Global Information Assurance Certification Paper

Security Awareness: Help the Users Understand

Kenton Smith

October 17, 2001

As security professionals, we spend hours every week trying to "defend our networks from every possible threat. Throughout all of this effort, we forget about the users. The users are the key to a successful security program and what do we do? Frank Hayes, writing for Computer World, "Permissions, virus filters, limited data access, digital certificates, encryption and piles of passwords - they're all pretty much the same to users. They're a pain. They chew up valuable time. They get in the way. So what do most users do when faced with this in-their-face, time-and-effort-consuming security? They look for ways around it. They thumbtack lists of passwords to their cubicle walls. They leave their PCs on when they're away so they won't have to log in again. They turn off filters, turn on scripting and swap unauthorized tricks and shortcuts for bypassing security. We get frustrated and throw our hands up in the air, "I can't believe what these users are doing to my network security!" We forget though, that the users don't read all the stuff we do, they don't get the daily security updates, the virus warnings (not the legitimate ones anyway), the bug fixes. They don't understand why we are implementing all this stuff. So what's a good security professional to do? Help them understand. Notice I said help, not make; it's a crucial difference.

Part of any security policy, should be an accompanying security awareness program. There are many different ways to offer this type of program, including workshops. "Holding a workshop is an excellent way to provide interaction and a personal touch to your awareness program." (http://www.securityawareness.com/workshop.htm) The purpose of this paper is to give you a guideline that you can use to put on a basic security awareness workshop. It can probably be done at a lunch hour, or two, and should be adapted to fit your company's policies and procedures. I've laid it out as if it was a PowerPoint type presentation so that you can easily adapt it to a more interesting visual presentation.

It's imperative that we remember that the purpose of a security awareness program is to make sure that each and every person *understands* that what they do, how they do it, and why they do it, impacts the safety of the company's assets and assets of individuals around the world.

Introduction

"People are the weakest link. You can have the best technology, firewalls, intrusion-detection systems, biometric devices - and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything."
- Kevin Mitnick

There it is in a nutshell; this is why it's important for all users to become "security aware". Kevin Mitnick, by the way, is one of the first people to be convicted and jailed for hacking someone else's computer. It's easy for us to sit at our computers and think to ourselves that everything is safe on our network. We have systems people who have built firewalls to protect our network, we have password-protected access to all of our network resources, we have virus software on our computers. Our corporate information is secure; let's get on with business. It's a pain in the neck sometimes too; we have to change our passwords again, it has to be 10 characters long, my virus software keeps popping-up messages, I have to get a key to get into the server room, etc.
The goal of this information session is to help you realize the role you play in the security of the company's information. There are people out there who will try to trick you on the phone. There are people who will come into your office when you're not there, looking for passwords and other sensitive information. There are hackers trying to get access to your network on a regular basis and, as Kevin Mitnick points out, employees are viewed as the weak link. I hope that by the end presentation of this you will start to see the reason for many of the policies and procedures that are put in place to help protect the company's electronic assets.

Passwords

- Users Possess the Keys to the Data
- Carelessness is Dangerous
- Hackers Have Tools that Will Get Your Password

Passwords are truly the keys to your corporate data. If someone with malicious intent is able to obtain the passwords and get confidential data, it can be the end of your company. Think for a few seconds about what your competitors could do if they knew all of your plans, financial information, employee information, and more. All a hacker needs is one password; with that they usually have all they need to start to break through all the security your systems people have put together. Hackers also have password cracking programs that'll take minutes to crack passwords that aren't properly constructed. If it's worth it, they'll spend hours, even days running passwords through these programs in order to break one.
You may think this is all a little overboard, but it's important that we, as the holders of the keys, learn to take the proper care just as we have with other types of keys. You would probably never think of lending someone your key or pass card to get into your office building. You'd certainly never give someone else your bank PIN number. Passwords need to be thought of in a similar way, a lot is at stake if the password falls into the wrong hands.

