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.

Essential Information Security For Corporate Employees

This paper was written to raise security awareness and provide corporate employees with essential security information that emphasizes critical issues surrounding an implementation of security "best practices" throughout an organization. Do not assume that this paper is an all inclusive guide to corporate information security. Information security consists of four major components: technology, process, policy and culture. This paper focuses on culture and specific human factors that weaken security in an organization. ...

Copyright SANS Institute
Author Retains Full Rights

AD
Investigate Insider Threats
Protect your company against corporate IP Theft
Learn More
SpectorSoft

ESSENTIAL INFORMATION SECURITY FOR CORPORATE EMPLOYEES

"THE MOST ESSENTIAL BEST PRACTICES"

SANS GIAC GSEC Practical

Version 1.4b Option 1

LLOYD GUYOT

June, 2003

Table of Contents

INTRODUCTION **1**
ABSTRACT **2**
PERSONAL BEST PRACTICES **2**
- **Social Engineering** 2
- **Electronic storage and transfer of information** 5
- **Passwords** 6
- **Email** 7
- **Portable Computers** 8
- **Telephone Voicemail** 9
- **Wireless Computing** 9

SUMMARY **11**
BIBLIOGRAPHY **13**
APPENDIX – A TEN WAYS TO GET SPAMMED **14**
APPENDIX – B YOUR PERSONAL CHECKLIST FOR ESSENTIAL SECURITY **15**
GLOSSARY **19**

INTRODUCTION

This paper was written to raise security awareness and provide corporate employees with essential security information that emphasizes critical issues surrounding an implementation of security "best practices" throughout an organization.

Do not assume that this paper is an all inclusive guide to corporate information security. Information security consists of four major components: technology, process, policy and culture. This paper focuses on culture and specific human factors that weaken security in an organization.

Please be advised that this is a "what to do" paper not a "how to do" paper. This paper is written in a style that attempts to address the non-technical person. We lightly touch on the "why to do" but comments are limited to providing only basic understandings. Our goal is to facilitate changing current culture through security awareness so that each day, every one of us demonstrates a proactive role in protecting intellectual assets from falling into the wrong hands.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ABSTRACT

Information Security's weakest link is people. The Computing Technology Industry Association states that nearly two-thirds of reported security breaches are primarily the result of human error [1]. Information security is a distributed responsibility and is very important to the survival of any business. Each one of us must make it our personal business to know and adhere to company security policies otherwise security attacks will always present an unacceptable risk to the enterprise and its future well being.

It is important to note that the risk of an information security breach increases significantly in the following scenarios: 1) Your organization is involved in a highly competitive business climate; 2) Your organization has terminated an employee that holds a grudge; 3) Your organization has individuals that lack security awareness and best practices.

Please read on to learn how you personally can help prevent a potential information security breach from taking place in your organization through personal awareness and information security best practices.

PERSONAL BEST PRACTICES

To follow are a few selected categories sensitive to security issues that you can use as a reference to protect you and your organizations information assets and help prevent a potential information security breach from taking place.

Social Engineering

Most individuals are trusting and helpful. People looking to acquire information they wouldn't normally have access to will attempt to exploit this natural behavior using deceptive practices to abuse your trust. Phony telephone calls, phony websites, dangerous email attachments and poorly configured equipment are just a few example methods that bad people use to acquire information they shouldn't have. Thieves commonly use deceptive tactics such as sympathy, guilt and intimidation to access or obtain confidential information by masquerading as a legitimate employee, contractor, vendor or business partner. These thieves, sometimes referred to as "social engineers", work to exploit your trust. As a counter measure to maintain effective information security, when you are requested to perform an action or provide confidential information, you must always *positively* identify the requestor and verify that they are who they say they are and that the requestor is a current employee and has verified content owner approval for access prior to acting upon their request. *In short, never provide personal or internal company information to anyone unless you recognize the requestor and they have a need to know.*

In the book, "The Art of Deception" by Kevin Mitnick and William Simon, we are reminded of how easy it is for social engineers to illegally gather sensitive information from any given organization.[2] If you find yourself on the following list then be aware, you are one of the common people targets of social engineering attacks…

1. Receptionists, Telephone Operators, Admin Assistants, security guards.
2. Help Desk personnel, technical support staff, system administrators, computer operators, telephone system administrators.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3. Finance, Human Resources, Engineering, and Information Technology personnel.
4. Any employee new to a given area.

Social engineering methods are all about defying your expectations. Be aware that there are hidden dangers with seemingly innocent conversations. Social engineering comes in many flavors with many hidden agendas. One kind may involve an attacker getting to know you intimately and then using that knowledge to steal vital information, even your identity. If you are on the above "hit list" you really need to watch yourself. Be careful that your desire to be helpful in performing everyday tasks does not lead to giving away confidential details to the wrong person about your organizations business. Don't fall into the trap of trusting a person until they prove to be untrustworthy. Ask the right questions by first positively verifying the requestors' identity before any sensitive information is released.

