may be able to find this phone number on a previous statement. Do not send this information over email because it may not be secure.
- Look for the "lock" icon on the browser's status bar before submitting confidential information to a website. This means the information will be sent in a secure transmission.
- Forward suspicious emails to uce@ftc.gov.

Stealing

Stealing is to take the property of another without their permission. The Information Bandit will steal to obtain customer or company information or equipment. Once an Information Bandit gets into a corporation they are on the hunt for any type of equipment or confidential information that is out in the open

[7] Piscitello, pg 1

and unsecured. They will also look for unsupervised equipment in public places, such as airports, restaurants, or equipment left unattended in a vehicle. Here is an example of how confidential customer information was stolen because of careless employees;

> A laptop computer containing the names, addresses and Social Security numbers of thousands of Wells Fargo mortgage customers nationwide was stolen in late February when a pair of bank employees traveling in the Midwest stopped at a gas-station convenience store, leaving the keys in the ignition of their unlocked rental car.
>
> As the Wells workers shopped for snacks, a thief made off with the car, a yellow Ford Mustang, around 2 p.m. on Feb. 26, according to police. When the vehicle was recovered five days later, all its contents were gone, including the laptop containing Wells' confidential information. [8]

There has been one law passed that will provide harsher penalties to people who steal trade secrets from a company. In 1996, Congress passed the Economic Espionage Act of 1996 to provide stronger trade secret protection at the federal level. A trade secret is a secret formula, method, or device that gives one an advantage over competitors. This law made it illegal to do the following things:

- To steal or fraudulently obtain trade secrets
- To copy or convey a trade secret without authorization.
- To receive, buy, or possess a trade secret, that was obtained without authorization.
- To conspire to commit any of the acts listed above.

Individuals who violate section 1832 (domestic misappropriation of trade secrets) face penalties of up to ten (10) years in prison and unspecified fines. 18 U.S.C. § 1832(a). (Under federal law, the general maximum fine for felonies is $250,000.) Corporations or other organizations that violate section 1832 may be fined up to $5 million. The penalties for engaging in foreign economic espionage in violation of section 1831(foreign economic espionage) are even greater: the maximum organizational fine is increased to $10 million and the maximum prison term is raised to fifteen (15) years.[9]

Stealing can be an easy and effective way for Information Bandits to gain access confidential company or customer information. Employees should be educated on how to avoid having this information stolen. Here are some ways to protect this information:

[8] Lazarus, pg 1
[9] Schwab, pg 1

- Make sure your laptop is secured with a cable or similar device when left unattended.

- Do not leave your laptop in an unlocked vehicle. Make sure your laptop is kept out of sight in the trunk. If you do not have a trunk, then cover it up so it cannot be seen.

- Be sure to keep an eye of your laptop while going through airport security. Laptops are known to be stolen when they come out of the x-ray machine.

- Use a password protected screen saver when you leave your computer.

- Confidential information stored on a floppy disk, CD, or other storage media should be kept locked up when not in use.

- Confidential printouts should be retrieved from the printer immediately. These documents should be stored in a locked cabinet when not in use.

- Mobile devices should be locked up when not in use. Make sure you keep them closely guarded when taking them with you to a meeting, or any other place.

Shoulder Surfing

Shoulder surfing is when somebody looks over shoulder to obtain information you are working on, or your password. Information Bandits may watch you type your password in so they can access the system using your id and password. This gives them complete access to a system and they are able to obtain confidential information once in the system. They may shoulder surf to read what you are working on. If they are discrete then they can obtain the confidential information on your screen just by looking over your shoulder and reading it.

A more technical Information Bandit may use a camera to record what is on your screen so they can read the details at a later time. Since cameras can be very small and easy to hide, it is easy for an Information Bandit to use this technique without anybody realizing they have a camera. They may also use binoculars to read what is on your screen. This is more common when you are using your computer in public.

Sometimes it is nearly impossible to guarantee nobody is looking over shoulder while you are working. This is especially difficult to do in public places. There are some ways to protect yourself from a shoulder surfer. Here are some tips:

- Do not type in your password if you are suspicious of somebody. If you think somebody has seen your password, change it after they're gone.

- Watch out for people looking over your shoulder or lurking nearby when you are working.

