Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

The Importance of Security Awareness Training

One of the best ways to make sure company employees will not make costly errors in regard to information security is to institute company-wide security-awareness training initiatives that include, but are not limited to classroom style training sessions, security awareness website(s), helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of company security policy, procedure and best practices.

Copyright SANS Institute
Author Retains Full Rights

AD

© SANS Institute 2009, Author retains full rights.

The Importance of Security Awareness Training

GIAC Gold Certification

Author: Cindy Brodie, cstakley@wccnet.edu

Adviser: Rick Wanner

Accepted: June 30th 2008

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

Introduction 3

Types of Training 4

Classroom-Type Training 5
Security Awareness Website 6
Helpful Hints 7
Visual Aids 8
Promotions 8

Training Topics 8

Physical Security 9
Desktop Security 9
Wireless Networks and Security 10
Password Security 11
Phishing 13
Hoaxes 14
Malware 15
Viruses 15
Worms 17
Trojans 18
Spyware and Adware 18
File Sharing and Copyright 18

Conclusion 19

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

I. Introduction

One of the greatest threats to information security could actually come from within your company or organization. Inside 'attacks' have been noted to be some of the most dangerous since these people are already quite familiar with the infrastructure. It is not always disgruntled workers and corporate spies who are a threat. Often, it is the non-malicious, uninformed employee (CTG, 2008).

The focus will be on uninformed users who can do harm to your network by visiting websites infected with malware, responding to phishing e-mails, storing their login information in an unsecured location, or even giving out sensitive information over the phone when exposed to social engineering.

One of the best ways to make sure company employees will not make costly errors in regard to information security is to institute company-wide security-awareness training initiatives that include, but are not limited to classroom style training sessions, security awareness website(s), helpful hints via e-mail, or even posters. These methods can help ensure employees have a solid understanding of company security policy, procedure and best practices.

Some of the more important items to cover in your security awareness training are your

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

organization's security policy, data classification and handling, workspace and desktop security, wireless networks, password security, phishing, hoaxes, malware, file sharing and copyright (University of Tennessee).

II. Types of Training

Organizations are starting to realize there really is a need for security awareness training. According to a study conducted by McAfee in 2005, the following statistics revealed a rather startling necessity:

- "One in five workers (21%) let family and friends use company laptops and PCs to access the Internet" (Schneier, 2005).
- "More than half (51%) connect their own devices or gadgets to their work PC... a quarter of who do so every day" (Schneier, 2005).
- "One in ten confessed to downloading content at work they should not" (Schneier, 2005).
- "Two thirds (62%) admitted they have a very limited knowledge of IT Security" (Schneier, 2005).

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

- "More than half (51%) had no idea how to update the anti-virus protection on their company PC" (Schneier, 2005).
- "Five percent say they have accessed areas of their IT system they should not have" (Schneier, 2005).

Security awareness training can be performed in a variety of ways that can be utilized alone or in conjunction with each other. Those mediums can consist of a more thorough classroom-style training, creation of a security-awareness website, pushing helpful hints onto computers when they start up and/or e-mailing helpful hints on a weekly or monthly basis, and utilizing visual aids like posters.

A. Classroom-Style Training

Utilizing a classroom setting for security-awareness training can offer the benefit of lecture-based and interactive learning as well as the availability of someone to answer questions in real time. There can also be a Q&A period after the materials are presented as well as contact information distributed for questions that might pop up afterward.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Some companies offer both live and web-based training and utilize a variety of methods such as role-playing and simulation games so the interaction is more two-way than one-way. Other companies offer videos, web-based training, and live trainers. The method you use is by no means limited (Dublin, 2006).

This type of training can vary in the amount of time it can take. The security awareness training I have implemented at Washtenaw Community College takes about two hours, but it has no real interactivity such as role-playing or simulations; just PowerPoint and Q&A. Training time can depend on the effectiveness and the extent of the material discussed. Training sessions could possibly take a full day if need be.

B. Security Awareness Website

Another way of implementing a security awareness program is through the creation of a security awareness website. This website could consist of different sections with the different areas that need to be covered (e.g. Malware, hoaxes, file sharing and copyright, etc). The University of Tennessee implemented a very impressive security awareness website complete with videos, examples, and helpful external links (http://security.tennessee.edu/).