One successful method "social engineers" use is to call you pretending to be a "hopeless user." This method allows an attacker to learn about a specific process. Such an approach plays off gaining your trust by making you feel good about yourself. Be suspicious if you get a request from someone asking you to fax or email information to them right away, but refuses to provide you a direct callback number. This "social engineering" tactic works especially well when combined with the theatrics of pushing, rushing, yelling, and even screaming at you for the information to be sent without delay. Don't be intimidated into giving out information to an irate caller, or one who seems to know the structure of your organization. Another intruder tactic to watch out for is the "odd" request. If a caller asks for information that seems a bit out of the ordinary--such as what operating system does your company use -- that caller may be a "social engineer" trying to understand the infrastructure of your network.

Be careful not to cut corners by writing down passwords or leaving confidential material lying around. Follow the password best practices as detailed in the next section of this paper. Also remember to securely store confidential material. That means don't leave sensitive information lying around, especially at the printer. And if you are throwing confidential material away, shred it first. Far too often social engineers find the company confidential information they are seeking just by looking at what is left sitting around at the printer or fax machine or by looking through your trash. If you print something or have something faxed to you, pick it up right away and store it securely. If you are throwing it out and you are not sure if it is confidential, shred it anyway, just to be on the safe side.

Watch for these *warning* signs of a possible attacker…

1. The person refuses to provide a direct callback phone number.
2. Their request is not ordinary.
3. They try to claim authority.
4. They stress urgency.
5. They threat negative consequences If you don't comply.
6. They show discomfort when questioned.
7. They will often use name dropping to get what they want.
8. They will often compliment, flatter or flirt with you to get what they want.

Sharing Information

Always verify the identity of the requestor before providing confidential information. Verify the requestors' identity in person with a picture ID or on-line with a secure-id key-fob / token. If you are on the phone, verify the requestors' identity by recognizing the voice of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

someone you know and then confirm with the requestors' manager, supervisor or Human Resources the requestors' employment status. Based on your requestors' current responsibilities, verify their need to know with the content owner of the confidential information they are requesting.

Always be aware of how sensitive the information is that you are working with and the need to verify the identity of the requestor to ensure proper procedures for protection of corporate data is followed. A quick reference is provided in the chart below.

Authentication Procedure Model

CLASSIFICATION	DESCRIPTION	PROCEDURE
Level – 1 **PUBLIC**	Non-Sensitive information that can be freely released to anyone. Examples: - product brochures - corporate website	No action - no need to verify identity of requestor.
Level – 2 **INTERNAL**	Information intended for use only between employees and partners. Examples: - personnel reporting structure - employee names and titles - internal phone numbers - names of departments & projects	Verify identity of requestor to ensure they are indeed an active employee or verify that a nondisclosure agreement is on file and management approval of non-employee / partner is confirmed.
Level – 3 **CONFIDENTIAL**	Sensitive information that is shared only between employees and partners that have a *verified* need to know. Examples: - social security numbers - credit card numbers - salary information - quotations - computer configuration info - computer system procedures - source code - all remote access info - manufacturing processes - marketing data - business plans - product / part specifications - customer lists - trade secrets	Same as Internal procedure above plus… Verify need to know with content owner before disclosing any information to the requestor. Note: - Only management personnel may authorize disclosure of this level of information to non-employees. - Shred all documents that contain any confidential information before throwing away.
Level – 4 **RESTRICTED**	Information that is not to be shared. Example: passwords	Never disclose restricted information to anyone under any circumstance, especially your password - not even to the IT Help Desk or IT Security.

* Model adopted from various sources including the book, "The Art of Deception" by Kevin Mitnick and William Simon

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Personal Best Practices – (cont.)

Electronic storage and transfer of information

Private internal networks are not as private as one might think. In an effort to improve business efficiencies, many private internal networks are connected to the Internet and possibly one or more partner networks. Because an organization has no control over the quality of security methods practiced on the Internet or partner networks you personally need to take special care when storing or transferring sensitive data.

Determine your data sensitivity from the Information Sensitivity Model listed previously and use the following guidelines for security best practices.