- Be alert when using your laptop or PDA in public places. It can be tough to spot a shoulder surfer in public places but it you are alert, you will have a better chance of avoiding a shoulder surfer.

Reverse Social Engineering

Reverse social engineering is when an Information Bandit creates a reason for a victim to contact them and reveal information. Someone experienced in reverse social engineering may use a three step approach to obtain confidential information.

- **Sabotage-** The Information Bandit will cause damage to a victim's computer. They can do this by sending malicious code in an email to gain access the computer. They may cause an error message to come up when the person starts the computer. This causes the victim to seek help.

- **Advertisement-** The Information Bandit's next step is to ensure the victim contacts them for help. The best way to do this is to place their phone number in the error message.

- **Support-** Finally, the Information Bandit will assist the victim with the problem. During this time, they will gain the information they need without making the person suspicious.

It is not as common for an Information Bandit to use reverse social engineering because it requires a great deal of preparation and research. There are some ways to avoid becoming a victim of reverse engineering. Here are some tips;

- If the Information Bandit cannot cause a problem with the workstation or network then they cannot use reverse social engineering. Make sure you do not open any email attachments if they look suspicious or you do not know the recipient. This will help prevent the sabotage stage from being successful.

- Most companies have an IT department that they contact for all system problems. Always call that number when you have computer problems and not the number in an error message. The IT department will determine if somebody else needs to be contacted regarding your problem. If you do this then you will avoid accidentally contacting an Information Bandit.

- Unless you can verify that you are talking to a person that works for your company then never give them confidential information over the phone.

You should be able to verify their identity using some type of unique identifier that your company uses.

Conclusion

Finding good, real-life examples of social engineering attacks is difficult. Target organizations do not want to admit that they have been victimized. For them to admit a fundamental security breach is not only embarrassing, it may be damaging to the organization's reputation. The real goal of organizations should be to prevent these attacks from happening, not covering them up.

Now that you have learned all the tricks that Information Bandits use to obtain confidential information, you should be able to prevent these types of attacks from happening to you. The key to avoiding an Information Bandit is training your employees on the techniques they use. If your employees are knowledgeable about social engineering and how to prevent it, then the less likely your company's confidential information will fall into the hands of an Information Bandit. It is very important for companies to keep confidential information away from these people. Otherwise, they will evidentially obtain all the pieces of the puzzle using the techniques I have described. Then they will be able to use it for malicious behavior, and possibly cost your company money and customers.

References

1. Richardson, Mark. "The Weakest Link: Social Engineering." URL: http://www.internetviz-newsletters.com/shavlik/e_article000204422.cfm?x=%5B%5BIMN.LID%5D%5D,%5B%5BIMN.USER_ID%5D%5D (27August 2004)

2. Troxel, Roy. "Social Engineering and other Low-Tech Hacking Methods." URL: http://www.edevcafe.com/viewdoc.php?eid=472 (31 August 2004)

3. McClure, Stuart & Scambray, Joel. "Forget the firewall; guard your garbage against 'Dumpster diving' hackers." URL: http://www.infoworld.com/articles/op/xml/00/07/03/000703opswatch.html (1 September 2004)

4. Warren, Peter. "India call centre staff bribed." 9 February 2004. URL: http://www.engology.com/ArchStallBribed.htm (22 October 2004)

5. Vanderploeg, Alan. "Wireless Communications Security" URL: http://www.wirelessgalaxy.com/cellularrelatedarticles/wirelesssecurity_art.html (9 November 2004)

6. Kay, Russell. “Phishing.” http://www.computerworld.com/securitytopics/security/story/0,10801,89096,00.html (9 November 2004)

7. Piscitello, David. “Anatomy of a Phishing Expedition.” 3 September 2004 URL: http://hhi.corecom.com/phishingexpedition.htm (9 November 2004)

8. Lazarus, David. “Car thief whisks off Wells data” 16 April 2004 URL: http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/04/16/BUGH865O141.DTL (10 November 2004)

9. Schwab, Arthur J. “Federal Protection of Trade Secrets: Understanding the Economic Espionage Act of 1996.” URL: http://library.lp.findlaw.com/articles/file/00323/002741/title/Subject/topic/Intellectual%20Property_Trade%20Secrets/filename/intellectualproperty_1_764 (10 November 2004)

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event