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Another implementation of the security awareness website could be a self-paced tutorial where users can log in and go through it, taking mini quizzes at the end of each section to make sure the material is actually being read and absorbed. Utilizing logins can also be a means of keeping track of who has (and more importantly who has not) taken the training. An FAQ section could be implemented as well as contact information for users to ask questions that are not addressed in the FAQ.

C. Helpful Hints

Utilizing helpful hints and tips is more of a supplement to the training, be it via classroom style or online, and should not be used as a means of security awareness training on its own.

Helpful hints can consist of tips and reminders that are pushed to user screens when they log in. These tips and reminders can consist of key points emphasized in the training (e.g. "Never keep your password in a place that can be accessed or viewed by anyone besides yourself."). Reminders can be as simple as reminding someone to change their password or run their virus scan.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

D. Visual Aids

Visual aids are another item that should not be used as the lone source of security awareness training, but more as a supplement. The University of Michigan recently created a series of catchy password security posters that compare passwords to underwear. One says to change them often, another says to not leave passwords lying around, and another one says to not share them with friends (www.itd.umich.edu/posters/).

E. Promotions

Security tips can appear on flyers distributed across the user base and one could even go so far as to hand out pencils and/or key chains with a catchy security-related phrase or reminder (e.g. "Unexpected attachments can mean unexpected chaos: Please do not open them").

Now that we have addressed possible methods in implementing security awareness training, what should be covered in the training will be addressed.

III. Training Topics

Topics addressed by the security awareness training should consist of a combination of

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

existing organizational policies and procedures (how they tie in with each aspect, if they do), physical security, desktop security, password security, phishing, hoaxes, malware (viruses, worms, Trojans, spyware, and adware), and copyright with regard to file sharing.

These topics will help employees understand why security awareness is important and guide them in knowing how to prevent incidents from happening and what to do if one occurs.

A. Physical Security

When addressing physical security, locking your doors and desk/file cabinet drawers should be the main focus. A helpful item to include could be the crime statistics, more specifically thefts, from the organization. Another item to lightly touch upon (but go into greater detail in Desktop Security) is the fact that if a potential attacker has access to a user's computer, they could install a key logger or actually get into a machine that has not been locked.

B. Desktop Security

The desktop security section should go into detail as to why it is important to either have a password-protected screen saver or, even better, to get into the habit of locking computers when users walk away from them. A screensaver timeout should be utilized

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

so if a user walks away from their computer, the password-protected screensaver would come up. Personally, I have mine set to 5 minutes, but upon doing a Google search regarding typical screensaver timeouts, the average response was 10 minutes. This information can and should be supplemented with information on how to do this. Tactics a potential attacker could utilize (e.g. Shoulder surfing, key loggers, etc) also need to be addressed. The pill of having to take extra measures to make sure your desktop is secured can be swallowed more easily if users understand WHY they should be taking them.

Another item that could be addressed is to make sure users understand that it is important that they shut down their computers at the end of the day. Sometimes this allows for valuable updates to be applied and doing your own part for a greener environment. If somehow a potential attacker gains access to a computer that is turned off, they will be less likely to utilize it than one that is already turned on and unlocked.

C. Wireless Networks and Security

The wireless networks and security section should address the unsecure nature of wireless networks as well as tips and tricks to exercise caution and harden laptops

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

against the dangers of ‘sniffing.’ Emphasis should also be placed on not storing any kind of sensitive information on laptops that will be accessing a wireless network.

Another area that should be covered is the importance of firewalls. Windows Firewalls by themselves are not enough. Most times companies will provide a purchased firewall on company-supplied laptops and computers (e.g. Sophos, McAfee, Norton, etc), but personal laptops that may utilize the company wireless network need to have a firewall on them. For small office environments as well as those who remotely access their workstation from home, it is always helpful to provide information on free firewall options like ZoneAlarm and Comodo as well as relatively inexpensive firewall options like McAfee and Norton. The free firewalls are more for the personal user, though and not for commercial use. It may also be a benefit to the training to compare the price of a laptop to the price of a breach. A breach would not only cost the company a vast sum of money, it could also cause the user

D. Password Security

The password security section should include what constitutes a strong, secure password or passphrase, with an emphasis on passphrases since they are harder to guess and to crack. This section should also outline the minimum password

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

requirements of the organization.