1. If you are unsure of the level of sensitivity of the information you are working with, contact the owner of the data to verify the level of sensitivity before storing or transferring the information.
2. If you are a data owner, be sure to communicate the sensitivity of your data to administrators and users so they can treat information appropriately.
3. Assign security permissions to a role or group rather than to an individual. It is far easier to ensure the security of a few groups than it is to administer a long list of unique names.
4. Always take a "default deny" stance in providing access to information. Only provide the minimum level of access necessary to meet specific business requirements. For example, if you are storing a file on the network to share with others, only provide write access (the ability to change the file) to those few that have a real business need to change the file. Provide everyone else "read-only" access. Contact your I.T. Help Desk or I.T. Security for assistance.
5. Set up a process to proactively audit who has access to your information. Remove or disable all unused access IDs and privileges on a regular basis. Provide only active personnel that have a real business need with access to your information. Log and monitor access of sensitive information and notify your management and IT Security of any noticeable misuse.
6. Classify data you own according to the Information Sensitivity Model listed previously and keep the data partitioned by as many levels of technology separation as practically possible. E.g. separate databases, hosts, schemas, etc. Using this method, if an information breach occurs in one area the other areas of data are protected from exposure. In other words, keep Level 1 – "Public" information separate from Level-2 "Internal" information and keep Level-3 "Confidential" information separate from Level-2 "Internal" information and so on. As an example: Never place Level-2 "Internal" or Level-3 "Confidential" operational manuals (company or equipment) in a web area that is accessible to the public. Social Engineers surfing the web can use this information for inappropriate activities exploiting weaknesses that could harm your organization.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

7. **A)** If you transfer Level-2 "Internal" information across the Internet, make sure that the data transmission is encrypted to prevent non-authorized access.
   B) If you transfer Level-3 "Confidential" information across the Internet, make sure both the transmission and storage of your information is encrypted.
   NOTE: Contact your IT Help Desk to determine the best tools and method. The **Email** section below provides additional information.
8. If you have a choice between storing Internal or Confidential information on your local hard drive or a company network drive choose to store your information on the company network drive. Company network drives are more secure and are backed up on a regular basis. If you have no choice but to store Internal or Confidential information on your local hard drive make sure to password protect and / or encrypt your sensitive files. Also be sure to backup your local hard drive on a regular basis. Your backup will come in handy if ever your PC is compromised or stolen. Again, contact your IT Help Desk to determine the best tools and method for your backups.

Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of your organizations entire corporate network. As such, all corporate employees (including contractors and vendors with access to the organizations systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The result of selecting a good password means that the password can not be guessed, searched for or predicted by others.

Only you can protect your organizations sensitive information. In many instances confidential information is only as safe and secure as the strength of your password. Do not use family names, nicknames, anniversaries, birthdays or pet names. Don't use sports teams either. If someone were at your desk and sees you have a Detroit Lion's poster, guessing your password, like 'Go Lions' or something similar is quite easy. Finally, do not use the word "password" for any of your personal password selections. It is important that you select a password that is long and strong and a non-dictionary word. Ideally, use a minimum of 8 characters using both upper and lower case letters, and a mix of numbers and special characters or symbols. To help you remember your password use the first letter's of each word in a phrase that means something to you. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R@" or "Tmb1W#r$" or some other variation.

Keeping your password to yourself is critical to your company's security. Only you can protect your organizations sensitive information. Never change your password to something known to anyone else, not even for a moment. Never share your password with anyone – including your manager, IT Security, IT Help Desk, family, friends or co-workers. Even if someone calls you and says they are from I.T. Security or the I.T. Help Desk and they need your password to check something, don't give it to anyone who asks. This could very well be an attempt by an unauthorized person to "social engineer" you into giving them your password. No one in I.T. should ever ask for your password over the phone for ANY reason. If this happens, you should get their name and number and call your manager and IT Security to report a possible security incident. Never display your password anywhere especially on a post-it note near your computer, or under your

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

keyboard as we've seen so many times. Finally, never use the same password for both your work and personal accounts. Be accountable and take responsibility for the usage of your password(s). Only you can prevent a security incident from happening. Remember to do your part to help keep company confidential information secure.

Email

What would we do without email? Today it's hard to imagine any organization not providing its employees with Email access. Successful organizations leverage email as a competitive advantage. As with most tools, Email has its risks and user responsibilities. Did you know that by default, Email systems send the body of your Email in plain text? That means that anyone with easily available tools can sniff the Internet and read the content of your Email without you knowing. If you have sensitive Email destined to an Internet address use an encryption tool to send the content body of your Email as an encrypted attachment that is password protected. There are several encryption tools available. Check with your organizations IT Help Desk to confirm your use of an approved encryption tool. If your IT group has not selected an encryption tool and you are shopping for one yourself you will want to make sure that the encryption software you select supports the 128-bit Advanced Encryption Standard (AES).

If you have provided your Email address in response to a website or newsgroup you can be assured that your address has been collected by a spammer. A spammer is one who scans the Internet looking for as many email addresses as possible and then uses them to flood the Internet with copies of the same message (typically commercial advertising) in an attempt to force the message on people who would not choose to receive it.[3] Because of this bad practice, never open or respond to spam (junk Email). A response confirms that your Email address is an active one, and invites even more spam. For more information on how to keep your Email address off a spammer list reference the Appendix at the end of this document.

When it comes to Email the best security practice you can perform is to never open or respond to an email or attachment from an unknown source as it may contain a Virus, Trojan or Worm that can adversely affect your computer and others on the network. If you don't recognize who the Email sender is It is always best to not open the Email. Your safest bet is to delete unrecognized Email.

