SANS Security Essentials
GSEC Practical Assignment, Version 1.2e

Security Education for Users: A Starting Place for Network Administrators

Blou Baker

July 23, 2001

Table of Contents

Security Education for Users – The Who

Instructor

Who will teach the class? A Network Administrator, the Security Administrator, or a consultant? The size and culture of your company will help determine this. Often the Network Administrator or Security Administrator is chosen because they are the ones with the knowledge. However, they also tend to be more analytical in nature and not the best choice for teaching others. If this is whom you have chosen to be your Security Instructor make sure they have the extra time to learn about effective verbal and written communication.

Students

Management should be the first class. This shows the other employees that Management supports the policies behind what you are teaching. Encourage management to let their employees see them being security-conscious in their day-to-day business.

Use your available resources to determine the size of the classes. The size of the room available to teach in, the acoustics of the room and equipment available will all affect the size.

Security Education for Users – The Why

Security issues affect everyone. It is not just an I.T. issue. It is not even just a management issue. If you have a user ID and password then security is an issue that concerns you. Here is an example:

> You have just changed your password so you write it on a post-it note and stick it under your keyboard. Your neighbor just happens to be walking back to their desk and sees your new password as you write it down. Not a big deal. After all, your neighbor is a trustworthy employee. A week from now that employee does not get the schedule that they wanted, they are not very interested in the job anyway and decide to quit. They stay through the day to collect their check and will have some fun with your user ID and password while they wait. Customers will be receiving shipments of items they did not order. People inside and outside the company are receiving crass email from you. In addition, that spreadsheet you spent two hours on this morning? Gone. You will be the one to answer your manager's questions. You will be the one to have the I.T. Department restore your spreadsheet from last night's backup. You will be the one to re-do your work on that spreadsheet.

Security does affect you. It is not limited to your place of employment either.

Security Education for Users – The What

Passwords

Passwords are the only thing keeping your computer access secure. The other piece of information that you use is your user ID. If an attacker knows your name, they know your user ID.

With a possible attacker knowing half of the combination (your user ID) you want to make the other half (your password) difficult to guess or crack. On the other hand, the password needs to be easy enough for you to remember. Most users choose passwords that are too easy to guess (McAuliffe, p.1). A good middle ground is to use the phrase acronym. Think of a phrase and use the first letter of each word.

Include a special character and make a couple of the letters uppercase and you have a password you will remember. You will not need to write it down, nor will it be easily guessed or cracked.

It used to be that putting a number or two on the end of a password increased its complexity substantially but that is no longer the case. The password cracking programs now take that tendency into effect. Adding a special character (from the SHIFT of the number keys on the letter side of the keyboard) and including both upper case and lower case gives your password a fair degree of complexity. It can still be cracked but it would take a while.

Password Protocol: Never watch someone else type his or her password. Make it obvious that you are turning your head so the person typing the password knows you are not watching.

Does anyone have any questions? Does anyone have any feedback?

(Note to teacher: If the feedback session starts taking too long suggest that thread continue after class privately or on a bulletin board. Make a point to make a note of it so the students do not feel put off.)

Social Engineering

How many here know what Social Engineering is?

Definition from the Hacker's Jargon Dictionary, version 4.3.1 (Raymond):
"[…] The aim is to trick people into revealing passwords or other information that compromises a target system's security."

From Bernz's Social Engineering Intro on Packetstormsecurity.org (Bernz);
"According to The Fugitive Game, Kevin Mitnick, one of the most renowned hackers, did most of his work through social engineering. Only the last 15% or so was on the computer. The rest was scamming phone agents for codes. It works."

Safety Rule #1) Do not give your password to anyone.
Safety Rule #2) Do not give out any company information to anyone you do not know should have it. Do not take the caller's word for anything.

Another social engineering trick is to pop up a window on your computer screen that says, "Your connection has timed out. Please log back in." The window will have a place for your user ID and password. The window is a fake. It is just a way for someone to try to collect your user ID and password for their own use.

Does anyone have any questions? Does anyone have any feedback?

Virus Software And Procedure

There are thousands of different viruses, worms, and Trojans. Virus software will help keep your PC clean. There are two parts to virus software: the virus engine and the virus definition file. The virus definition file contains signatures of the known viruses. The virus engine uses that file to find viruses on your computer. We update the definition file weekly. This will happen automatically right after you log on every Thursday morning.

If you suspect a file of having a virus email it to the I.T. Department for evaluation before you open it. Call the Help Desk immediately if you ever receive a message that states you have a virus.