Sharing passwords as well as leaving them out where anyone but the user could access them should be strongly discouraged. Making this part of organization-wide policy could be very helpful in this arena. If this is incorporated into policy, this should be addressed in the training. Users need to be aware a policy is in place and general "rules of thumb" to make sure these policies are followed. Statistics could also be a good supplement. For example, a delegated individual could go around to all of the offices and see if they can uncover any unsecured passwords. They could even take this a step further and see how many computers are left on as well as without password-protected screensavers. No specific individuals would be singled out, just a number of instances out of the total number of computers would suffice.

Helpful hints and rules of thumb should also be a part of this section. For example, passwords should not contain the username or any part of the user's full name. Passwords also should not be based on personal information such as a spouse name, favorite team, or pet. Examples of passphrases (e.g. Isaw3redtrucks) could help win more users over from password to passphrase. Another important point is to stress that the default password given to users should always be changed immediately. Instructions on how to change passwords should also be included.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

To round out the password security section, it can be very beneficial to define what constitutes a poor choice of password as well as a listing of the most common passwords used.

E. Phishing

When discussing phishing, the term as well as the purpose should always be defined. Examples are key to this portion of security awareness training. Things to avoid (e.g. clicking on links provided in e-mail, submitting banking and password information via email, etc) should be highly emphasized so people know what to look for. It could also be beneficial to have users take a Phishing IQ Test. There are a number of Phishing IQ Tests online, but the one I highly recommend is at http://www.sonicwall.com/phishing/ since SonicWall is a company that actually deals in security. This way the bits and pieces that can identify a phishing e-mail can be explained and displayed.

Another item that should be addressed is how to actually fight phishing attacks. A couple of web sites actually encourage the reporting and tracking of phishing web sites and e-mails: PhishTank (www.phishtank.com) and The Anti-Abuse Project (www.anti-abuse.org/), which also addresses Spam and copyright. PhishTank appears to be a

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

bit more vigilant about fighting phishing in that it allows the user to enter a phishing site into their database, determine whether or not the site has been reported by others, and track the status of the submissions you make.

F. Hoaxes

Hoaxes should be addressed in the training because a lot of time and resources can be spent reading and forwarding hoax emails. The types of hoaxes as well as examples should be the meat of this section. Using familiar hoaxes is the best option so it will be easier to grasp. It could also be beneficial to compare hoaxes to viruses in that they are spread by continually forwarding them. The dangers of hoaxes should also be addressed because some hoaxes warn of a virus and tell users to delete valid and sometimes important system files.

Preventing the spread of hoaxes should also be covered. Hoaxes can be prevented by checking a number of hoax sites on the Web (e.g. Snopes – http://www.snopes.com and Vmyths – http://vmyths.com) and following a few rules of thumb. It is important to point out that if something sounds too good to be true, it probably is and if something seems suspicious it can be checked on one of the hoax sites.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

G. Malware

When addressing malware, it should always be defined and then broken down into its categories: viruses, worms, Trojans, spyware, and adware. After each category is broken down, address how they end up on systems.

1. Viruses

Start out by outlining what makes a virus a virus. It is important for users to be able to identify a potential virus when they see one or to identify characteristics of a virus that has already infiltrated the user's system. What a virus is capable of is also something that should supplement the defining of what makes a virus what it is.

Defining what a virus is and how to identify one must be complemented with the important of antivirus software. Most organizations will have this installed on all organization-wide computers, but this might not be installed on laptops used by employees. Users also need to learn the importance of not only performing regular scans of their computers, but also of any file they download from a web site, e-mail, or thumb drive.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Another important tip to include is how vital it is to keep systems and applications up-to-date. Never assume that a system or application is always going to update itself. Users should proactively see if the systems and applications they are using need updated.

Finally, it is important to let users know what to do if their system does become infected. Make sure not to incite a sense of panic (e.g. "You let this happen! You are on probation!") that would steer employees toward hiding the infection until it has gotten out of control or their machine is beyond repair. The main procedure to address is what to do if and when a virus infects a work machine, since it would differ considerably to what to do at home.

When your work machine becomes infected, do not do anything to the computer aside from performing a scan with the anti-virus software on the machine. Phone the I.T. Department of your business (or I.T. person) to come evaluate your machine and hopefully get rid of the virus.

If your machine at home (especially if you work from home) becomes infected, it is important to follow the following steps outlined on Viruslist.com:

1. Do not panic.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

2. Disconnect from the Internet and any Local Area Network it may be connected to.

3. If computer cannot boot, try starting in Safe Mode or boot from the Windows boot disk.

4. Back up any important data you cannot afford to lose to an external drive (scan the file with your anti-virus software first) (floppy, CD, jump drive, etc).