Personal Computers

Personal computers are today's workhorse tool of choice. While computer prices continue to fall and functionality and performance continues to rise, we find more and more people are adapting to this new way of "auto-magically" getting more work done faster. Problem is most computer users are self-taught, not having the time or money for formal computer training. If you do not take responsibility for the safe management of the computer you use, you may be at risk of loosing sensitive data or even worse, having your personal identity stolen.

First things first - Only install software from trusted sources. Often, digital signatures are used by software vendors to ensure trust and to verify authentication so that you know that they are who they say they are. If you are not 100% certain that the software you want to install is from a trusted source stop – do not install. Un-trusted software is known to provide back doors for would be thieves to access your computer.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Make sure to keep all your software versions up to date with the most current patches and fixes. Manufacturers usually provide these updates free of charge. If you are looking to update your home computer visit the Internet website of each software vendor for their respective updates. Check with your organizations IT Help desk to get an understanding of the process for obtaining the latest updates for your business computer.

Before using a personal computer to access the Internet the first thing to do is to install antivirus and firewall software. Anti-virus software is designed to prevent a program or piece of code from loading on your computer without your knowledge and running against your wishes. Anti-virus software can protect you against known Viruses, Trojans and Worms which can be annoying or destructive. Often this type of malicious code will allow hackers to gather your personal data or take control of your machine.

A Firewall is a system designed to prevent unauthorized access to or from a network or individual computer. Firewalls can be implemented in both hardware and software or a combination of both. A firewall examines the data flow and blocks data that does not meet your specified security criteria. Trend Micro Inc. OfficeScan is one popular software package that includes both anti-virus and personal firewall protection. No computer should be connected to the Internet unless it is protected by an anti-virus and firewall system. Always run Anti-Virus Software and ensure you always have the latest definition file updates from the software vendor. If you are not sure if your business computer is protected by an anti-virus and firewall system you should contact your IT Help Desk to verify you are protected before connecting to the Internet.

An important point to remember for good personal computer security is to never change any settings within your business computer BIOS (see Glossary for description), the operating system, or any applications (this includes personal firewalls and anti-virus utilities) and never enter unfamiliar commands or run programs at the request of any person unless you can positively verify their identity as a current IT Group employee.

Last but maybe most important, always be prepared for the unexpected. Make sure you regularly backup critical data on your local hard drives and record your critical configuration settings either to a corporate network drive or a CD-ROM on a routine basis. The more often you use your computer the more frequent you will want to backup critical data on your computer hard drives. If ever a disaster occurs such as a hacker breaking into your computer and deletes or changes your data you will be prepared to quickly restore your system back to its original state.

Portable Computers

Portable computers, laptops, handhelds and PDA's are most vulnerable to being stolen. According to Gartner analyst John Girard, the most common places for laptop thefts are airport security checkpoints, ticket counters, hotel restrooms, meeting rooms, and registration lines.[4] Are you aware that most PDA's power on by default with no security? You should practice all the security items listed above for stationary personal computers plus the following. To prevent your portable computer from being stolen use a security cable to "tie down" the computer to a desk or other heavy object. You can also install an alarm system with motion detectors that will sound if someone tries to move your portable computer and / or case. There are also "locking plates" for portable systems that will remain in one primary location. Another helpful security item is software solutions that will cause stolen portable computers to "call home" when connected to the Internet and GPS

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

devices that will allow you to track the computer's current location. Another good security step to take, especially for portable computers, is to implement startup security options that will prevent your computer from booting into the operating system unless a pass phrase is entered or unless a specific floppy disk is in the drive. If you are running a Microsoft operating system consider using Microsoft's Syskey utility to manage your startup security options.

Never leave your portable computer unattended, even briefly, in any public place. If you leave your computer in your car, make sure to always keep your car locked and store your computer out of site under a rear pull-cover or in the trunk. Don't leave your computer bag lying visible in the seat. This is only an open invitation for any would be amateur thief. If you must leave your portable computer in your hotel room, secure it to an immovable piece of furniture with a cable lock as mentioned above or store it away in a locked suitcase. Does your briefcase / portable computer case scream "computer inside!"? Your portable computer is more secure when stored in a regular briefcase specifically padded internally to fit your device. It's also a good idea to avoid using any storage / carry cases that include a computer manufacturer's label on the outside. On the computer case and the portable computer itself use tamper-resistant tags or directly engrave identifying information like your company and personal name and contact information.

Finally, don't store any associated security devices in the same carry bag as your computer, such as a secure ID Key-Fob / Token. If your computer bag is ever stolen it makes it far too easy for the thief to hack into your computer and your organizations network. Treat your secure ID Key-Fob / Token the same way you treat your credit cards. Always keep your secure ID Key-Fob / Token with you personally or store it in a secure location separate from your computer.