Passwords

- Cracking Passwords is Pretty Easy
- Microsoft Passwords are Easier than Others
- No Password is "Un-crackable"
- Remember – It Only Takes One Weak Password

There are many programs available to hackers to enable them to crack passwords. Once they have gained entry to a server there is a lot of information that can be gained quickly to aid the process. For example, once on a Windows machine with very few privileges, a hacker can open the user manager and at least get everyone's names, if not their phone numbers, birth date, and more. With this information a hacker can tune his software to search for variations on that information. Most crack programs will also work with common variations, like substituting the number one where there would normally be the letter "i" (I.e. tr1cky).
Microsoft make this even easier for the hacker because in *some** versions of Windows a password is broken into seven character chunks. This means if your password is "harold22", the software can very quickly crack the last two characters by just going through numbers one after the other. The first seven characters will be easily broken as well because it is a dictionary word, and a smart hacker would have put employee names at the start of her dictionary file.
If given time a hacker could use a "brute-force" attack (every combination of characters) to crack every password in the file. The idea behind building strong passwords is to make it so time-consuming that the passwords will have changed by the time the hacker has cracked the file. Using a very high-end computer that is doing nothing else, a hacker could crack a password that uses a (difficult) combination of letter, numbers, and symbols in about 20 days. Generally by then someone would have noticed that a system has been compromised, and have fixed the vulnerability and any back doors the hacker left behind.
Remember the one bad apple analogy; It only takes one weak password to allow a hacker to gain *authorized* entry to your network.

*This can be "fixed" by your network security personnel in some situations

Passwords

- How to Make it Stronger:
  - Make it moderately long
  - Use a seemingly random combination of letters (both upper and lower case), numbers, and symbols
  - Don't use your username or full name

It is unreasonable to expect any of us to remember a 20-character password that is just a hodge-podge of characters. You would just end up having to write it down and negate the strength of the password. You also might try to avoid having to enter it all the time. Therefore use a moderately long password that you know you'll be able to keep in your head.

Use a seemingly random combination - to outsiders it may look like random characters, but you know the secret code. Most people, when they were kids experimented with codes to talk to their friends. Most of them would be very easy to decode too. However you can use that idea in constructing your password. One suggestion is to make-up a phrase, and then use the first letter and some numbers to make a password. An example might be: Iug4l@12:05! At first glance it looks impossible to remember, however here's the decoded version: I usually go for lunch at 12:05! After you've typed it a couple of times you'll have no problem entering your password. Is it stating the obvious to say don't use your username or full name? I hope so, but many people do or use variations that would take less than 5 minutes for a crack program to resolve.

Passwords

- How to Make it Weak Again
  - –Write it on a sticky note
  - –Tell it to someone
  - –Write it on a piece of paper and then throw it in the garbage or recycling
  - –Use the same one all the time

These are just some of the ways that you can negate all the work you put in constructing a strong password. How many of you would write your bank PIN number on a piece of paper and then put it in your wallet with your bank card? Hopefully no one! This is equivalent to writing your password on a sticky note and sticking it to your monitor.
If you received a phone call from someone who said they were from a software vendor doing work on your servers. Would you give them your password if they asked? You know, they just need it to do a test. Hopefully your company has a policy about what to do in this situation, but you should have a personal policy for passwords just like you would for any other personal information (like your PIN or SIN/social security number).
How many of you have written your password on a piece of paper and then thrown it away once you remembered it? Did you know that there are people who will go through your garbage (or pay someone else to do it) just to find information like this? If your company has a shredding program make sure you use it; if not, never write down your passwords.
Many companies have a policy that prevents you from using your last x-number of passwords. This helps in thwarting a brute force attack because it might be a year before you use a password again. If your company doesn't force you to do this, you should do it anyway. Also, don't use the same password for everything. Most of you have probably registered at a web site and then saved your password in your browser so you don't have to keep entering it. If you use the same password for this that you would to access your corporate network, all the information a hacker needs is on your computer.

Viruses & Hoaxes

- Malicious Code
  - – Viruses, Worms, Trojans, etc.

- What Can You Do?
- Hoaxes – Can You Spot One?

There are all sorts of malicious programs "in the wild" that could infect your computer in many different ways. Mostly we hear about the program viruses and the macro viruses, although more and more we're hearing about worms too (Code Red, Nimda, etc.). There are many other viruses and trojans that we don't hear about. We will talk mostly of the viruses you'll encounter from day to day and what you can do to help stop the spread. If you have a high-speed connection at home, you'll want to educate yourself a little more on the worms and trojans, as you'll have more cause for concern when your computer is really on the front-line.
You might think that since you have virus software on your computer and that you're behind a firewall that your network administrator has taken great pains to secure, you're safe. You are relatively safe, particularly from worms and trojans, but there are many viruses that can get through all that and you can help to protect yourself if you have a little knowledge of how they work. Your company may also have policies about opening file attachments, which will help in the prevention as well.
What about hoaxes? Are they really that bad? How many of you have received a chain e-mail or virus warning that had been sent to you via 100 other people? These may not cause harm to your computer but they account for a lot of unnecessary Internet traffic, not to mention time spent replying to and reading the e-mail. E-mail servers get clogged up, bandwidth gets used, and system administrators lose time trying to sort out the good from the bad. With a little knowledge you can learn to spot hoaxes and stop them before they get out of control.

Viruses & Hoaxes

- Virus
- Worm
- Trojan

A virus is a piece of code that is written specifically to execute itself without the users knowledge or permission. It will usually attach itself to a file in order to replicate and spread itself. Some viruses are harmless while others can cause serious damage. You should never leave a virus on a system even if it appears harmless. The types of viruses with which we will concern ourselves are program viruses and macro viruses. Program viruses are usually EXE or COM files and must be executed to activate and begin to spread. The first signs of this kind of virus might be files being saved with strange names. Many of these viruses will have some sort of delay so that it is not immediately obvious that you have triggered it, or what file is infected. Macro viruses are the ones that we hear about a lot these days. With the proliferation of the "macro language" Visual Basic, these have become increasingly common not to mention dangerous. Familiar examples of a macro virus are the "Love Letter" and "Melissa" viruses. Only the language being used and the skill of the virus author limit the capabilities of macro viruses.
Malicious code that requires no specific action on the part of the user is called a worm. Worms are self-contained programs (or sets of programs), that are able to spread functional copies of themselves to other computers (usually via a network). These programs can originate and infect

from a single machine or infect a machine and then propagate to others while removing itself as it moves along. Recently, Internet servers around the world have been battling the CodeRed/Nimda worms that take advantage of various documented vulnerabilities in Microsoft IIS.
It is possible for a computer to be infected by malicious code that appears to be a harmless program; this is called a trojan. Trojans are very often used by hackers as back doors into a computer. By planting a trojan, a hacker can gain control of your computer through applications that look legitimate but are actually malicious. These programs might open a "hole" through which a hacker could then access your computer, or just monitor what is going on. The most well known trojan is the Back Orifice trojan.

Viruses & Hoaxes

- Things You Can Do to Stop Viruses
  - Run Anti-virus Software
  - Make sure it's up-to-date and configured properly
  - Don't open e-mail attachments
  - Watch file extensions carefully

So, how can you help to reduce the possibility of getting a virus? There are a number of things, although you may be limited by your systems department so check with them before making any changes that may not be authorized.
Run anti-virus software may seem like an obvious suggestion, however many companies don't run it. If you have Internet access at home you should also be running it at home. Some companies make their anti-virus software free to home users.
Make sure it's up to date and configured properly. The company I work for had a problem with a "love-letter" type worm and one of the reasons that it spread was that the default installation of our anti-virus software didn't scan VBS files (the file extension of an infected file). Make sure that you have your anti-virus software set to scan all file types. Computers today are powerful enough that this doesn't put a strain on your system resources (unless it's a heavily used file server). If your system is "old and slow", make sure you have selected the most common file types to be scanned. These should at least include: EXE, COM, VBS, DLL, TXT, MP3, JPG, and TIF. You should also make sure that it is actively scanning files rather than just doing scans every night or every week. Make sure that your DAT files are being updated regularly. Most anti-virus software has an automatic update function; make sure you use it. You should schedule it to run weekly, if not nightly for the most up-to-date files. Scheduling a general system scan weekly is another good idea. Remember, there are viruses that you can launch but don't see immediate signs that they have been activated. Many viruses work across networks, scanning weekly can pickup files that may have been infected by a virus on someone else's computer.
In the wake of the Love-letter and Melissa viruses, many companies have made policies regarding e-mail attachments. If your company has a policy, make sure you abide by it. Some companies even remove attachments at the mail server. If you never open an attachment, you are almost guaranteed to avoid e-mail borne viruses. I say almost, because there are new viruses now that don't require you to actually open the file yourself, thankfully these are pretty rare at this time. If you sometimes must send and receive e-mail attachments (many people do), then make sure you

take some basic precautions. Don't automatically open every attachment. Make sure that the text of an e-mail makes sense in the context of a file for which you might be waiting. If someone is sending you a text document, don't open an attachment that has a JPG extension. Making sure that the text of the e-mail is personalized is a good rule too. If the text looks very generic, it could very well be a virus. On the other hand if it has text that is typical of the sender (I.e. it ends with "Cheers, John") then chances are it's authentic (assuming the sender is actually John). When in doubt, delete the e-mail. You can also check with the sender to find out if they may have knowingly sent you something.

Virus writers are tricky and they are very good at using the operating system to their advantage when creating a virus. A good example of this is the number of viruses that take advantage of the address book in Microsoft products. Something else they've taken advantage of is multiple file extensions. Default installations of most Microsoft operating systems hide known file extensions. (Known file extensions are those extensions to which an application has been associated. For example, when you double-click on a text file it will usually open in WordPad or Notepad. This is because the operating system has associated the TXT extension with one of these applications.) Stick with me; my point is coming. If you look at a detailed file listing in Windows Explorer, most people will see the file names but no extension for files that have associated applications. VBS files are associated with the visual basic scripting language and therefore you won't see the VBS extension. Now a virus writer comes along and sends you an infected file called love-letter-for-you.TXT.vbs; if your operating system is in it's default setting, you will see (in Explorer and Outlook or Outlook Express) love-letter-for-you.TXT, and that looks harmless enough, doesn't it? Tahdah, I'm at the point-making part now. You can never trust the file just by the extension you see. You should also go to your Windows Explorer settings and turn off the "Hide file extensions for know file types" option. You can do this by opening a Windows Explorer window, click on *tools* then *folder options*, click on the *view* tab and uncheck this option.

Viruses & Hoaxes

- What's Wrong With the Odd Hoax Virus Warning?
- How to Spot a Hoax from a Mile Away

The problem with hoaxes and chain e-mail is that you aren't the only person getting and forwarding that particular note. If you've ever looked at the header of one of these e-mails, you have probably noticed that there were 10's or 100's of people who received it before you. Think of the old "and they told two friends, and so on" ad from a number of years ago. If the person who sent it to you sends it to 10 people and each of those people send it to only 10 more, that's already 100 people who have received it. If this all happened in the same company, think of the effect on the mail server and the network. The other problem with it is that there are some hoaxes (like sulfnbk.exe hoax) that tell you to delete an actual Windows file from your computer. To make matters worse, a virus then started to circulate (W32.Magistr.24876@mm) that actually had an attachment called sulfnbk.exe that was infected with a virus. You can see how these harmless pranks can get serious. Even without the virus coming out, many people deleted a perfectly

healthy file from their computers and then had to find out how to get it back.
So you want to know how to tell if something's a hoax, but you don't want to ignore a valid warning. First of all; if you have a System Administrator, you should just forward the e-mail to him and let him research it. However, if you get it at home (or don't have a systems person) here are some clues below that are common to almost every virus hoax around.

Clues to Spotting a Virus Hoax:
Clue 1 - It's a warning message about a virus (or occasionally a Trojan) spreading on the Internet. (Some even describe a "Trojan horse virus." There is no such thing.)
Clue 2 - It's usually from an individual, occasionally from a company, but never from the cited source.
Clue 3 - It warns you not to read or download the supposed virus, and preaches salvation by deletion.
Clue 4 - It describes the virus as having horrific destructive powers and often the ability to send itself by e-mail.
Clue 5 - It usually has lots of words in all caps and loads of exclamation marks.
Clue 6 - It urges you to alert everyone you know, and usually tells you this more than once.
Clue 7 - It seeks credibility by citing some authoritative source as issuing the warning. Usually the source says the virus is "bad" or has them "worried."
Clue 8 - It seeks credibility by describing the virus in specious technical jargon.

Okay, so you get a message that seems to match these clues, but you're still not sure. There are two ways to find out for sure: 1) Go to the site of the company that supposedly released the information. If there isn't anything there that's relatively conspicuous, you can be sure it isn't a dangerous virus (don't you think they'd have a big headline?). 2) Go to a trusted anti-virus or hoax debunking site, examples would be Symantec, McAfee, or Vmyths. At any of these sites you can do a simple search on the name of the "virus" and there will almost always be information relating to it. Here's a sample of a hoax that made the rounds recently:

> Subject: Fw: VIRUS ALERT DO NOT OPEN "NEW PICTURES OF FAMILY" It is a virus that will erase your whole "C" drive. It will come to you in the form of an E-Mail from a familiar person. I repeat a friend sent it to me, but called & warned me before I opened it. He was not so lucky and now he cant even start his computer! Forward this to everyone in your address book. I would rather receive this 25 times than not at all. Also: Intel announced that a new and very destructive virus was discovered recently. If you receive an email called "FAMILY PICTURES," do not open it. Delete it right away! This virus removes all dynamic link libraries (.dll files) from your computer. Your computer will not> be able to boot

This one covered just about all of the clues, plus all you have to do is go Intel; if they don't have

it on their site you can be sure it isn't real (and Intel doesn't generally release virus warnings). The example is courtesy Stiller Research.

Social Engineering

- What is Social Engineering?
- Can Someone Actually Get Useful Information This Way?
- What Can You Do To Thwart This Type of "Attack"?

Robert Graham in his document "Hacking Lexicon" defines social engineering as: "Social engineering is a form of hacking that targets people's minds rather than their computers." Here's the scoop folks; for the most part we are the weak link. This isn't meant as an insult, it's just human nature. We all want to help decent hard-working folks just like ourselves and we generally assume that most people around us are honest. We also don't want to get in trouble from our superiors, and value the fact that we have a job. Unfortunately there are people out there who can take advantage of these common human traits and use them to their advantage. Many times, this type of information-gathering is used a precursor to a hacking attempt. Some times it is used to get into an office and steal equipment or information from the physical premises rather than from computers. The important thing to remember is to set up some personal guidelines to help you avoid this type of situation.

Social Engineering

- It Comes in Many Forms
- What Information Can Be Gained?
  - Network Information – Server Types, Network Protocols, Internet Access
  - Company Information – Name, Address, Internet Domain
  - Personal Information – Passwords, Name/User name

I'm going to give some examples of the different ways in which social engineering can be employed, then we'll see how much information was gained.
The telephone is a very common way of getting information:
"Hi, my name if John Doe from Xyletronicalipso Printers International. How are you today?"
Amy takes in the information she just heard in her phone receiver and responds with the typical, "I'm fine thanks. How may I help you?"
The phone says to Amy, "First of all, let me clearly state that this is not a telemarketing call. I am not going to try to sell you something. And this is not a phony sweepstakes gimmick. This is for real."
"Amy," continues the pleasant voice on the phone, "your company has been chosen to receive five of our latest model XJ573 1200 dpi laser printers. You will be receiving these printers free of charge. How does that sound?"
"Well it sounds great." Amy mouths into the phone, "but how did you get my number?"
"Do you remember, about three months ago, you filled out an entry card? Well, no matter. You've won. I just need to get some quick information to send you the printers. Is now a good

time?"
"Yes. Now is fine I have a few minutes."
The phone continues to speak and Amy continues to listen. After asking for the address and the person to attention the printers to, the phone asks for an e-mail address for contact purposes. Then the phone begins to explain how that these printers are network capable and that they should really come preconfigured for easiest installation.
"So. What network operating system are you using?" asks the now-best-friend-of-Amy phone.
Amy quickly replies, as she is in the quick reply mode, "Oh we're using Windows 2000 servers and mostly Windows 98 clients?"
The phone replies, "I assume, then, that you're using the TCP/IP protocol. To make it as easy as possible for you, I need you to give me five IP addresses that are available on your network so the printers can be ready right out of the box."
Amy tells the phone the IP addresses and the conversation continues for some time...

Another example is of an impersonator coming into your office. How many time have you walked by your photocopier or fax machine and seen someone with a laptop computer working away? This person is probably dressed in official clothes or a nice suit and tie. How did he get there? Is this your concern? You assume the receptionist let him in so it must be legitimate right?

Or how about this last example? You're browsing the Internet and a pop-up comes on the screen saying the connection has timed-out, please re-enter your username and password.

By the end of the first example you've probably gotten the idea. This person on the phone has just acquired all sorts of valuable information. He got an e-mail address that usually contains a user name on the mail server or network plus the domain name for the company's network. He then goes on to find out the operating systems of the workstations and servers, the network protocol being used, and some internal IP addresses that aren't being used. "Amy" was just trying to be helpful, after all it was going to be a great thing for the company, and her boss would be pretty happy too.

Example number two is a little less clear-cut. This isn't to suggest that you shouldn't let anyone else into your office. We all need to be vigilant though, because people can get past the receptionist (legitimately) and if they are by themselves, have free run of the office. Is there a network outlet near your copier or fax machine? If it's "live" the service person could easily connect to your network with their laptop; this is an issue for your systems people. You might want to stop by the office of the person responsible for that particular piece of equipment and mention to them that someone is working on the copier; do they know? There were many times when I was doing this type of customer support that I could be let in just because I knew where I was going. The person responsible may not even have known I was there. Whatever you do (or don't do), it's important to be vigilant about what's going on around you. Service people have excellent access to sensitive material and if an imposter was to get in, you could lose valuable information without even knowing it.

Example number three should at least make you stop and think. What password do I need to enter? Could this happen? The important thing is that you just don't go and re-enter passwords and usernames without stopping to ask why. Talk to your network people and find out if this is true, or just cancel the window and see if you can continue to surf. This type of intrusion is not theory, it could certainly happen.

Social Engineering

- Some Things You Can Do
  - Never give information about your network over the phone
  - Never give information about your network via e-mail
  - Always say you'll call people back when they start to ask "private" questions
  - Don't give work information out during your "at home" hours
  - And finally, never, never tell anyone your password under any circumstances

All right, you say, what can I do to prevent this sort of evil from hurting our company? First of all, it's important to use common sense and you should always be vigilant when conversing with a stranger. I just had a call while I was writing this (honest, I'm not just saying that), it was from a company telling me that I had been pre-approved for their MasterCard; all they needed was a little information in order to process the application. I stopped the conversation at this point because I didn't want the card, however it made me think about what information I might have been asked for, and what I would have said. Don't worry; I'm not going to tell you what to do at home too. However, as our world completes more business transactions over the phone, fax, and e-mail, we lose the ability to authenticate the person on the other end of the transaction. The tips above and the sample conversation are provided by Tom Carpenter the founder of SysEdCo (www.sysedco.com). They're pretty self-explanatory and really common sense, however it's easy to forget these things when you're in the middle of a conversation. Familiarizing yourself with these tips will help you when you're in the middle of a conversation and the questions start to become more probing.
I hope that the last tip is one that you'll already have thought of from the previous discussion on passwords.

Conclusion

Hopefully you have a better understanding about what you can do to increase the security of your company's information. It isn't just the job of your IT people; you have a lot of control over what happens at your desk. It's important to be vigilant, and interested in what is happening around your office and on your computer.

Sources Cited/Referenced

ComputerWorld Magazine
http://www.computerworld.com/cwi/stories/0,1199,NAV47_STO62041,00.html

Security Awareness
http://www.securityawareness.com/workshop.htm

Symantec
http://securityresponse.symantec.com/avcenter/venc/data/sulfnbk.exe.warning.html

Stiller Research
http://www.stiller.com/stiller.htm

Robert Graham Hacking Lexicon
http://www.robertgraham.com/pubs/hacking-dict.html

SysEdCo
http://www.sysedco.com/library/security/socialengineering_social_engineering.htm