5. If you do not have anti-virus software installed (which SHOULD not be the case), install it and then update it.

6. Perform a full scan of your system (2008, Viruslist.com)

2. Worms

The worms section can be handled much the same way the virus section is handled: Definition, how to spot, what it is capable of, how to prevent, what to do if one invades the system.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

3. Trojans

Like the previous 2 sections, the Trojans portion should define what they are, what they can do, what can be done to prevent them, and what to do in the event of one making it onto the system.

One item that should be emphasized is that Trojans are different from viruses and why they are two different things.

4. Spyware and Adware

Again, spyware and adware should be defined, what they can do should be outlined, prevention tips and tricks, and then what to do if it is found on the system.

Spyware and adware identification and removal programs should also be addressed, most of which are free (e.g. Ad Aware, Spy Sweeper, etc).

H. File Sharing and Copyright

When addressing copyright with regard to file sharing, the types of copyright being referred to (e.g. recordings, videos, and software) should comprise the introduction.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Suggestions on how to legally acquire copyrighted works digitally should conclude the introduction.

File sharing programs and methods should be the next item to be covered (e.g. peer-to-peer programs and bittorrenting). It should also be emphasized that, while being illegal, these programs and sites offering the resources for them are breeding grounds for viruses. It should also be stated that illegal file sharing and downloading is a waste of resources and, if the organization's policy addresses it, can be a punishable offense.

This section should be rounded out by stating the legal consequences of illegal file sharing and downloading as well as examples of cases that have been brought against people who have been caught doing this.

IV. Conclusion

In conclusion, security awareness training, if implemented correctly, is an important necessity for any organization. If the user base is properly informed as to what to watch for, prevention, and remediation procedures, this alone could prevent a lot of potential problems that could affect the infrastructure and the company as a whole. Often it is just awareness that is the

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

key to prevention and protection.

"Employees can and should be the last line of defense." Security awareness training can pay off by training users on what they can do to prevent malicious activity and what to do in the event of such activity. Of course security awareness training is not the be-all-end-all, it is a significant layer of security to add to existing security measures (Rothman, 2007).

© SANS Institute 2009, Author retains full rights.

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

References

(Anti-Abuse project 2008). Retrieved September 29, 2008, from The Anti-Abuse Project (TAAP) Web site: http://www.anti-abuse.org .

(Corporate Technology Group 2008). The threat within: is your company safe from itself? Retrieved September 22, 2008, from Corporate Technology Group Web site: http://www.ctgyourit.com/newsletter.php .

Dublin, J (2006, November 1). Security awareness training: stay in, or go out?. Retrieved September 23, 2008, from SearchFinancialSecurity.com Web site: http://searchfinancialsecurity.techtarget.com/tip/0,289483,sid185_gci1294533,00.html?bucket=ETA&topic=300030 .

Information security office. Retrieved August 28, 2008, from The University of Tennessee Web site: http://security.tennessee.edu/ .

ITCS: passwords are like underwear poster program. Retrieved August 28, 2008, from Information Technology Central Services at the University of Michigan Web site: http://www.itd.umich.edu/posters/ .

Mikkelson, D.P. (2008). Urban legends reference pages. Retrieved September 29, 2008, from

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Snopes.com Web site: http://www.snopes.com .

(Phishing IQ test 2008). Retrieved August 28, 2008, from SonicWall Web site: http://www.sonicwall.com/phishing/ .

(Phishtank 2008). Retrieved September 29, 2008, from PhishTank Web site: http://www.phishtank.com .

Rothman, M (2007, May 3). Ask the security expert: questions and answers. Retrieved September 23, 2008, from SearchSecurity.com Web site: http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1262609,00.html .

Schneier, B (2005, December 19). Insider threat statistics. Retrieved September 23, 2008, from Schneier on Security Web site: http://www.schneier.com/blog/archives/2005/12/insider_threat.html .

(Viruslist.com 2008). Viruslist.com: What to do if your computer is infected. Retrieved September 29, 2008, from Viruslist.com Website: http://www.viruslist.com/en/viruses/encyclopedia?chapter=153280800

(Vmyths 2008). Vmyths: truth about computer security hysteria. Retrieved September 22, 2008, from Vmyths Web site: http://vmyths.com .

© SANS Institute 2009, As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**