Telephone Voicemail

An often overlooked area of personal security best practice is telephone voicemail. How secure is the access to your personal voicemail? Are you currently using a strong password to protect your voicemail or is your voicemail password one that is easy to guess after just a few tries? During the initial stages of attempting to merge Hewlett Packard and Compaq an intruder obtained access to the voicemail of HP's CEO and then leaked the controversial information to the press.[5] Phone "Phreaking" is a term used when an intruder tries to break into your voicemail box. To make it difficult for phone "phreaks" to obtain access to your voicemail follow the Password best practices listed in the section above. Do not set your voicemail password to the same number as your phone extension or any other common personal information others might think you could use. Also, change your voicemail password often, at least every three months.

Wireless Computing

While wireless computing offers increased flexibility and mobility, there is also more risk. You might enjoy working on your laptop computer from your favorite easy chair or a grassy spot on your lawn or a picnic table on a nice day outside. The problem is, intruders and would-be hackers could potentially access your wireless network from a car parked across the street or from a house three doors down.

Because wireless communication is broadcast over radio waves, eavesdroppers who merely listen to the airwaves can easily pick up unencrypted messages. Wireless network data travels over radio waves that cannot be constrained by the walls of most buildings.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The theft of an authorized user's identity poses one of the greatest risks. You must take specific steps to ensure proper wireless security to protect both your organizations data and yourself.

Wireless access points are widely sold and implemented with **NO** security. Incorrectly configured access points create a significant hole in network security. Today, most wireless access points are initially configured to communicate openly. For example: Most wireless PC cards sold today have a default setting of "ANY" which allows all open networks within range of the PC to respond and associate with the strongest signal regardless of who it is. In contrast, closed networks require the exact Service Set ID (SSID) to be entered in the PC configuration settings and only wireless access points with the same SSID will be able to talk to each other.

If you have a wireless network at home and you have the required technical skills, we strongly recommend you configure your home wireless access point to the security best practices listed below. This is of particular importance if you connect your business computer to your personal home wireless network. You should always check with your IT Help Desk to make sure you understand your organizations current policy and procedure before connecting your business computer to another network.

Wireless Configuration

1. Enable encryption and use a key of at least 128 bits.
2. Change your default access point SSID name to something unique making sure that the new name does not identify who, what or where you are.
3. Disable SSID broadcasting.
4. Change the access point's administrator password
5. Make sure your administrator password is at least 8 characters long and includes a mix of upper and lower case letters and non-alphabetic characters.
6. If you enable DHCP, limit the number of DHCP Users to the number of wireless computers you will be using.
7. For Authentication type select "Shared Key" rather than "Open System".
8. If your access point has an SNMP feature, disable it.
9. If your access point allows you to select between using a "Short Preamble" or "Long Preamble", select "Short Preamble". A long preamble could make it easier for an intruder to gain entry into your network.
10. Disable Remote Management.
11. Disable Remote Upgrade.
12. Check the access point manufacturer's web site at least once a month for firmware updates and apply accordingly.
13. Installation of a personal firewall and anti-virus software are very strongly recommended on all wireless enabled computers.

NOTE: Unauthorized wireless access points are not to be connected to an organizations network. Most corporate policy and standards prohibit access to organizations networks via unsecured wireless communication mechanisms. To summarize, it is best practice that only I.T. accepted wireless systems that meet specific criteria are approved for connectivity to an organizations networks.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

SUMMARY

Who is responsible for security at your organization? You are! The protection of your organizations assets is everyone's responsibility. Every one of us must take personal responsibility for the security of the information we own, provide, and work with.

Who can you share your password with? No one – your password is your own. Information on your computer is often only as safe as the strength of your password. We must use passwords that are "long and strong" so they will be difficult to guess – not something someone would associate to who we are or what we do. We must never share our passwords with anyone and never display our passwords in our work area.

We must take it upon ourselves to understand the sensitivity of the information we work with. We must store and transport our information according to its sensitivity, using more secure methods for more sensitive information. For example, emails and attachments not intended for public viewing should be encrypted prior to sending to an Internet address.

It is important to install anti-virus and firewall software to protect our personal computers from outside threats. Another way we can protect ourselves is to make sure that our personal computer software is always kept up to date with the latest upgrades and patch releases from the manufacturer. And to be prepared for the unexpected we should routinely take backups of our systems.

While our portable computers provide more flexibility and mobility they also present increased risk and responsibility. Never leave your portable computer unattended, even briefly, in any public place. If you leave your computer in your car, don't leave your computer bag lying visible in the seat. Make sure to always keep your portable computer locked up out of site under a rear pull-cover or in the trunk.

Like portable computers, wireless computing also offers more flexibility and mobility along with increased risk and responsibility. To keep intruders and would be hackers from accessing your wireless network be sure to change your access point default configuration and require authentication and encryption. Also, don't forget to change the access point administrators password often and disable any administrative remote functionality.

Asset's come in many different forms – tools, machines, technology and non-physical assets like information and ideas. We must always be aware of our surroundings and report any suspicious activity to our organizations security team and management. For any organization asset, if you think you've just discovered a breach in security or even if you just suspect that security may have been compromised: record the time of the event, record a description of the suspected security breach and contact your organizations security team and management right away. Always remember not to share the information with anyone else. Your organizations position of leadership depends on it.

