Global Information Assurance Certification Paper

Implementing User Security Awareness Training

Author: Kelly Allison
Assignment Version: GSEC Practical Version 1.3
Date: 4 March 2002

Summary

User security awareness training is an important part of keeping your network secure. Untrained users often unwittingly expose the network to malicious internal attacks. However, there are simple measures that the users can implement to prevent these attacks, if they are properly trained.

This paper looks at why it is important to train users in security awareness and also includes information on security issues, such as password and laptop security, that could be included in your user security awareness training program.

Why Your Organisation Needs User Security Awareness Training

“We don't need user security awareness training. We have policies that cover these issues. Our current users know our policies and all our new users have to read and sign against them before they start work".

Does this sound like your company? Having policies is a great beginning but have you educated your users as to why you have these policies? Do they understand the implications to their data and the IT systems they use if they don't adhere to the policies? When the users understand how the policies are protecting their network and data they will be more inclined to follow them.

The 2001 CSI/FBI Computer Crime and Security survey states that 31% of attacks reported are initiated from the inside of networks, a large drop from the 49% in 2000. One of the factors attributed to the decline included “increased awareness of the consequences (of employee on-line activity) through user education programs”.[1] This does not imply your users are the ones attacking the network. Rather, that attackers exploit weak security inside the network. Untrained and unaware users create weak internal security. Could you be part of this 31% that was subject to attacks through internal means?

Do you understand the dangers involved with users running executables and of the weak passwords they choose? If you have policies and are an IT security professional then you must, so why not share your knowledge with the very people who may inadvertently pose risks to your network. By assisting your users to be security aware you are reducing the likelihood of attacks initiating from inside your network.

There are a variety of means available to educate your users on security, each is effective in their own way and using one is better than none. You can give presentations, distribute posters and handouts, have an internal website and send weekly/fortnightly/monthly emails, all dedicated to IT Security as it relates to your users. To see how one company implemented user security awareness in their organisation please visit http://rr.sans.org/aware/infosec_policies.php.

The following section is intended to be used as a base for your user security awareness training program. It contains information on aspects of IT security that is relevant to users, such as laptop and password security, social engineering and malicious software.

Information for Users

IT Security, How You Are Involved

Attacks are designed to compromise the Confidentiality, Integrity and Availability, the CIA, of your network and the data stored within it. For instance, viruses can affect the Availability of your network by clogging mail servers. They can affect the Integrity of your data by making changes to documents and they can affect the Confidentiality of your data by attaching documents to the emails the virus automatically generates and distributes. IT Security is there to protect the CIA of your network and data.

You may think, "what can I do? We have a firewall, we have IT staff to protect the network".

For your organisation to have a strong security infrastructure and therefore deter attacks and/or minimise the damage they cause there are three components that need to be focused on. They are technology, processes and people. Your organisation can have the latest technology, the best firewalls, the most skilled IT Security professionals in the industry but all it takes is one user who doesn't understand the risks of attaching a personal modem to a networked PC so they can dial in from home, and the whole system could be compromised. When you are aware of how you can deter, prevent or minimise attacks you are assisting your IT Security people to protect the Confidentiality, Integrity and Availability of your data and network.

The following pages cover ways you can protect your network, information related to your network and the data stored within the network.

Before we continue, an important point. Ensure you are familiar with your organisations IT security policies. By following the policies guidelines you will be protecting your network – that's what they are there for. Your organisation may have policies on topics such as the following:

- Passwords.
- Anti-Virus.
- Acceptable use; use of email, internet, intranet.
- Remote access.
- Unauthorised modems.

Specific Ways of Protecting Your Network and Data

Password Security

"Passwords are one of the first lines of defense that users have to protect their systems."[2] Once an attacker has your password they are able to access anything your account has access to. This means they can access the data you can, they can use your email, and they can use your Internet connection to browse sites they shouldn't. What's even worse is that the attacker could use your account to further probe the network and cause damage to more than what you can normally access.

"But if I don't tell them how can they know it?"

There are many free programs available on the Internet to scan networks for vulnerable passwords. Some programs compare your password to a list of words including some numbers, characters and even foreign languages until it finds a match. Other programs called 'sniffers' are used on the network to capture all data travelling the network, including your user ID and password. A 'weak' password will be cracked, or simply guessed, long before a 'strong' password.

A weak password will be composed of some or all of the following characteristics:

- All letters.
- A dictionary word.
- A dictionary word spelt backwards.

- Two dictionary words together eg rainumbrella.
- A dictionary word with numbers placed at the end or beginning.
- A dictionary word with certain letters replaced with corresponding numbers eg 1 in place of I or 0 in place of o.
- A word that is personal to you such as names of the members of your family, your favourite food or hobby.
- A word that is all one case be it upper or lower.
- Less than 7-8 characters.
- Follows a pattern eg 1bubble, 2bubble.
- Not changed frequently.

A strong password will be composed of all the following characteristics:

- Contain a mixture of upper and lower case.
- Have numbers and characters interspersed seemingly randomly.
- Changed frequently.
- At least 7 characters long.
- Unique, you will not use it as a basis each time you change your password eg April1, April2.
- Treated as Top Secret information by you.

"Fantastic", you say "but how on earth do I choose something that I will remember that fits all those characteristics."

The best method for choosing strong passwords is to create a phrase, take the first letter of each word and replace some of the letters with characters, numbers and intermixed upper and lower case letters.

For example:
I bought my dog on the 5th of November from Best Dogs = iBMd5/11@bd
Christmas is on the 25th of December = *XmS*25/D12

More tips on password security:

- **Change your password often** or depending on the value of the data you are trying to protect. For example, for not so sensitive data you could change it every 30 days, where as for extremely sensitive data you may choose to change it every 14 days, 7 days or maybe even every 3 days
- **Change your password if you think it's been compromised**. If you think someone may have seen you type your password in, if you wrote it down and then threw it out, change your password.
- **Don't use the same password for every account you have**. Split your accounts that need passwords into groups of three or so and select three different passwords. This way if an attacker obtains one of your passwords they wont be able to access all of you accounts, immediately at least.
- **Never write down your password.** If you absolutely must write it down store it in a safe or locked cabinet that only you have access to.
- **Never tell your password to anyone**. No one but you ever needs to know it.

Laptop Security

Not only is it expensive in terms of hardware costs when laptops are stolen, it can be expensive in terms of the information that is stolen off it. Think about your work laptops – what information do they contain, could it be valuable to another individual or organisation? What would the effect be on your organisation if the laptop was lost or stolen and the data on it accessed?

If the laptops are configured to connect to your work network and your laptop is stolen the new owners will

now have information related to your network that could be used for attacks. Information they could obtain includes IP addresses, user IDs, passwords and remote access capabilities. If, after thinking this over, you still think the data stored on your laptop is of little value do you want to be responsible for losing a $3000+ piece of equipment?

Here are some simple measures you can take to protect your laptop and the data stored on it:

- **When out and about keep the laptop with you at all times**
  - When travelling via plane do not check your laptop in as luggage, take it on board. Luggage has a habit of going missing
  - Do not leave the laptop in your car, not even in the boot. Your laptop might not be targeted but your car might be.
- **Keep the laptop in a bag that does not shout, 'laptop here'**, for example a normal briefcase or a backpack.
- **Do not write down the password to your laptop**. If you must write the password down please don't keep the password with the laptop. This is the equivalent to leaving your keys dangling in the lock to your house.
- **Do not keep sensitive data on the hard drive**. Process the data and then copy it to a floppy that you will keep on your person or separately from the laptop; if you must store it on the hard drive please see below.
- **Encrypt the hard drive**. If your laptop is not encrypted put a request through to your IT Department for it to be so. With encryption your laptop might be stolen but at least they can't steal the data off it.
- **Use strong passwords** as by recommended methods described in the password security topic of this document.
- **Consider using anti theft devices** such as cables or motion sensors.

Please visit this site for information on the products available to assist in securing your laptop: http://www.advisor.com/Articles.nsf/aid/VACCJ08-01.

Malicious Software - Viruses, Trojans, Worms
Email, Internet and Media Storage

By now we should all be aware of the dangers posed to our networks and data from malicious software; viruses, trojans and worms. Malicious software can make changes to your data, they can distribute and delete your confidential information, they can install trojans, programs that enable attackers to take control of your PC and they can propagate so quickly that administrators can be forced to shut down servers. Malicious software is a major risk to the CIA of your network and data.

Despite the widespread knowledge of how malicious software uses email to spread and infect, this is still the most common way your network and/or PC will become infected. "Over 90 percent of 2001's top threats used email as their primary means of propagation."[3] This is in part because the virus update often comes out a little bit too late or is not applied quickly enough and also through the very effective way malicious software writers use social engineering, for example the Love Bug. People liked the idea that someone they know, or even someone they have never heard of before, would send them an 'I Love You' message, the subject heading of the worm. So they double clicked on the 'LOVE-LETTER-FOR-YOU' attachment. People are also tricked into opening attachments through the use a double extension technique. Some software will hide well-known extensions so 'virus.doc.exe' looks like 'virus.doc'. The document is actually a program (.exe) but to you it just looks like a simple document.

Another common method of virus infection is via the Internet. The lovely screen saver you are about to download and install may look innocuous but is it? How do you know it doesn't have a virus or trojan

hidden within the program? Sure, you'll get a cute mouse running around your screen but what else might you get, an attacker controlling your PC with or files deleted off your hard drive!

What about those files you about to copy off that floppy disk or CDrom? Many organisations can become infected with malicious software from infected files copied to the network. How do you know the files you are transferring came from a 'clean' source?

'Well my organisation has anti-virus software installed. We are safe and there's nothing I can do to help anyway', I hear you saying. You are wrong. As mentioned above the virus updates can take longer to produce and install than the time it can take for the virus to reach your PC or mailbox.

Here are some ways in which you can help to keep your organisation free from viruses, trojans and worms:

- **Save all documents and executables (programs) to your hard drive or a floppy then scan them with up-to-date virus software before opening or installing**. This applies to all email attachments, no matter the file type, and software downloaded from the Internet.
- **If you receive an unsolicited email that seems unusual or suspicious then delete it**, or at least follow the above suggestion.
- **Always scan floppies and cds before copying the files to your network or work PC.**
- **Don't start up your PC with a floppy in the disk drive**. Your PC may be configured to boot off the floppy drive before the hard drive if there is a disk inserted. If the floppy is infected it can infect your PC on start-up.

Virus Hoaxes

While certainly not as damaging as a real virus these messages can affect the Availability of your network by clogging mail servers. Virus hoaxes have a sense of urgency and panic about them along with the specification in their message 'you must forward this message to everyone in your address book - immediately'. If you do this, and your colleague next to you does this, and the one next to them, and the one down the corridor and so on you can well imagine the amount of emails generated. The sheer amount of emails been forwarded on can slow down the transfer of legitimate, possibly urgent, email messages.

Below is a copy of a prevalent hoax message, commonly none as the 'sulfnbk.exe' hoax:

> IT IS IMPORTANT THAT YOU LOOK INTO YOUR COMPUTERS AND CHECK IF YOU HAVE THE FOLLOWING VIRUS:sulfnbk.exe
> IF ANYBODY HAS THIS VIRUS IN C:\, DELETE IMMEDIATELY BECAUSE IT ATTACKS ON NEXT DAY 25 OF THE MONTH MAY AND WILL DELETE ALL FILES ON YOUR PC.
> THIS VIRUS CAME WITH E-MAIL AND IS INVISIBLE FOR VIRUS SCANNERS.
> PLEASE PASS THIS MESSAGE TO OTHER PEOPLE.[4]

Most hoax messages have similar characteristics as the sulfbnk message:

- The virus may have extreme consequences if you are infected, for example as seen in the extract above, the virus 'will delete all files on your PC'.
- It claims the virus to be undetectable and/or incurable.
- The message may contain a large amount of exclamation points (!!!!!!!) or words in UPPERCASE to generate a sense of URGENCY!!!!!!!.
- It requests that you forward the message to everyone in your address book.
- The message does not include any reliable sources of information with regards to the virus.

- Spelling or grammatical errors.

What you can do to protect the Availability of your network with regards to hoax messages:

- Forward the message to your IT Security section notifying them that the message is been distributed throughout the organisation, then delete the message. Hopefully your IT section will send out a calming message to all staff.
- Just Delete the Message.

This site www.vmyths.com keeps records of virus hoaxes. You can search them to confirm the accuracy of any warnings you receive.
Note: Be aware of your organisations policies regarding virus hoaxes and/or acceptable use of email.

Social Engineering

We humans, as a general rule, like to think that all people are nice. That no one is going to go out of his or her way to trick us or manipulate us for any reason, let alone to gain access to our network. But unfortunately attackers do exactly this and when they do it is called 'social engineering'.

How do they do it? Social engineering plays on some common human characteristics, the main ones being our desire to trust and to help others. For example, the attacker may befriend you at a party. Once you 'warm' to the person they will try and extract information about the network from you (you may know more than you think you do). They may pretend to be an IT technician who has come to look at the server but who cannot find his way to the server room from the instructions 'Jack' from IT gave him. "He's obviously been asked to come here, he looks like a techy, I'll help him find the room. I'd hate there to be problem with the network".

Why do they do it? If you were a hacker what would you choose: A hours, possibly days or weeks or months, in front of a computer trying to guess or crack people's passwords or B 10-20 minutes on the phone to a user pretending to be a systems administrator who urgently needs to gain access to your account to fix a problem that if not fixed soon will prevent you from logging on tomorrow. Yes, he/she will need your password. Social engineering is effective and saves time.

Social engineers will attempt to get access to the network or obtain insider corporate information from you via:

- Telephone; eg "This is Jane Doe from IT Support. There seems to be a problem with your network account that is causing disruption to the network. Could you please log out and tell me your User ID and password so I can log in and resolve the issue."
- Email and/or Internet; eg "your organisation AAAAA has requested you take part in our 'insert any topic' online survey. Please click on the link below, enter your normal user ID and password and complete the survey before the end of the week."
- Snail Mail, eg Please fill out our survey and resend to 88888 Post Office Box for your chance to win a new car!' The 'survey' may be asking questions that could assist a social engineering attack directed at you, or it could be trying to gather information for an attack on the network.
- In person. Attackers may try to gain access to your building by posing as labourers, IT technicians, or fellow workers. They can gain access through locked doors by tailgating you through doors that require keys, pretending to be a genuine employee who has forgotten their pass or by carrying something heavy so you will open doors for them that normally require keys.
  Physical access to your building can lead to access to your network through data points and cabling. When an attacker is inside your building they will look for the passwords stuck to monitors or logged on PCs with no users on them.

Ways you can protect your self and your organisation:

- **Make sure you shred, burn, eat if you desire, all sensitive data be it on paper, CD or floppy**. Social Engineers may do what's called 'dumpster diving', searching through rubbish to obtain corporate information that may assist in an attack. For example, discarded corporate telephone directories can provide valuable information to a social engineer. Knowledge of peoples names, telephone numbers and positions of the people in your organisation or section enable an attacker to selectively choose targets.
- **Never reveal your password to anyone, for any reason**. If they really are an IT administrator they don't need to ask you your password, they can just change it.
- **Do not reveal network information to people.** This includes operating system information, known system vulnerabilities or mechanisms ie how often you are required to change your passwords.
- **Escort visitors at all times.** If your organisation does not have or wont implement this policy then it could be a requirement for your own section.
- **If you think you have experienced an attempted social engineering attack, either in person, Internet or mail based, report them to IT security or the relevant department.** Your organisation may have guidelines for reporting incidents such as these. Signs of an possible socially engineered attack as posted by the Computer Security Institute include "refusal to give contact information, name dropping, requesting forbidden information and misspellings." [5]

Principle of Least Privilege
Data Access Control

In IT security there is a term Principle of Least Privilege. When applied to users this means ensuring people have the least amount of access to or on the network they need to be able to perform their duties. Essentially, the less network accounts have access to the less that can be compromised if the network account is used by an attacker. By following Principle of Least Privilege you are protecting the Confidentiality, Integrity, and possibly the Availability, of your network and data.

How you can help ensure Principle of Least Privilege:

- **Control the amount of access you have**. If you are able to access information you shouldn't, or don't need to be able to then ask your IT section to remove the access. For example, you recently moved sections but you are still able to access the old sections data, ask your IT section to remove the access. If you have the 'rights' to be able to install software onto your PC, but you don't need to, ask that it be removed.
- **Control access to the data you are responsible for**. Are you the person who is responsible for authorising access to information related to your section? If so check who has access to it regularly. Ensure people who do not need access, don't. Using the above example, has someone recently left your section? Be sure to notify your IT section that the person can have their accessed removed.

Attaching Modems to Work Computers

"Using a modem while connected through a local area network" is number 5 on SANS "The Five Worst Security Mistakes End Users Make"[6] list.
Hopefully you are not making this mistake. Here are two reasons why you might be:

- To access sites on the internet that are blocked to your organisation
- To remotely connect to your organisations network from home.

It doesn't matter why; despite almost undoubtedly breaching IT security policy, both reasons are placing your network and data's Confidentiality, Integrity and Availability at serious risk. If a modem is attached to a PC without adequate security configuration attackers can completely bypass your organisations firewall, surface directly in the PC and then access and/or attack the network from there.

"But how could attackers know I have a modem attached?"

There are programs, freely available off the Internet, that can dial up phone numbers looking for PCs with modems set to auto answer attached to them. The programs are called 'war dialers' and the process is called 'war dialing'. The program will log the results of each call and the attacker will probe the positives further. Some war dialers will attempt to identify if any remote control software is running on the PC and then may try to crack the password, assuming there is one.

Once the attacker has access to your PC they can install a trojan, a facility to control your PC through the internet. Using the trojan the attacker has the same access to the network you have, they will be sharing your account and will have the same access as you have. But the attacker wont stop where you normally would, they will probe and scan and launch attacks until they penetrate deeper into the organisations IT infrastructure, causing untold damage, such as data corruption and changes to critical network configurations, along the way.

Here's how you can protect your network:

- **Do not attach modems to your work PC** and then connect to a private Internet Service Provider.
- **Do not attach modems to your PC** and then install remote control programs so you can dial in to work from home.
- **Submit a request to your IT department if you have a valid business need that requires private access to the internet or to remotely access the network**. They can install and configure the connections for maximum security.
- **Turn the auto-answer function of your modem off and use extremely strong passwords for remote control program**s. This applies to people with authorized modem connections and particularly to those who insist on having unauthorized modem connections.

Conclusion

One of the components of IT security often overlooked is the need to increase awareness amongst users of the role they play in maintaining the security of the network. The results of a recent survey by the Computer Security Institute and the FBI Computer Intrusion Squad has indicated that user security awareness training can lead to a decrease in internally initiated attacks on the network. There are many ways of increasing user security awareness, for example, regular emails, posters and even a website all containing relevant IT security information for users.

Users are thought to be the weakest link in the IT security chain as they often provide hackers with the opportunity to attack the network. This is because users are not aware of the ways they can help to keep the network secure, such as by choosing strong passwords, not attaching modems to networked PCs and by being aware of social engineering attacks. Implementing user security awareness training is an important part of your IT security infrastructure. It cannot be ignored forever.