Has anyone here ever received a message that warns of some new virus and tells you to tell all your friends? If you have not received one in the past, I can guarantee you will receive one in the future. They fly around the Internet like annoying mosquitoes. Any true virus alert will not tell you to forward it to all your friends. All that does is clog the mail server. These emails are hoaxes and you should delete it. If you suspect that it might be a true virus alert, check it out first. Go to your favorite virus information site or one of the following sites:

http://www.hoaxkill.com/ (Hoaxkill)
http://www.symantec.com/avcenter/hoax.html (Hoaxes)

If you do not have web access forward it to your I.T. Department and we will check it out for you.

Does anyone have any questions? Does anyone have any feedback?

Email

Here we have some important points to keep in mind when using email:

- Never open an attachment from someone you do not know and trust. Do not open attachments from someone you know and like. Only open attachments from someone you know keeps their computer virus-free. Forward to the I.T. Department any attachments that you want to open but are not sure about the source.
- Email is not private. Only communicate in email what you would be comfortable communicating to a crowd of people. Use encryption to secure messages that need to be private. We will cover encryption in the next section.
- During an "econversation", an email message can become long and cluttered with quoted replies. Trim the quoted replies to keep only the relevant material. An exception to this would be when communicating with another company's Customer Service Department, for example. Keep all quoted replies in these messages so that the representative reading your email can easily see the history.

- The computer you work on and the email account you use are company property. Represent yourself and the company in a professional manner through email.

Does anyone have any questions? Does anyone have any feedback?

Encryption

"Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood" (Whatis).

This definition from the I4K Internet Dictionary (Kells) is easier to understand:

"Encrypt is a fancy word that means, "to put something in to secret code". On the Internet, you put things like e-mail and important files in to a secret code so that others will not be able to find a copy and read it. In order to encrypt messages you need two keys; a public key to put the message in to code and a private key to get the message out of code."

(Note to Instructor: If you want to get technical you can teach them about the four requirements of a cryptosystem; confidentiality, integrity, authentication, and non-repudiation. It depends on your students.)

PGP is an encryption program. You can use it to encrypt or sign your email. You can also use it to encrypt files. Here we have already installed PGP for you. If you want to get it for your home computer go to the MIT Distribution Center for PGP (MIT).

The first step is to generate your public/private key pair. This is an asymmetric key. The public key is for encrypting messages or files. The private key is for decrypting messages or files. To send an encrypted message to someone you need his or her public key. You encrypt the message with their public key. They decrypt the message with their private key. It works the same way for them to send you an encrypted message. They encrypt it using your public key and you decrypt it using your private key. In order to communicate with someone using encryption you must exchange public keys. Do this via email or certificate server. Either way, you must have the individual's key on your key ring to send them a message.

PGP can be very involved. You can get more instruction from the PGPi FAQ (Ytteborg).

Does anyone have any questions? Does anyone have any feedback?

Internet

Guard your personal information carefully while out on the Internet. There are frauds out there designed to get information from you. Contests are one way of gathering information about you. To enter a contest you are asked for your name, address, etc. The more contests you enter, the more Spam you will receive. Never give your Social Security Number out.

Does anyone have any questions? Does anyone have any feedback?

Neighborhood Watch Program – "Network Neighborhood Watch"

Everyone knows what a Neighborhood Watch program is. Here at work we do the same thing. Question the presence of anyone you see inside the building that you do not recognize. If they are not with a fellow employee and do not have a badge ask them if you can help them. Ask them who they are and what they need. Validate their answer. Do not let someone just walk in and help him or herself to company property, whether it is reports, a computer workstation or a phone.

This also extends to your fellow employee. Do you have access to privileged information? Make sure it stays private and away from roaming eyes. The reverse applies also. Keep your eyes off your neighbor's privileged reports or displays on their computer monitor.

Does anyone have any questions? Does anyone have any feedback?

Remote Access (Only for employees who use remote access.)

VPN and RAS. Our company allows remote access by VPN or RAS. They work differently but they achieve the same end – secure communication with our network. You can check your corporate email, get a document or spreadsheet from the file server, or process orders on the AS/400.

- VPN is an acronym that means Virtual Private Network. VPN creates an encrypted tunnel between your laptop/PC on the Internet to the corporate firewall. This keeps all the data secure from prying eyes on the Internet. To use VPN your first step is to log on to the Internet. Then open the VPN connection that the I.T. Department configured for you. Proceed with your work as usual.
- RAS stands for Remote Access Service. You do not use the Internet when accessing the RAS server. There is a modem and phone line on the RAS server. To use RAS open the RAS connection that the I.T. Department configured for you. Proceed with your work as usual.
- Many people check the "Save Password" box so that they do not have to type the password each time they log on. Do not do this. Laptop theft is common. Checking that box gives the thief not only the laptop but also access to the company computer systems. Even if they do not do any damage to the company computer system, they can use it to hack other companies and make it look like

one of our employees did it.

Personal Firewalls

A lot of us are lucky enough to have broadband access to the Internet. Broadband access is cable modem or DSL. Your access speed is much greater and you do not have to dial up to log on. If you have "always on" access to the Internet and you want to remotely access the corporate server you must have a firewall installed and configured correctly. It is too easy for a potential hacker to hack your PC and get your user ID and password to the corporate network. It is much easier for an attacker to get to your PC than it is for the attacker to try to break through the corporate firewall.

There are in general two different kinds of firewalls. We will look at each.

Packet-filtering Firewalls. These firewalls examine the headers of the IP traffic to determine whether they will be allowed in or out. These firewalls are fast but can be less secure than application-level firewalls.

- Network ICE -- BlackICE Defender (BlackICE)
- C&C Solutions -- ConSeal PC Firewall (ConSeal)
- Network Associates – PGPFire (PGPFire)

Application-level Firewalls. These firewalls deal directly with the programs that communicate with the Internet. They are usually easier to configure, especially for a novice.

- Zone Labs – ZoneAlarm (ZoneAlarm)
- McAfee – McAfee Firewall (McAfee)
- Symantec – Norton Personal Firewall (Norton)
- Zone Labs – ZoneAlarm Pro (ZoneAlarm Pro)
- Tiny Software – Tiny Personal Firewall (Tiny)

I have used BlackIce Defender for the last couple of years and have been very happy with it. The other firewalls listed here also have faithful followings. Do a search on the web for "personal firewalls" to research which firewall is right for you. Here are a few URLs to get you started:
Personal Firewalls: What Are They, How Do They Work? (Zych)
Shields Up: Internet Connection Security for Windows Users. (Gibson)
Personal Firewalls / Intrusion Detection Systems: An Analysis (Boran)

Other Home PC Security Issues

- Who uses the PC? If you have sensitive company data on the PC, you should encrypt it to keep it private.
- Are you running virus software on the home PC? Do you keep the virus definitions updated?

- Do you backup your data? The backups need to be stored in a secure location if they contain company information.

Does anyone have any questions? Does anyone have any feedback? .

Security Education for Users – The How

This section is for the Instructor. It includes different resources that are available and tips for teaching. Keep in mind that this resource is a guide only. You can add to the material and customize as needed. If you use all the sections in this paper you will probably want to design two classes instead of trying to put it all into one.

- Be organized and prepared.
- Put a visual of the Table of Contents up so the students can see where the class is currently and where it is going.
- Begin and end the class on time.
- Vary the pitch and volume of your voice. See this online newsletter, Improving Verbal Skills (Taylor), for help
- Keep eye contact with the students.
- More tips are located at the following sites.
  - A Berkeley Compendium of Suggestions for Teaching With Excellence (Davis)
  - A Brief Summary of the Best Practices in College Teaching (Drummond).

- Different people learn in different ways. Use as much interesting visual content as possible.
  - Flip charts
  - PowerPoint presentations – get help here, Microsoft PowerPoint Tips and Tutorials (Bear).
  - White boards
  - Handouts
- Use analogies and stories. Stay away from telling jokes unless you are proficient at it. Make the class fun and interesting as possible.
- Be a motivating individual. Lessons in Lifemanship: Chapter 26 (Bell) is a good resource for learning how to motivate others.

- Create a “Suggestion eBox”. One way is to set up an email address, suggestions@yourdomain.com. Have users send suggestions to that address. Another way is to use a bulletin board application. Very Important: Read and reply to the suggestions.

- Keep classes short and repeat often.

- Write a weekly I.T. newsletter. Get help here, 101 Newsletter Answers (Alexander)

- Email a tip-of-the-day.
- Set up a bulletin board application that allows users to ask questions about viruses, passwords, etc. Monitor and respond to any questions.
- Use logon banners to remind users of company policy.
- Have your Creative Services Department make some posters to put around the offices reminding employees of computer security tips.

- I.T. Encyclopedias
  - Webopedia.com (Webopedia)
  - TechEncyclopedia (Tech)
  - Whatis.com (Whatis.Techtarget)
  - Kids' Internet Dictionary (Kells) – for definitions using very simple words.

List of References

Alexander, Mike, and Jan. "101 Newsletter Answers: Using Newsletters to Communicate Effectively." July 2, 2001.
URL: http://www.101newsletteranswers.com/ (July 23, 2001).

Bear, Jacci Howard. "Microsoft PowerPoint Tips and Tutorials." Desktop Publishing, About.com.
URL:
http://desktoppub.about.com/cs/powerpoint/index.htm?iam=dpile&terms=%2BPowerpoint+%2Btutorial

Bell, Brian. "Lessons in Lifemanship: Chapter 26."
URL: http://bbll.com/ch26.html (July 23, 2001).

Bernz. "Bernz's Social Engineering Intro and Stuff."
URL: http://packetstormsecurity.org/docs/social-engineering/socintro.html (July 23, 2001).

"BlackICE Defender." Network ICE / Internet Security Systems.
URL: http://www.networkice.com/products/blackice_defender.html (July 23, 2001).

Boran, Sean. "Personal Firewalls / Intrusion Detection Systems: An Analysis of Mini-firewalls for Windows Users." June 14, 2001.
URL: http://www.securityportal.com/articles/pf_main20001023.html (July 23, 2001).

"ConSeal PC Firewall." C&C Solutions.
URL: http://www.consealfirewall.com/ (July 23, 2001).

Davis, Barbara Gross, Lynn Wood, and Robert C. Wilson. "A Berkeley Compendium of Suggestions for Teaching with Excellence."

URL: http://uga.berkeley.edu/sled/compendium/ (July 23, 2001).

Drummond, Tom. “A Brief Summary of the Best Practices in College Teaching.”
URL: http://nsccux.sccd.ctc.edu/~eceprog/bstprac.html - lecture (July 23, 2001).

Gibson, Steve. “Shields Up: Internet Connection Security for Windows Users.”
URL: http://grc.com/su-firewalls.htm (July 23, 2001).

“Hoaxes.” Symantec.com.
URL: http://www.symantec.com/avcenter/hoax.html (July 23, 2001).

“Hoaxkill.com”.
URL: http://www.hoaxkill.com (July 23, 2001).

Kells, Tina. “Kids’ Internet Dictionary.” Internet for Kids, About.com.
URL: http://kidsinternet.about.com/library/dictionary/words/blencrypt.htm (July 23, 2001).

Kells, Tina. “Kids’ Internet Dictionary.” Internet for Kids, About.com.
URL: http://kidsinternet.about.com/library/dictionary/bldictionarymain.htm (July 23, 2001).

“McAfee Firewall.” McAfee.com
URL: http://www.mcafee-at-home.com/products/firewall/default.asp (July 23, 2001).

McAuliffe, Wendy. “Computer Passwords Reveal Workers Secrets.” ZDNet News. June 29, 2001.
URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2781327,00.html

“MIT Distribution Center for PGP.” Massachusetts Institute of Technology.
URL: http://web.mit.edu/network/pgp.html (July 23, 2001).

“Norton Personal Firewall 2001. Symantec.
URL: http://www.symantec.com/sabu/nis/npf/ (July 23, 2001).

“PGPFire.” Network Associates.
URL: http://www.pgp.com/products/pgpfire/default.asp (July 23, 2001).

Raymond, Eric S. “Jargon File.” Version 4.3.0, April 2001.
URL: http://tuxedo.org/~esr/jargon/index.html (July 23, 2001).

Taylor, Barbara. “Improving Verbal Skills.” The Institute for Management Excellence. February 23, 2001.
URL: http://www.itstime.com/aug97.htm (July 23, 2001).

“TechEncyclopedia.” Techweb.com.

URL: http://www.techweb.com/encyclopedia/ (July 23, 2001).

"Tiny Personal Firewall." Tiny Software
URL: http://www.tinysoftware.com/pwall.php (July 23, 2001).

"Webopedia Online Dictionary." Webopedia.com
URL: http://www.webopaedia.com/ (July 23, 2001).

"Whatis.com". TechTarget.com. December 26, 2000.
URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html (July 23, 2001).

"Whatis.com IT-specific Encyclopedia." Whatis.techtarget.com.
URL: http://whatis.techtarget.com/ (July 23, 2001).

Ytteborg, Stale Schumacher. "PGPi FAQ." FAQs about PGPi, The International PGP Home Page. March 2, 2001.
URL: http://www.pgpi.org/doc/faq/pgpi/en/ (July 23, 2001).

"ZoneAlarm." Zone Labs.
URL: http://www.zonealarm.com/ (July 23, 2001).

"ZoneAlarm Pro." Zone Labs.
URL: http://www.zonealarm.com/ (July 23, 2001).

Zych, Tina. "Personal Firewalls: What Are They, How Do They Work?" SANS Information Security Reading Room.
URL: http://www.sans.org/infosecFAQ/homeoffice/personal_fw.htm (July 23, 2001).