Many information access thefts start when someone internal to the organization is fooled by a good story that is well presented. These "con jobs" are typically presented from a safe distance and often at the other end of a phone call. They may represent themselves as fellow employees, relatives of fellow employees, subcontractor employees, consultants, and suppliers. These con artists are clever at making their story or request seem believable or normal. They work invisibly at conferences, airports, hotel lobbies and other such public places along with using phones relentlessly trying to trick people into

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

disclosing useful bits of information that can be pieced together into something important. The more "bits and pieces" they learn, the easier it is for them to infiltrate a secure system. In public places, always be on guard to prevent your conversations, your phone calls, your ATM transactions or your personal computer screen from revealing clues to your identity, your business affairs, or your system access.

After reading this paper we trust we have raised your level of awareness and your sense of responsibility towards information security. This paper has provided you with essential security best practices that will enable you to be most effective in protecting your organizations critical information. Information Security's weakest link is people. You do not have to be a weak link. Take advantage of your new understandings as you are now well prepared to take a proactive role in protecting intellectual assets from falling into the wrong hands.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

BIBLIOGRAPHY

[1]Jackson, William. "Experts repeat: Security is a people—not technology—problem." Government Computer News. March 18, 2003.
URL: http://www.govexec.com/dailyfed/0303/031803td2.htm

[2] Kevin Mitnick & William Simon. "The Art of Deception." Whey Publishing Inc.2002

[3] What is Spam? URL: http://spam.abuse.net/

[4] Tech Republic - CNET Networks Inc,
"IT Support Best Practices Compilation" December 11, 2002 pg 15
URL:
http://www.techrepublic.com/download_now.jhtml?url=ftp%3A%2F%2Fftp.techrepublic.com%2Fsupport%2Farticle_comp%2Fr00320021211det01.zip&id=r00320021211det01.htm&title=IT+Support+best+practices+compilation

[5] The Washington Times, "H-P CEO's merger comments surface" April 10, 2002
News World Communications, Inc
URL: http://www.washtimes.com/upi-breaking/10042002-070323-8042r.htm

Additional references…

Email

URL: http://searchnetworking.techtarget.com/tip/1,289483,sid7_gci866113,00.html

Glossary
URL: http://www.onelook.com/
URL: http://foldoc.doc.ic.ac.uk
URL: http://www.webopedia.com/

Passwords
Edward Hurley, "Employees willing to share passwords with strangers" April 24, 2003
SearchSecurity.com URL:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci895483,00.html

Personal Computer
"7 Steps to Help Protect Personal Computing Security" April 2, 2002 Microsoft Corporation
URL: http://www.microsoft.com/security/articles/steps_default.asp

Portable Computer
URL: http://www.labmice.net/articles/laptopsecurity.htm

Spam
Information Week, "Ten Ways To Get Spammed" May 21, 2003 by TechWeb News
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=10000422

Wireless
Jim Rendon, "Wireless LAN doesn't mean worriless LAN" April 15, 2003,
SearchMobileComputing.com URL:
http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci893380,00.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

APPENDIX – A TEN WAYS TO GET SPAMMED

InformationWeek - Ten Ways To Get Spammed

By TechWeb News - May 21, 2003

E-mail protection vendor FrontBridge offers its top 10 list of ways spammers find victims

How E-mail addresses attract spam shouldn't be news to IT and security administrators, but company workers often need reminders. In that vein, FrontBridge, an E-mail protection vendor, released its top 10 list of ways spammers find people.

Based on its evaluation of hundreds of millions of messages, FrontBridge distilled the characteristics of filtered spam to identify how spammers obtain, or in some cases, guess, Email addresses.

* Put an E-mail address on a high-traffic Web site
* Post (or reply to a post) on UseNet
* Post (or reply to a post) on a public Web-based discussion group
* Register the address with a Web site that goes out of business and sells its list
* Register the address with a Web site that sells its list
* Subscribe to a porn site with the address
* Reply to an opt-out E-mail or click on an opt-out link in a message
* Use an address with a common name that can be easily guessed. Eg. Bob@Company.com
* Register a domain name
* Post an E-mail address in a chat room

Reminding employees of these bad habits, said FrontBridge, will reduce the risk of having workers inundated by spam.

http://www.informationweek.com/story/showArticle.jhtml?articleID=10000422

========

Editor's Note: It is most likely impossible for you to avoid all of the "bad habits" listed above but the fewer you practice the less chance you may have of overloading your Email Inbox with Spam.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

APPENDIX – B YOUR PERSONAL CHECKLIST FOR ESSENTIAL SECURITY

Social Engineering

1. Be careful that your desire to be helpful in performing everyday tasks does not lead to giving away confidential details to the wrong person about your organizations business.
2. Don't fall into the trap of trusting a person until they prove to be untrustworthy.
3. Be suspicious if you get a request from someone asking you to fax or email information to them right away, but refuses to provide you a direct callback number.
4. Don't be intimidated into giving out information to an irate caller, or one who seems to know the structure of your organization.
5. Watch out for the "odd" request or when a caller asks for information that seems a bit out of the ordinary.
6. Be careful not to cut corners by writing down passwords or leaving confidential material lying around. Securely store confidential material.
7. If you are throwing confidential material away, shred it first.
8. If you print something or have something faxed to you that is sensitive, pick it up right away and store it securely.