References

1 Power, Richard. "2001 CSI/FBI Computer Crime and Security Survey." Computer Security Issues & Trends. Vol. VII, No. 1. Spring 2001
URL: http://www.gocsi.com/forms/fbi/pdf.html (5 Feb. 2002)

(Note: Link is to a form that needs to submitted before receiving a free copy of the survery via email).

2 "Password Protection 101." National Infrastructure Protection Center.
URL: http://www.nipc.gov/publications/nipcpub/password.htm (19 Feb. 2002).

3 "Computer Associates Releases Top 10 Virus List for 2001, Warns of Increasingly Complex Threats in 2002." Computer Associates. 27 Dec. 2001.
URL: http://www3.ca.com/press/pressrelease.asp?id=1856 (25 Feb. 2002).

4 "Sulfnbk." Sophos Anti-Virus. URL: http://www.sophos.com/virusinfo/hoaxes/sulfnbk.html (12 Feb. 2002)

5 Anonymous. "Social engineering: examples and countermeasures from the real-world." Computer Security Institute. Nov. 1999.
URL: http://www.gocsi.com/soceng.htm (11 Feb. 2002).

6 "Mistakes People Make that Lead to Security Breaches." SANS Institute. 23 Oct. 2001.
URL: http://www.sans.org/mistakes.htm (17 Feb. 2002)

Kaur, Harbinder. "Introduction and Education of Information Security Policies to Employees in My Organization." SANS Institute. 29 Aug. 2001.
URL: http://rr.sans.org/aware/infosec_policies.php.(19 Feb 2002)

Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics." SecurityFocus. 18 Dec. 2001.
URL: http://www.securityfocus.com/cgi-bin/infocus.pl?id=1527 (14 Feb. 2002)

Granger, Sarah. " Social Engineering Fundamentals, Part II: Combat Strategies." SecurityFocus. 9 Jan. 2002.
URL: http://online.securityfocus.com/cgi-bin/infocus.pl?id=1533 (14 Feb. 2002)

"Laptop Security Guidelines." LabMice.net.31. Jan.2002. URL:
http://www.labmice.net/articles/laptopsecurity.htm (17 Feb. 2002)

Vacca, John. "Laptop Security Product Overview. These tools can help you keep your laptop on your lap, and out of thieves' hands". Advisor. 21 Feb. 2002.
URL: http://www.advisor.com/Articles.nsf/aid/VACCJ08-01(22 Feb. 2002)

"Computer Viruses Dymstified." Sophos Anti-Virus. URL:
http://www.sophos.com/sophos/docs/eng/refguide/viru_ben.pdf (13 Feb. 2002)

"The SANS Security Policy Project." SANS Institute. URL:
http://www.sans.org/newlook/resources/policies/policies.htm (12 Feb. 2002).

"Password Security: A Guide for Students, Faculty, and Staff of the University of Michigan. Questions You May Have About Password Security." University of Michigan, Information Technology Division. Apr. 1997. URL: http://www.umich.edu/~policies/pw-security.html (25 Feb. 2002).

"War dialing noun." Logophilia. 17 Feb. 1997, URL http://www.logophilia.com/WordSpy/wardialing.asp (11 Feb. 2002).

Berg, Al. "Security. Cracking a Social Engineer. Enterprising thieves use a variety of common techniques to pilfer information." Packetstorm. 16 Aug. 1999.
URL: http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html (24 Feb. 2002).

Cole, Eric. Hackers Beware. Defending your network from the Wiley Hacker. United States of America: New Riders Publishing, 2002. 57 -58, 710-713.

Scambray, Joel. McClure, Stuart. Kurtz, George. Hacking Exposed. Second Edition. Network Security Secrets & Solutions. California: Osborne/McGraw Hill, 2001.121-128, 561-562.