Sharing Information

1. Verify positive identity of requestor before providing any confidential information.
2. Verify requestors need to know.
3. Never disclose Level – 4 Restricted Information such as your password to anyone for any reason.
4. Always be aware of how sensitive the information is that you are working with.

Electronic storage and transfer of information

1. Determine your data sensitivity.
2. Always take a "default deny" stance in providing access to information.
3. Assign security permissions to a role or group rather than to an individual.
4. Only provide the minimum level of access necessary to meet specific business requirements.
5. Remove or disable all unused access IDs and privileges on a regular basis.
6. Log and monitor access of sensitive information and notify your management and IT Security of any noticeable misuse.
7. Classify data you own according to your organizations Information Sensitivity Model.
8. Keep classified data partitioned by as many levels of technology separation as practically possible.
9. Encrypt the transmission of Level–2 Internal and Level–3 Confidential information when sending to an Internet address.
10. Encrypt Level–3 Confidential information when stored in the DMZ or on the Internet.
11. Choose to store important and confidential information on a company network drive.
12. Backup your local hard drive on a regular basis.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

APPENDIX – B (CONT.) YOUR PERSONAL CHECK-LIST FOR ESSENTIAL SECURITY

Passwords

1. Do not use family names, nicknames, anniversaries, birthdays, pet names, sports teams or any such items that others would associate you with.
2. Do not use the word "password" for any of your personal password selections.
3. Select a password that is long and strong and a non-dictionary word.
4. Use a minimum of 8 characters using both upper and lower case letters, and a mix of numbers and special characters or symbols.
5. To help you remember your password use the first letter's of each word in a phrase that means something to you. One way to do this is to create a password based on a song title, affirmation, or other phrase.
6. Never change your password to something known to anyone else, not even for a moment.
7. Keeping your password to yourself is critical to your company's security. Never share your password with anyone – including your manager, IT Security, IT Help Desk, family, friends or co-workers.
8. Never use the same password for both your work and personal accounts.

Email

1. Always encrypt sensitive Email and attachments destined to an Internet address.
2. Always delete unrecognized Email. Never open or respond to any Email or attachment unless you positively recognize or trust the sender. This includes spam (junk Email).

Personal Computers

1. Only install software from trusted sources.
2. Keep all your PC software versions up to date with the most current patches and fixes.
3. Install Antivirus and Firewall software.
4. Never change any settings within your business computer BIOS, the operating system, or any applications (this includes personal firewalls and anti-virus utilities)
5. Never enter unfamiliar commands or run programs at the request of any person unless you can positively verify their identity as a current IT Group employee.
6. Regularly backup critical data on your local hard drives and record your critical configuration settings either to a corporate network drive or a CD-ROM on a routine basis.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

APPENDIX – B (CONT.) YOUR PERSONAL CHECK-LIST FOR ESSENTIAL SECURITY

Portable Computers

1. When you leave your portable computer unattended use a security cable to "tie down" your portable computer to a desk or other heavy object.
2. Consider software solutions that will cause stolen portable computers to "call home" when connected to the Internet and GPS devices that will allow you to track your portable computer's current location.
3. Implement startup security options that will prevent your portable computer from booting into the operating system unless a pass phrase is entered or unless a specific floppy disk is in the drive.
4. Never leave your portable computer unattended, even briefly, in any public place.
5. If you leave your computer in your car, make sure to always keep your car locked and store your computer out of site under a rear pull-cover or in the trunk.
6. Avoid using any storage / carry cases that include a manufacturer's label on the outside and scream I have a computer inside.
7. On the computer case and the portable computer itself use tamper-resistant tags or directly engrave identifying information like your company and personal name and contact information.
8. Never store associated security devices in the same location as your computer. For example, Secure ID Key-Fob / Tokens should never be stored near your desk or in your carry bag next to your computer. Always keep your security devices with you personally or store them in a secure location separate from your computer.

Telephone Voicemail

1. Do not set your voicemail password to the same number as your phone extension or any other common personal information others might think you could use.
2. It's best to change your voicemail password often, at least every three months, especially if you think you may receive sensitive messages.
3. Follow the Password best practices listed above.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

APPENDIX – B (CONT.) YOUR PERSONAL CHECK-LIST FOR ESSENTIAL SECURITY

Wireless Computing

1. Always check with your IT Help Desk to make sure you understand your organizations current policy and procedure before connecting your business computer to another network.
2. Never connect a personal access point, router or bridge to your organizations network.
3. Change your home Access Point / Router / NIC default configurations
   a) Enable encryption and use a key of at least 128 bits.
   b) Change your default access point SSID name to something unique making sure that the new name does not identify who, what or where you are.
   c) Disable SSID broadcasting.
   d) Change the access point's administrator password
   e) Make sure your administrator password is at least 8 characters long and includes a mix of upper and lower case letters and non-alphabetic characters.
   f) If you enable DHCP, limit the number of DHCP Users to the number of wireless computers you will be using.
   g) For Authentication type select “Shared Key” rather than “Open System”.
   h) If your access point has an SNMP feature, disable it.
   i) If your access point allows you to select between using a “Short Preamble” or “Long Preamble”, select “Short Preamble”. A long preamble could make it easier for an intruder to gain entry into your network.
   j) Disable Remote Management.
   k) Disable Remote Upgrade.
   l) Check the access point manufacturer’s web site at least once a month for firmware updates and apply accordingly.
   m) Installation of a personal firewall and anti-virus software should be used on all wireless enabled computers.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

GLOSSARY

AES – Advanced Encryption Standard

Description: A symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its preferred encryption technique in October 2000, replacing the DES encryption it used to use.

Anti-Virus software

Description: A software system installed on your PC designed to prevent a program or piece of code from loading on your computer without your knowledge and running against your wishes. Viruses, Trojans and Worms can be annoying or destructive. Some code will allow hackers to gather your personal data or take control of your machine. Trend Micro Inc. OfficeScan is one popular virus software package that also includes a personal firewall.

AP – Access Point

Description: In wireless networks an access point is a device used to connect and transfer data between wired and wireless devices, similar to the base unit of a cordless phone. Often access points are used to allow mobile devices to connect to a home-based network and provide access to the Internet.

BIOS - basic input/output system

Description: The BIOS is built-in software on a chip that determines what low level functions a computer can perform. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions. BIOS instructions are read each time you power on your computer.

DHCP - Dynamic Host Configuration Protocol

Description: A protocol that provides a means to dynamically allocate IP addresses to computers on a local area network. The system administrator assigns a range of IP addresses to DHCP and each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server. The request and grant process uses a lease concept with a controllable time period.

Firewall

Description: A system designed to prevent unauthorized access to or from a network or individual computer. Firewalls can be implemented in both hardware and software or a combination of both. A firewall examines the data flow and blocks data that does not meet specified security criteria.

GPS - Global Positioning System

Description: A system for determining your position / location on the Earth's surface by comparing radio signals from several satellites. When the system is completed it will consist of 24 satellites equipped with radio transmitters and atomic clocks. Depending on your geographic location, the GPS receiver samples data from up to six satellites, it then calculates the time taken for each satellite signal to reach the GPS receiver, and from the difference in time of reception, determines your location.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

GLOSSARY (cont.)

Hacker

Description: In the context of this document, a hacker is any individual who gains unauthorized access to a computer system for the purpose of stealing or corrupting data.

PDA - Personal Digital Assistant

Description: A small hand-held computer typically providing calendar, contacts, and note-taking applications but may include other applications, for example a web browser and media player. Small keyboards and pen-based input systems are most commonly used for user input.

Personal Firewall

Description: A software system installed on your PC designed to prevent unauthorized access. All data entering or leaving your PC passes through the firewall, which examines all data and blocks data that does not meet specific security criteria.

SNMP – Simple Network Management Protocol

Description: A set of protocols for managing complex networks.

Social Engineering

Description: attacking or penetrating a system by tricking or subverting operators or users, rather than by means of a technical attack. More generally, the use of fraud, spoofing, or other social or psychological measures to get legitimate users to break security policy.

SPAM

Description: Commercial Email advertising for various products sent to a mailing list or newsgroup. Spam often wastes people's time with unsolicited Email and consumes a lot of unnecessary network resources.

SSID - Service Set ID (identification)

Description: A unique name given to a wireless network that may consist of one or more access points. Each access point and wireless participant must be assigned the same SSID.

Trojan

Description: A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojans is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

Virus

Description: A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. All computer viruses are manmade and are capable of replicating themselves. A virus can quickly use all your available memory and bring your computer system to a halt. A virus is also capable of transmitting itself across networks and bypassing security systems.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

GLOSSARY (cont.)

WEP – Wired Equivalent Privacy

Description: Encryption used to provide a secure method of communication between wireless network participants. WEP is designed to provide the same level of security as that of a wired network.

Wireless Device

Description: A computing device that uses radio signals instead of wires to transmit network data. Wireless hardware is available for many different computing devices, including personal desktop computers, notebooks or laptops, Palm or iPaq PDAs, and many others.

Worm

Description: A worm is a special type of virus program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the computer system down. A worm does not attach itself to other programs.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

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

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced