Information Security in the Workplace: What Every User Should Know

By
Melissa J. Dark, Ph.D.,
Assistant Professor &
Assistant Director for Educational Programs

CERIAS
Center for Education and Research in Information Assurance and Security

URL of this document (click the link to reach the document)**:**

http://www.cerias.purdue.edu/training_and_awareness/downloads/information_security_workplace_preview.pdf

Information Security in the Workplace: What Every User Should Know ©

Published by: CERIAS, The Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, Indiana.

Table of Contents

Introduction

Course Goals

The purpose of this security awareness course is to promote:

- Understanding of the value of information security.
- Understanding of the responsibility to protect the organization's assets.
- Ability to recognize potential security risks and violations.
- Understanding of practices that promote computer security.
- Knowledge about whom to contact if you detect a security breach.

Course Objectives

Upon completion of this course, you will be able to:

- Identify the value of information to your organization and more specifically your department.
- Outline a responsibility tree that indicates responsibilities of various persons within your work group for protecting organizational assets.
- Describe common security risks and violations for computer users in the workplace.
- Describe the importance of password protection and techniques for creating strong passwords.
- Describe the importance of physical security and techniques for improving physical security in your work area.
- Describe social engineering risks and techniques for thwarting social engineering attacks.
- Describe email security risks and techniques for using email more securely.
- Describe the role of proper use.
- Identify whom to contact in the case of a security breach in your workplace.

Section 1: Understanding the Value of Information Security

Did You Know…

"The goal is to ensure that everyone understands that protecting the enterprise is part of each person's job."

-Kabay, Mich. "The Internet Changes Everything – Especially Security." Network World White Paper. Mar '01:16.

"Everyone is familiar with the old adage "knowledge is power". This saying has taken on new meaning in the information technology world. Why? Because with new information technology systems, **more** information is **more** readily available to **more** people. Information security has always been a concern, but the concern has been considerably heightened due to the advent of IT systems.

Computing and communications technology used to reside on stand alone mainframes housed in the computing center. Therefore, security was the responsibility of the computing manager and staff. Today, computing and communications technology are distributed systems with terminals in individual offices and homes. As the systems themselves have become more dispersed, so too has the responsibility for security. Furthermore, many IT systems and products have been designed with ease of use and accessibility as primary functional requirements. You and I, as end users, think that is a good thing. However, from a security perspective, security can decrease as ease of use and accessibility increase. The aim of all information security is to create the **appropriate** balance between ease of use and security.

Did You Know…

"U.S. colleges and universities are ranked among the poorest protected systems because tightening security often means restricting access."

-Walsh, Lawrence. "Blocking Napster Isn't Elementary." Information Security.

So how does an organization strike the appropriate balance? The answer to this question varies from organization to organization, department to department, and person to person. The appropriate balance depends upon the need for confidentiality, integrity, and availability.

Confidentiality – how important is it that this information be protected so that unauthorized persons cannot access it?

Integrity – how important is it that this information be protected from intentional or accidental unauthorized changes?

Availability – how important is it that this information system be accessible by authorized users whenever needed?

On the following page there is an exercise for you to complete. In the space provided, give examples of types of information present in your workplace that must be kept confidential and potential consequences if it is not kept confidential. Then do the same thing for information integrity and availability.

Did You Know…

"The value of information, especially on original research, will eventually compel academic institutions to harden their defenses. 'All it will take is a few well-publicized incidents of intellectual property theft to get the universities to lockdown their networks.' "

-Walsh, Lawrence. "Blocking Napster Isn't Elementary." Information Security. Feb '01: 45.

Exercise #1: The Value of Information and Information Security in Your Workplace

Directions: give examples of types of information present in your workplace that must be kept confidential and potential consequences if it is not kept confidential. Then do the same thing for information integrity and availability.

	Types of Information that Must Be Secure	Potential Consequences of Poor Security Practices
Confidentiality		
Integrity		
Availability		

Section 2: Protecting the Organization's Assets

Did You Know…

"We find that many problems arise from people: human errors or actual internal threats."

-DeJesus, Edmund. "Managing Managed Security." Information Security. Jan '01: 45.

There is no recipe that any organization can follow to protect its assets…..it requires a combination of well-created policies that are fully implemented. The policies and practices in place in any organization should be commensurate with the value of the information that must be protected and the impact of the failure to protect it adequately, as discussed in the exercise at the end of section 1.

Policies for information security should be derived not only from the information security needs of the organization and its users, but also from information security laws and regulations. Furthermore, it should be designed based on the information security needs of the various functions (departments, programs, sections, classifications, etc.) within the organization.

An effective information security policy is explicit, well thought out, comprehensive, fully implemented, evaluated regularly, and revised as needed. The following components are commonly found in information security policy and presented here to show you the big picture and specifically where user practices fit into the bigger scheme of information security policy.

Did You Know…

"Without a good security policy, the best tools in the world will have little impact on the environment."

-Henderson, Frank. "Follow the (Smart) Money." Network World White Paper. Mar '01: 6.

1. Policy on Physical Controls, i.e., back up files and documentation, fences, security guards, badge systems, double door systems, locks and keys, biometric access controls, site selection, fire extinguishers, etc.

2. Policy on Technical Controls, i.e., access control software, anti-virus software, passwords, smart cards, encryption, audit trails, intrusion detection systems, etc.

3. Policy on Administrative Controls, i.e., security awareness and technical training, separation of duties, user registration, disaster recovery, contingency, and emergency plans, etc.

Note that security awareness and training is one initiative/program that is part of the larger policy undertaken to protect the organization assets. This training is one component of the security awareness and training program, which is part of administrative controls, which is part of information security policy as shown in figure 1.

Did You Know…

"Most companies have enough to do just taking care of their own business, never mind thinking about security."

- DeJesus, Edmund. "Managing Managed Security." Information Security. Jan '01:45.

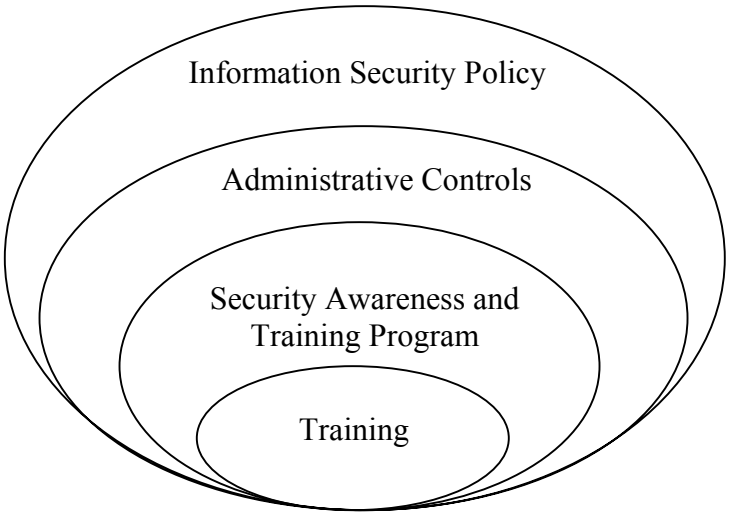
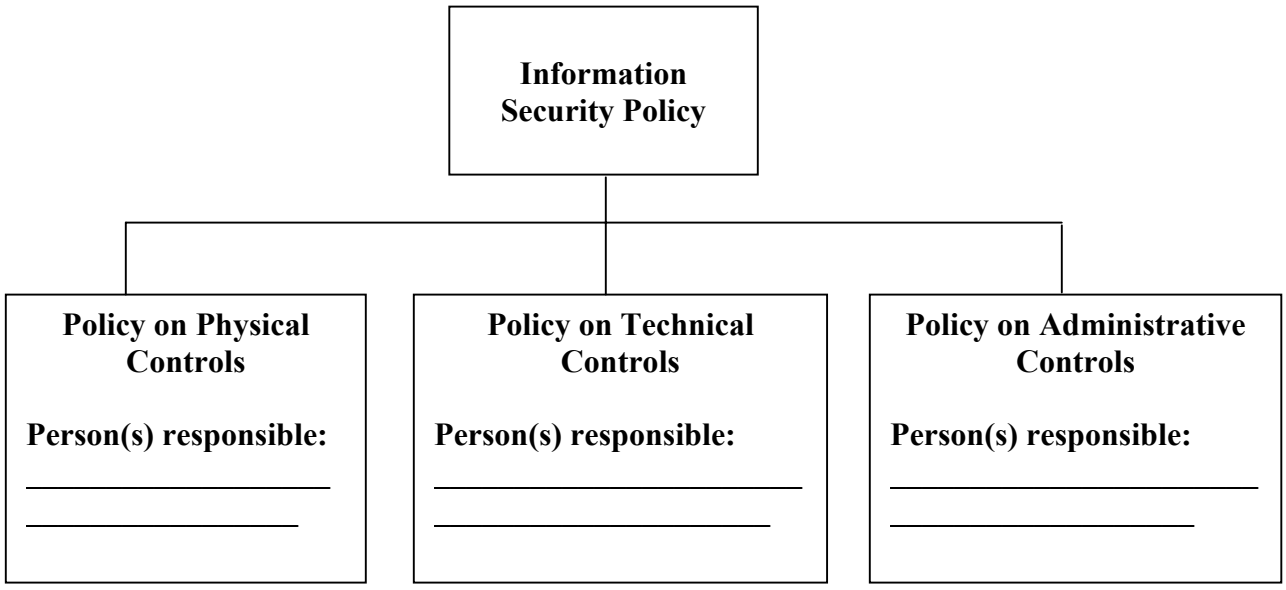


Figure 1. Elements of information security policy.

Exercise #2: Information Security Responsibility Chart

Directions: This is a two-part exercise. In part one, you need to draw and complete the chart to show the information security responsibilities of various persons in your organization. In part two, you need to specify who in your workgroup is responsible for protecting the assets that you identified in exercise #1. There is no penalty for leaving spaces blank.

Part 1



Part 2

Go back to exercise #1. For each type of information that you indicated must be secure, list all of the people in your organization who are responsible for protecting each asset.

Asset/type of information that must be secure.	List of all persons responsible for keeping it secure.

Section 3: Security Risks and Countermeasures

This section will cover the following 5 security threats common to computer users in the workplace:

- Passwords
- Physical Security
- Social Engineering
- Email
- Untrusted Software

After discussing each type of threat, you will be introduced to countermeasures that you can take to reduce your risk.

Section 3A: Password Basics

Did You Know…

"One-quarter of respondents to the 2000 Information Security Industry Survey reported breaches from attacks using insecure passwords."

-Bertin, Michael. "The New Security Threats." Smart Business for the New Economy. Feb '01:81.

Why Worry About Passwords?

Passwords are often used to grant access to computer systems to approved parties. Likewise, passwords are often used as the first line of defense against unauthorized access. In the case of passwords, access is granted according to what you know, i.e., the password.

The fact is that users, for their own convenience, often pick passwords that are simple and easy to remember. Most users would like to pick one password, and 1) use it for all of their accounts, 2) use it all the time, 3) never have to change it, and 4) write it down so that they can reference it if they happen to forget it during vacation.

The problem is if the password is easy to remember, it is easy to guess. If the password is written down, guessing doesn't even matter. And if the password is never changed, then repeated attacks are more likely to occur.

Many people also think it is inconvenient to have a timeout feature on their computer. Timeout features lock your account so that when you are away from your desk, other unidentified users cannot access your computer.

Passwords versus Pass Codes

Unfortunately, when the term password is used, it connotates exactly that with user, the notion of using a word to enabling passing the barrier to enter the system. Rather than think in terms of passwords, we prefer to think in terms of pass codes.

A code is a system of signals used to represent letters or numbers in transmitting messages. To create your own code, you might want to consider creating a pass phrase. A pass phrase is sort of like a personal algorithm. The phrase makes it easy for you to remember, but hard for someone else to guess.

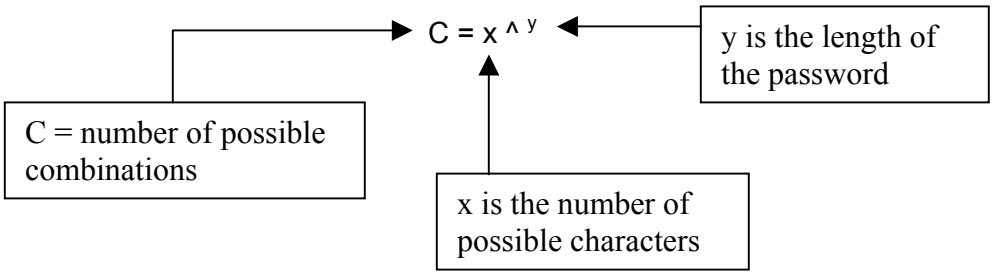
For example: m+j=3rke This password represents the names of the people in my family. Melissa is my name, Jay is my husband, and we have three children, Rachel, Kate, and Erin.

2niletak This is one of my childrens' names (Katelin) spelled backwards and she is the second of three children in our family, hence the 2.

Password Length and Possible Characters

The strength of your password is dependent upon the length of and the number of possible characters used in your password.

The formula for calculating the total possible number and letter combinations is:



So if you are using numbers, you have the characters 0-9 as possible characters or 10 possible characters. If the password length is 4 characters, then the number of possible combinations is $C = 10^4$ or 10,000.

If you increase the possible characters to include numbers and all letters of the alphabet, then you have increased the number of possible characters to 36. For a password that is 4 characters long using 36 possible characters, the number of possible combinations is $C = 36^4$ or 1,679,616.

If you increase the possible characters to include numbers, all letters, and special characters (i.e., !, @, #, $, %, ^, &, *, and so on), then you have increased the number of possible characters to 68. For a password that is 6 characters long using 68 possible characters, the number of possible combinations is $C = 68^6$ or 98,867,482,624 (more than 98 trillion)!

Password Protection Fundamentals

The following are ten tips to help you select a password that is more secure, yet still relatively easy for you to remember.

1. Use a minimum of 6 characters.

2. Use a combination of numbers (1-9), alphanumeric characters (A-Z), and special characters (!, @, #, $, %, ^, &,*,+,=).

   Try this on for size: Get>Sm@rt

   If it is hard for you to remember special characters, create a common substitute that makes sense to you. For example, use $ as a substitute for s or S. Or use + as a substitute for t or T.

   So instead of Get>Sm@rt, the password could be Ge+>$mar+

3. Don't pick a password that someone can easily guess. What types of things are easy to guess? Here's a list of things that we advise you not use because they are easy to guess.

   - Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
   - Don't use your first or last name in any form.
   - Don't use your spouse's or child's name.
   - Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
   - Don't use a password of all digits, or all of the same letter. This significantly decreases the search time for a cracker.
   - Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.

4. Use a pass phrase. A pass phrase is sort of like a personal algorithm. The phrase makes it easy for you to remember, but hard for someone else to guess.

   For example: The title of the song I Left My Heart in San Fransisco is a phrase that could be represented as the following password: EYELMHISF

   If you like the idea of using personal information in a pass phrase, consider the following passwords:

5. Use a separate password for different accounts. I know this makes it tough to remember multiple passwords. Try associating the password with the account. If you have an account to purchase books on line, use a pass phrase that is derived from a book title.

   For example: Using the book title The Seven Habits of Highly Effective People could result in the following password: 7Hof^EP!

6. Do not write down your password and leave it in an easy to view spot. There isn't much else to say here…..just don't do it.

7. Change your password regularly. There is a temptation to recycle old passwords. You have two and you flip flop their use. Resist the temptation….it is too predictable.

8. Do not give other people your password, intentionally or unintentionally. While it might seem efficient to give your colleague your password so s/he can get a file off of your computer, who is to say that they will not write it down somewhere for ease of remembering. You also want to make sure that it is difficult for others to see you type in your password.

9. Use the timeout feature to prohibit access when you are away from your desk.

10. Report any suspicious or abnormal circumstances to your system administrator as soon as you notice it.

Exercise #3: Passwords, Passwords, Passwords

Directions: Using the guidelines provided, brainstorm and write down ten passwords that would be easy for you to remember, but hard for someone else to guess or crack. If you have multiple passwords that you have to use, try to create themes that you can use as well, but don't write down which password is for which account…….that wouldn't be very secure. Be prepared to share with the class.

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

Section 3B: Physical Security

Did You Know…

The FBI estimates that computer component theft is responsible for over $8 billion a year in losses to corporate America. Moreover, this number fails to take into account the invaluable loss of data and information that is stored onto these computers.

Houston Business Journal, August 18, 1998.

Did You Know…

- ✓ Experts say laptop theft is a big problem.
- ✓ 57 percent of firms suffered losses from laptop theft in 1999.
- ✓ Laptop theft is the second most prevalent security threat after virus attacks.
- ✓ Insurance industry estimates reveal that an estimated 319,000 laptops were stolen in the US last year.

CNN, September 20, 2000

Why Worry About Physical Security?

With all the hype about viruses, hackers, and crackers, accompanied by the availability of firewalls, vulnerability testing, and intrusion detection, the physical security of computer systems is often overlooked. Unfortunately, many people do not realize the importance of physical security until it is too late.

Most people believe that the data on the computer is the most important thing to protect, but imagine if you came into work one day, and booted up your computer only to find that it did nothing. A quick check shows that the power is fine, but the computer is completely dead. You report this incident to the system administrator. Upon investigation, you learn that someone entered the box of the computer and stole your hard drive. Suddenly, the data you have been protecting is gone…..and not even a password would have protected it in this situation.

So don't overlook the obvious. A skilled computer thief knows exactly what s/he is looking for and can make quick work of stealing hard drives, memory, CPU chips, and other components. While many of the required precautions for physical security are the responsibility of the system administrator, there are also basic physical security safeguards that every computer user should practice.

Physical Security Fundamentals

The following are six tips to help you create a physical work environment that is secure and protects your information assets.

1. Lock up – be sure to lock the facility when it is not being attended.

2. Do not leave resources unattended during the workday. Have you ever walked into an empty office in the middle of the day? I have… many times. Usually everyone has a legitimate reason to be away from their desk whether it is due to an immediate meeting with the boss, last minute copies for a presentation, a crisis down the hall that required help, or an urgent bathroom break. Preventing physical loss during these times requires two things:

   A) Awareness that you are at risk, and
   B) A willingness to work as a team and communicate to ensure that the office is not left unattended.

   Create a schedule for office coverage so that someone is in the office at all times. Then during times of emergency, be sure to communicate with others to let them know if you need to be away during your scheduled time.

3. Know whose responsibility it is to lock up. While this might seem overly simple, sometimes the simplest things are the easiest to overlook. The time when this becomes especially important is when the person who normally locks up goes on vacation, is sick or away from work for other reasons. Now all of the sudden, someone in the office has to fill in for the person who normally locks up. The person filling in is usually trying to do two jobs at once. And, considering the fact that we all get busy and used to our routine, it is easy to see how doors get left unlocked.

Did You Know…

"The cost of replacing the device is quite irrelevant in comparison to what the device holds."

-Armstrong, Illena. "Road Warriors Run Rampant." SC InfoSecurity Magazine.Jul '00:24.

4. Do not grant unauthorized people access to equipment. Many workplaces have become very reliant upon computer and information systems to conduct business. I know, firsthand, the frustration of lost productivity due to the computer system being down. It is easy to understand why we want our computer and information systems available for use ALL THE TIME. However, the need for constant availability sometimes can put the organization at risk.

   People who want access to your computer system know that businesses have become increasingly more reliant upon their computer systems. They also know that they can play on this reliance by posing as system auditors, certifiers, administrators, etc., to gain access. And lastly, they know how to create the proper identification to convince others that they are authorized to access the equipment. So it is also important that you know how to confirm 1) that an individual really does have authorization and 2) exactly what they have authorization to.

   This topic will be discussed in greater detail in Section 3: Social Engineering. The bottom line is this: Do not grant access to unauthorized persons and know where and how to confirm authorization.

5. If you are in an open area, request a security cable for your equipment. After all, it is harder to walk out with something that is tied down than something that's not!

6. <u>If you use a laptop, keep it close by at all times.</u> Consider the following story:

Did You Know…

"Laptop theft is a growing problem – one insurance company says that nearly 320,000 laptops valued at $800 million were stolen in 1999."

-Briney, Andy. "Alarmed." <u>Information Security</u>. Feb '01:8.

Case in Point

The personal portable computer of Dr. Irwin Jacobs, Qualcomm's chief executive officer disappeared from a hotel conference room moments after Dr. Jacobs addressed a national business journalists' meeting. Qualcomm is a leader in developing, delivering, and enabling innovative digital wireless communications products and services. The laptop contained proprietary information that could be valuable to foreign governments. How did it happen? Dr. Jacobs left the computer unattended on a podium for about 15-20 minutes when he stepped down to talk to a small group of business Editors and Writers less than 30 feet away.

While you might not have proprietary information on your laptop, this story points out just how easy it is to steal laptops and how important it is to keep them close by.

Section 3C: Social Engineering

Did You Know…

"Kevin Mitnick, the well-known hacker that cost companies like NEC USA, Nokia, and Sun at least $290 million over a two-year span, sometimes didn't have to hack at all to defeat computer defenses. Using what's known as social engineering he was often able to get people to give him their passwords or whatever he needed to break in to a network."

-Bertin, Michael. "The New Security Threats." Smart Business for the New Economy. Feb '01:83.

Why Worry About Social Engineering?

To understand why it is important to worry about social engineering, you have to first understand what social engineering is in the world of Information Assurance and Security. Basically, social engineering is the art and science of getting people to comply with your wishes. The aim of many social engineers in the world of Computer and Information System Security is to trick people into revealing 1) passwords or other information that compromises a target system's security, 2) credit card numbers or other personal information that compromises the individual, or 3) to gain access to unauthorized areas where equipment is stored.

The fact is that all computer systems rely on humans. Humans turn on computers. Humans create passwords. Humans enter credit card numbers. Therefore, the human part of security is independent of platform, software, hardware, networks, and so on. This makes human beings a universal weakness in Information Assurance and Security. An individual experienced with social engineering techniques can practice this form of hacking wherever s/he goes.

Social engineering is performed in a variety of ways and you should be aware of all of them. The four predominant methods include: 1) over the phone, 2) via the Internet, 3) snail mail, and 4) in person. In addition, you should be aware of some of the psychological factors at play. Let's look at each of these in greater detail.

1. Telephone: The telephone is the most common means for social engineering. Why? Because it is easy, quick, and fairly cheap. Common scams include posing as the internal system administrator, the local phone company technical support, and so on. Consider the following true story:

Jack was a Computer Engineer with a masters degree. In December 1995 he got a phone call from Phillip Smith who identified himself as a customer service representative of New Mexico Internet Access.

Phillip started the conversation by saying "We're calling all of our customers to let you know that we have decided to start accepting credit card payments on your account." Jack reports thinking this was a great idea because New Mexico Internet Access had a terrible billing procedure. They did not use credit cards and they didn't send you a bill each month, not even by email. They relied upon the customer to remember to pay their access fee. If the customer failed to remember, the penalty was cancellation of their account. One day you try to dial up and "nada", nothing….no Internet access.

Now while this may sound strange to you, at the time no one thought much of it. This was the dawn of the commercial Internet, there were very few ISPs and people were just glad to have access.

Jack hesitated. Sensing his reluctance, Phillip added "Because this will guarantee and simplify billing, we will cut your monthly bill from $20.00 to $15.00, if you go to credit card payment".

That was all it took. Jack took the bait, hook, line, and sinker. The next month charges for computer games turned up on Jack's credit card statement. Not to mention that New Mexico Internet Access cancelled his account for lack of payment.

Social Engineering over the telephone often makes use of equipment. The following quote is from a website written by a social engineer who goes by the name Meinel. It reads as follows:

> "The phone should be of good quality and try to avoid cordless, unless you never get static on them. Some phones have these great buttons that make office noise in the background. Caller ID units are helpful if you pull off a scam using callback. Something else I use is a voice changer. It makes my voice sound deeper than James Earl Jones or as high as a woman. This is great if you can't change your voice very well and you don't want to sound like a kid. Being able to change gender can also be very helpful."

Did You Know…

"The IloveYou virus was the first to use the social aspects of viruses. Because of its friendly message, experts said, and the fact that it 'came from' a familiar person, the virus writers increased the odds a user would open the VBS payload."

-"Virus Authors Exploit Human Weakness." E-Week. Jun '00:20.

2. Internet: The Internet can also be a tool for social engineering. While many of the schemes on the Internet fall into the realm of hacking, when the means used to garner information on the net include scheming a person into divulging information, then it is still considered social engineering.

Common scams include posing as someone you are not via emails and chatrooms. The true example on the next page describes an email message sent to America Online customers that directed them to a copy cat website to collect user names, passwords, and credit card numbers.

Dear America Online Member,

We're sorry to bother you during the holiday season. However, with the change to the new millennium, thousands of hackers are taking advantage of the Y2K bug. America Online is taking a great amount of action and preparing for the worst. We need you to provide your current billing information by clicking <A HREF=http://verifybilling.cjb.net>here</A>. If you do not complete this form before you sign off today, your account will be suspended until you contact us directly with this information.

Sincerely,

Bill Fieldhouse, Billing Department,
Representative Identification # 103

3. Snail Mail: Regular U.S. mail service can also be an effective means for social engineering. It is effective for the person trying to get information because it is cheap and also because people tend to trust the written word.

A particularly effective way to get personal information is by simulating a sweepstakes. After all, it is hard to resist filling out a sweepstakes form.

The information that the social engineer is after might be your name and your Internet service provider, your name and your email service provider, etc. With that in hand, they are well positioned to call on you later and pose as the system administrator for your Internet Service provider. These scams can be elaborate, using more than one method to gain access to confidential information.

4. In Person: While it takes more time and effort for the hacker, sometimes social engineering must be done in person to get the needed information. People tend to trust people whom they can see. It is much easier to build a sense of trust in a person than it is via faceless communications. And most of us are trusting – it is human nature.

Because you can build a greater sense of trust in person, the goal of social engineering done this way is not just to gain access to a password, but to gain access to the entire system, i.e., the equipment room.

According to social engineers, a particularly effective method for in person social engineering is by posing as a trusted authority figure. For example, posing as the fire marshal, or as a security supervisor. Consider the following example:

A hacker posing as the fire marshal gains access to the public access areas including the company lunchroom. The local spa/exercise facility has an advertisement in the lunchroom. According to the ad, everyone who leaves a business card is eligible for one week of free membership to the spa, and one lucky winner will be chosen every month to receive three months of free membership. The hacker finds the jar full of business cards, sorts through them, and selects a few. S/he then takes them to a print shop, where business cards are made using a fake name and title.

Two months later the hacker returns to the company and announces her/himself to the receptionist……business card in hand. Assuming the card is legitimate, she issues the hacker a building pass.

Another mechanism for gaining access to confidential information is called dumpster diving. Discarded pieces of paper with passwords are among the many types of confidential information that can be found in the trash.

Psychological Ploys: An effective social engineer goes into every situation with a plan for how they are going to obtain the desired information.

While this is not an exhaustive list, the following psychological ploys are purposefully used by social engineers because of their effectiveness: 1) diffusion of responsibility, 2) ingratiation, 3) moral duty, and 4) conflict avoidance.

1. Diffusion of Responsibility: a social engineer will often look for ways to make the target perceive that they will not be responsible for their actions. Once relieved of personal responsibility, target's are much more likely to share information.

2. Ingratiation: social engineers know that compliance is more likely if the target believes that by complying they are ingratiating themselves with someone who may give them future benefits….basically getting in good with the boss.

3. Moral Duty: this is where the individual complies because they feel it is their moral duty. Sometimes this is conveyed as being able to feel a part of a greater good cause and sometimes it is a message of guilt for doing nothing.

4. Conflict Avoidance: this is where the target complies in order to avoid conflict. On the whole, people do not like conflict and will often take actions to avoid conflict and/or to resolve it.

Social Engineering Security Fundamentals

The following are six tips to help prevent you from becoming the target of a social engineering attack.

1. Realize that computer security is a part of everyone's job.

2. Awareness of social engineering. An effective and wise precaution against social engineering is knowing basic methods for social engineering, as presented in this manual.

3. Do not give out confidential information without verification.
   - Network administrators do not need to know your password. If you are ever asked for your password, it is probably a social engineering attack.
   - Do not share your userid and password with anyone.

4. Verification, verification, verification!
   - Verify that the person is who s/he says s/he is….on the phone and in person.
   - Verify that the business that the person says s/he is from is a real company.
   - Verify that the person actually works at that company.
   - Verify that the url matches the one you are familiar with.
   - Verify that the person is supposed to be working on the equipment.

5. Do not put confidential information in the trash without shredding it first.

6. Report any suspicious behavior to the system administrator immediately.

Exercise #4: Social Engineering Case Study

Directions: Read the following case study and questions. Be prepared to discuss the case study in a small group discussion. Assign one person in your group to be the recorder. The recorder should write down the answers to the questions that the group discusses to present to the class.

Three weeks ago Eastern College was hacked. The computer hacker posed as a system administrator for the school and called a clerk in the registrar's office. The conversation went something like this:

Hacker: "Hi, this is Daryl with tech support. We have had some folks in your office report slowdowns in logging in lately. Is this true?"
Clerk: "Yes, it has seemed slow lately."
Hacker: "Well, we have moved you to a new server, so your service should be much better. If you want to give me your password, I can check your service. Things should be better for you now."

Unfortunately, Daryl did not really work in tech support at Eastern College. Daryl hacked into the registrar's system, from there he found the bursar system. Eastern College had started accepting credit card payment two years earlier. Within four weeks, over 30% of the students and/or their parents reported that their credit card numbers had been stolen and used.

Questions:

1. What might be the consequences of this incident for Eastern College?

2. How easy would it be for something like this to happen in your place of work?

3. How would you propose preventing incidents like this from happening in the future?

Section 3D: Email Security

Why Worry about Email Security?

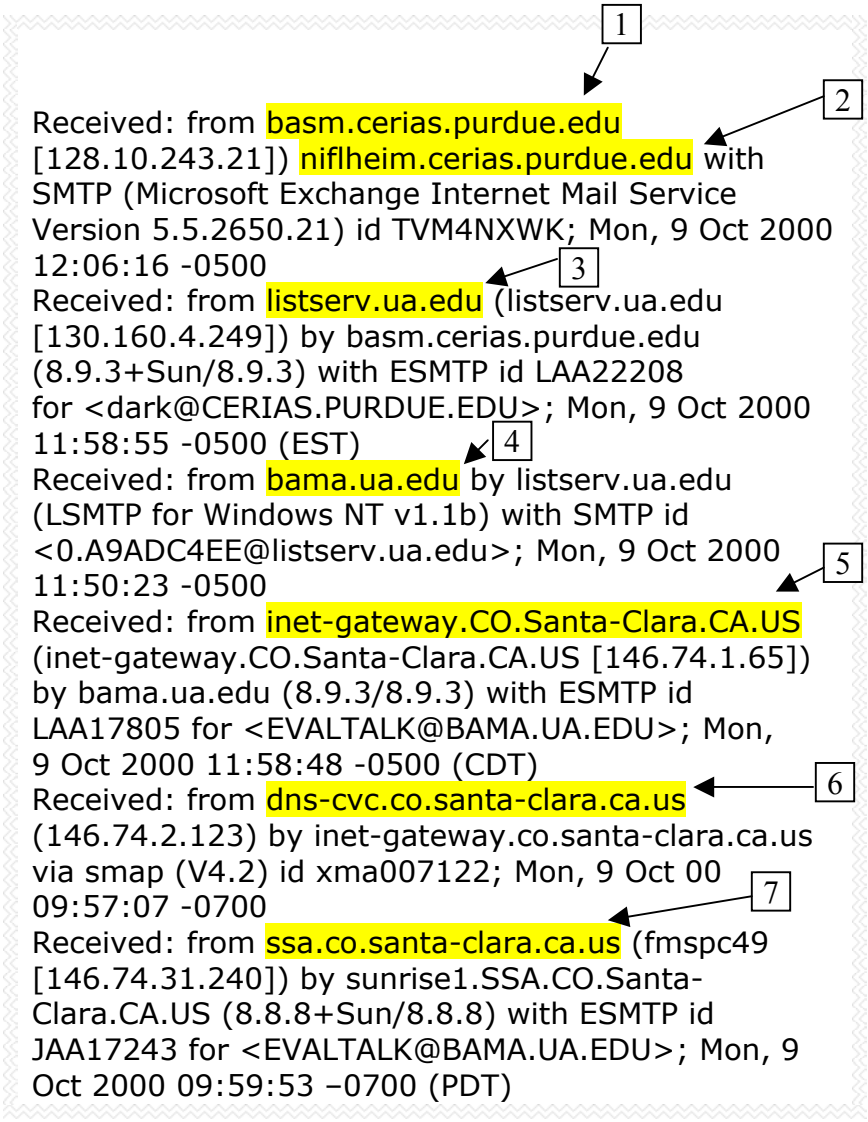
Email has been likened to postcards. Why? Because both email and postcards are easy to intercept. And if intercepted, both are easy to read, and/or change. By its very nature, all email is insecure. Furthermore, email costs little to nothing, so millions of people have it. For these reasons, email is an accessible method for exploitation.

You might think, "It's only email, why should I care?" There are several reasons you should care, and hopefully these will become apparent to you in this section. The insecure aspects of email manifest themselves in different ways. The following list will explain to you, in lay terms, issues associated with email that make it insecure.

1. Privacy – when you send an email message, your message passes through various networks as it travels to its final destination. This is somewhat similar to the U.S. Postal Service in that a letter that you mail goes through many different post offices before it reaches its final destination.

However, U.S. Mail is regulated so as the letter passes from post office to post office the same set of policies apply. The outcome, of course, is that the mail is more secure than it would be if we did not have uniform policies system wide. Well, email travels over the Internet, which is not regulated. As the email passes from one network to the next, there is no standard that regulates the level of security required on the network.

The information in the box on the top of the next page shows you the networks ("mail stops") that a recent email of mine traveled through to get to me from the sender. The networks are shaded. As you can see, this email message traveled through seven networks.



Each node is a potential security risk. Email can be read by anyone who is able to access any network between you and the person you are sending mail to. The only way to ensure that your email in not read by others is to encrypt it. However, there are many less technical things that you can do on a regular basis to reduce your email security risk.

2. Spam – this is the Internet version of junk mail. A spam email is generally defined as an unsolicited mailing, usually to many people. A message written for, and mailed to, one individual that is known to the sender is not spam, and a reply to an email is not spam, unless the "reply" repeats endlessly. Spam emailers have become a separate part of the Internet, with their own host computers, methods, and politics.

According to the Gartner Group, a research firm, about 90% of email users receive spam. It is prevalent and expected to grow. Why be concerned about spam? Actually there are several reasons why you should be concerned.

A. It is costing money. The recipient of the advertising is forced to pay the cost of the message. Your organization pays for email for various reasons, but not for you to receive advertising. It is costing the organization real money in terms of extra connection-time charges, phone time charges, disk space, and lowered bandwidth.
B. It results in lost productivity. Junk email wastes valuable time, because you have to spend extra time to download the unwanted messages, and then to wade through the junk email in order to get to the email you actually want.
C. Junk email clogs up people's email boxes, mingling with and sometimes even preventing receipt of legitimate email.
D. It may cause employers to pull employee internet email access, because they don't want to pay money for their employees to receive advertisements, nor for the lost productivity of their employees wasting (employer-paid) time identifying and discarding junk email.
E. It discourages people from participating in the Internet.
F. Spam is growing every day. As it continues to grow, the problems mentioned above will only worsen. The following story provides a glimpse of how spammers are facilitating the growth of spam on the Internet.

> A friend of mine conducted a small experiment. She got unsolicited commercial email with the usual message: "If you don't want to receive future email from us, use the REPLY button and place the word CANCEL in the subject header." My friend created a new email account, and used it to reply to the UCE. That email account was almost immediately flooded with a large number of UCE, not just from the first offender, but from others as well. So it appears that this REPLY solution is just another scam to collect addresses with which to further clog the net.

Did You Know…

Netcom estimates that approximately 10 percent of its customers' monthly bill is devoted to fighting SPAM.

Internet Week, May 4, 1998

Did You Know…

SPAM is estimated at more than 25 million emails per day or roughly 10 percent of all email world-wide.

Associated Press, March 30, 1998).

While spam comes in many different disguises, let's take a minute to look at some of the more frequently used and abused methods for spamming.

Chains - Chain letters are letters that promise a phenomenal return on a small effort. The return might be the promise of a free product or service, luck, love…..you name it, they will think of it. You are supposed to send the letter or some other thing on to other people. If you send it on, you will then get the promised in return. If you do not send it on, then you will get nothing in return or potentially suffer some type of harm. Here are a couple of classic examples.

Hello Everyone,
And thank you for signing up for my Beta Email Tracking Application or (BETA) for short. My name is Bill Gates.
Here at Microsoft we have just compiled an email tracing program that tracks everyone to whom this message is forwarded to. It does this through an unique IP (Internet Protocol) address log book database. We are experimenting with this and need your help. Forward this to everyone you know and if it reaches 1000 people everyone on the list will receive $1000 and a copy of Windows98 at my expense. Enjoy.

Note: Duplicate entries will not be counted. You will be notified by email with further instructions once this email has reached 1000 people. Windows98 will not be shipped until it has been released to the general public.

Your friend,
Bill Gates & The Microsoft Development Team.

This is a promise, send back to make the promise...

You are my friend and I hope you know that's true.
No matter what happens I will stand by you.
I'll be there for you whenever you need.
To lend you a hand to do a good deed.
So just call on me when you need me my friend.
I will always be there even to the end.

Forward this promise to all your friends to show your friendship and watch who sends it back.

Did You Know…

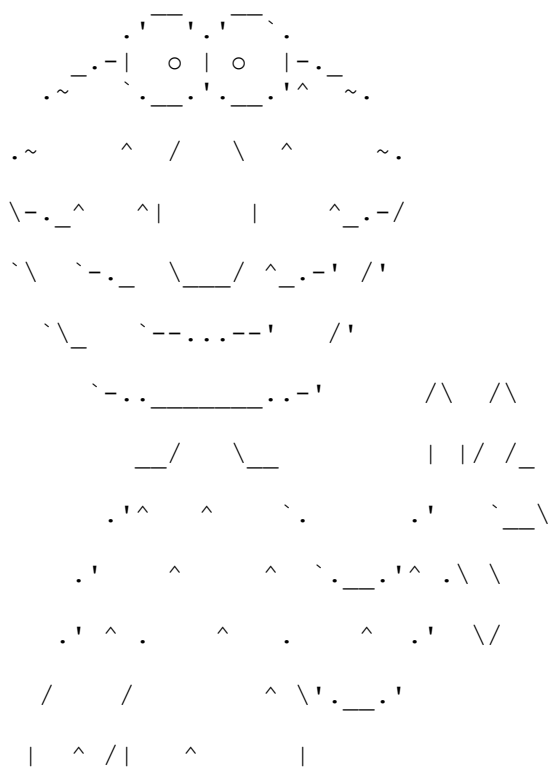
"I have spent more time and energy trying to quell rumors and e-mail hoaxes than actually fighting real virus threats."
-Patrick McFarland

-Berinato, Scott. "Virus Threats Take Toll on IT." E-Week. Jun '00:69.

Hoaxes – an email hoax is a specific type of chain letter that deceives you in order to prompt you to pass it along. Frequently email hoaxes pose as an alert and use technical jargon. This is done on purpose to confuse readers and to make them feel as if they are doing a service by passing the hoax email along. Anyone who sends these is doing just the opposite. The most common manifestations of hoax chain letters are phony virus alerts and appeals to fighting medical diseases. See the following examples.

If you receive an email titled "WIN A HOLIDAY" DO NOT OPEN IT. It will erase everything on your hard drive. Forward this letter out to as many people as you can. This is a new, very malicious virus and not many people know about it. This information was announced yesterday morning from Microsoft; please share it with everyone that might access the internet. This was sent to us by Jan Truskolaski at Lucent Technologies. Please, pass this along to everyone in your address book so that this may be stopped.

For cardiomyopathy research...Tickle me! :-)



For every new person that this is passed on to The American Heart Association will donate 3 cents to heart disease research. Please help us. Forward this to everyone you know. Thanks for helping!!

Rebuttals – the rebuttal is disguised as an attempt to combat chain letters, but in fact is a chain letter itself. A clever way to appeal to those who have grown very tired of chain email. Here is an example of this type of chain letter.

To Whom It May Concern:

This letter is being sent to you because recently, you were sent a chain letter, which you may or may not have passed on. This is an anti-chain letter. It originated at Portland State University. Its purpose is to put a stop to all of the silliness of chain letters and their complete lack of connection with luck, fortune, or
anything else. If you receive this anti-chain letter, keep it until you receive a chain letter. Then instead of spreading the chain letter, send this letter back to whoever sent that obnoxious piece of junk mail to you.

If you sent one recently, send this along to the same people. If we get lucky, maybe this will spread all over the world and eventually get back to those goobs who have nothing better to do than write meaningless letters that prey on people's superstitions. (How do they know how many times a letter has been "around the world" anyway?)

If you don't, your car will not break down; a close relative is not going to die; and you won't lose all of your money. If you do, you probably won't win a million dollars, receive a promotion, or suddenly find true love. (We sincerely hope you do anyway.) However, you will feel much better about ignoring chain letters in the future.

Thank you.

3. Information Leaks – sending out confidential information of any kind on email can be harmful. Given our conversation about networks and spam, you might be thinking that you only have to worry about email that uses the Internet; and that internal email that travels over your organization's Intranet is secure. In fact, you do have to worry about internal email….according to many experts, the biggest threat comes from within an organization. Consider the story on page 24.

Did You Know…

"80 percent of firewall breaches are due to internal causes, whether a disgruntled employee or an honest mistake."

-DeJesus, Edmund. "Managing Managed Security." Information Security. Jan '01:45.

Frank was not performing on his job and felt that his boss, Mark, was out to get him. Over the course of six months, Frank had several meetings with Mark. With each meeting that took place, Mark was using disciplinary actions that were progressively more serious. At their last meeting, Frank received a written warning. The warning spelled out performance expectations for Frank for the next month. It also specified that if Frank did not perform up to expectations, that he would be fired. Frank knew his job was on the line.

Five months earlier when all this began, Frank had been working on a special project with Nina, one of the Administrative Assistants in Human Resources. Nina was fairly new to the company and this was the first time she had performed some of her work on a computer system. Nina and Frank had regulary scheduled meetings to work on the project. However, Nina woke up with a fever one morning and called in sick. Frank, being a pretty shrewd guy, called Nina at home and volunteered to complete the task on his own. There was just one small problem, he would need access to the files, which were on her computer. Without hesitation, Nina gave Frank her userid and password, and thanked him for volunteering to do it by himself.

With termination pending, Frank began to intercept and read all of Nina's email. After about two weeks, Frank intercepted an email from Nina's boss to Nina indicating the official date of Franks termination…… Friday, the 15th. Frank came in to work early that morning and executed a program that would start running one week later. The program, which destroyed several financial records and the customer order database, wreaked havoc on the company.

4. Tampering – in addition to intercepting email for purposes of accessing confidential information, sometimes the underlying motive is for gain or harm by actually tampering with the message. If it is a case of tampering, then the message that is received will be different from the message that was originally sent.

In the case of a spoofed email, the message will appear to be from one person, when in fact, it is from an entirely different person.

5. Offensive contents – proprietary or confidential information is not the only kind of content that you should be concerned about when it comes to email. Offensive material can be equally troublesome. Offensive content would include, but is not limited to, sexual comments or images, racial slurs, gender-specific comments or any comments that would offend someone on the basis of his or her age, sexual orientation, religion or political beliefs.

Did You Know…

"In the scant few hours it took to develop a patch to defeat the IloveYou bug, the amorous worm had copied and distributed itself to some 10 million computers. Experts disagree on the total damages, but estimates range from $700 million to $15 billion."

-Bertin, Michael. "The New Security Threats." Smart Business for the New Economy. Feb '0!:81.

6. Viruses – due to viruses such as Melissa, Y2K, and the Lovebug, it is fairly wide known that email is used to spread viruses. The effect of a virus passed via email can range from simple annoyance to serious destruction.

Viruses are often spread via attachments. If your organization does not allow the use of attachments, this is probably why. As a user, you usually will not know that you have received a virus until you have opened the attachment. At this point, it is too late to keep from being infected. The act of opening the attachments activates the virus; it is now infecting your hard drive and possibly the network.

Viruses can also be transmitted via macros. Macros are tiny programs written to carry out actions. They are used to automate frequently performed tasks, such as addressing a letter to multiple recipients. Macro viruses are application specific and are most commonly found with applications such as Word, Excel, PowerPoint, and Access. The Melissa virus was a macro virus whose carrier was Microsoft Word 97 or Word 2000. If you received an infected document that you opened using another application, such as WordPerfect, you would not be infected with the virus. However, if you received an infected word document, and subsequently opened it with word, you can be infected if macros were enabled on your machine.

Sophisticated viruses are able to open your personal address list and send themselves on to everyone in your address book. This is an important point because it implies that sometimes you cannot even trust email that comes from a known source.

In addition to being embedded in .doc, .xls, and .ppt files, viruses are commonly transmitted in the following file types: .exe, .vbs, and .shs.

Email Security Fundamentals

Email poses a significant risk to security. One of the most effective tools for counteracting this security risk is an educated workforce and sound policy. The following tips will help you be more secure in your email use and practices.

1. Minimize the use of attachments. Copy and paste text as often as possible.

2. Question unsolicited documents. Unsolicited bulk mail and commercial email can put you and your organization at risk. Questioning it means not opening it, not passing it on, and notifying your system administrator immediately.

3. Never respond to spam email. For a spammer, one "hit" among thousands of mailings is enough to justify the practice. Instead, if you want a product that is advertised in a spam email, go to a Web site that also carries the product, inquire there, and tell them you do not approve of spam methods and will not patronize a company that uses spammers.

4. Never respond to the spam email's instructions to reply with the word “remove." This is just a trick to get you to react to the email -- it alerts the sender that a human is at your address, which greatly increases its value. If you reply, your address is placed on more lists and you receive more spam.

5. Never sign up with sites that promise to remove your name from spam lists. These sites are of two kinds: (1) sincere, and (2) spam address collectors. The first kind of site is ignored (or exploited) by the spammers, and the second is owned by them. In both cases your address is recorded and valued more highly because you have just identified it as read by a human.

6. Do not include confidential information in email. It does not matter if the information pertains to you or someone else, and it does not matter if the email system is Internet or Intranet based, confidential information in email is a risk that is not worth taking.

7. Do not include offensive information in email.

8. Question executable programs received via email. This is a common means for passing on viruses. Do not open them, do not

pass them on, and notify your system administrator if you receive them.

9. Disable macros on your machine. To do this, you will need to open the application. On Word 2000, select Tools, then select Macros, then select Security, and then check High: Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled.

10. Make sure that file extensions are viewable. This will alert you to files of the following types: .exe, .vbs, and .shs. To view file extensions in Windows select the Start menu, then select Settings, then select Control Panel, then select Folder Options, then select View, then **UNCHECK** the command that reads Hide File Extensions for Known file Types.

11. Notify the person you received an infected email from. This helps them correct the problem within their system before passing the virus on to other users.

Section 3E: Untrusted Software

Did You Know…

In the UK, 55 police departments were using unlicensed, counterfeit copies of Office Pro '97.

"Police departments have started replacing the software, at a cost of more than $10 million, to correct the licensing problem and avoid any security compromises."

-"British Bobbies Busted." Information Security. Jan '01: 27.

Why Worry about Untrusted Software?

Because it is untrusted, right? The hard part is differentiating between trusted and untrusted software. Obviously, we know that the software we buy from the local store that comes sealed with a shrink wrap and was produced by a legitimate company is "trusted." But we all like freeware and shareware that we can download from the Internet. Now we are faced with a different situation.

How can we verify that the software is safe? How can we verify that the source is a trusted source and therefore their software can be trusted. Furthermore, how can we verify that the software comes from whom it is supposed to be coming from and not an imposter?

Actually, the effects of untrusted software have already been referenced several times in this manual. However, we have not specifically identified all types of untrusted software yet. We will do that now. This section defines malicious software. Some of it will be review of concepts and concerns discussed earlier. Some of it will be new terms and definitions.

What is a computer virus?

A computer virus is a program that requires a host in order to make copies of itself on computer disks. Viruses may infect (copy to, and spread from), program files, programs in disk sectors, and files that use macros. The ability to self-replicate distinguishes viruses from programs that do not, and this parasitic nature is neither an accident, nor a computer glitch. All viruses are created by people who know how to write computer programs.

The first theories about the possibility of creating a self-replicating program date back to 1949, and experimental viruses were first programmed and tested in the 1960s. They got their name when a university professor used the term "virus" to describe them 1984, because like a biological virus, a computer virus is small, makes copies of itself, and cannot exist without a host. When personal computers became popular, PC viruses began to appear (in 1986-1987), at first intended as jokes, or developed for research or demonstration purposes.

THE VIRUS, CALLED W2K.STREAM takes advantage of a little-used feature included in Windows 2000 and older Windows NT systems that allows programs to be split into pieces called streams. Generally, the body of a program resides in the main stream. But other streams can be created to store information related to what's in the main stream. Joel Scambray, author of "Hacking Exposed," described these additional streams as "Post-it notes" attached to the main file.

The problem is that antivirus programs only examine the main stream. W2K.Stream demonstrates a programmer's ability to create an additional stream and hide malicious code there.

This virus begins a new era in computer virus creation. The 'Stream Companion' technology the virus uses to plant itself into files makes its detection and disinfection extremely difficult to complete.

What is an armored virus?
An armored virus tries to prevent analysts from examining its source code. The virus may use various methods to make tracing, disassembling and reverse engineering its code more difficult. A good example is the Whale virus.

The term armored virus actually comes from the medical field. Anyone suffering from a cold knows how tough and persistent viruses can be. Scientists have discovered that one type of virus actually comes equipped with an armored coat made of interlocking rings of protein. The structure of this virus is remarkably similar to chain mail suits worn by medieval knights. The head of the virus is organized exactly like medieval armor, referring to the chain mail suits worn by knights in the Middle Ages. These protective outfits were made of interwoven rings of iron that were designed to deflect arrows while allowing maximum freedom of movement during battle.

What is bacteria?
Electronic mail that spreads itself to all users when read or otherwise executed.

What is a chain letter?
Electronic mail that spreads similarly to real chain letters. You send a letter to ten people, who also send it to ten people, and so on. In addition, electronic chain letters can use your address book to spread themselves……something that physical chain letters could never do!

What is a cuckoo's egg?
A program that you maintain and nurture on your system, which you believe is yours, but is actually someone else's. The program is a malicious program and will eventually do evil.

What is a logic bomb?
A logic bomb is a type of trojan horse that executes when specific conditions occur. Triggers for logic bombs can include a change in a file, by a particular series of keystrokes, or at a specific time or date. See: Time Bomb.

What is malicious code?
A piece of code designed to damage a system or the data it contains, or to prevent the system from being used in its normal manner.

What is malware?
A generic term used to describe malicious software such as: viruses, trojan horses, malicious active content, etc.

What is a master boot sector virus?
Master boot sector viruses infect the master boot sector of hard disks, though they spread through the boot record of floppy disks. The virus stays in memory, waiting for DOS to access a floppy disk. It then infects the boot record on each floppy disk DOS accesses. Also: Master Boot Record Virus.

What is a rabbit?
A program that replicates itself very quickly.

What is a resident virus?
A resident virus loads into memory and remains inactive until a trigger event. When the event occurs the virus activates, either infecting a file or disk, or causing other consequences. All boot viruses are resident viruses and so are the most common file viruses.

What is a self-garbling virus?
A self-garbling virus attempts to hide from anti-virus software by garbling its own code. When these viruses spread, they change the way their code is encoded so anti-virus software cannot find them. A small portion of the virus code decodes the garbled code when activated. Also called: Self-encrypting Virus, Polymorphic Virus.

What is a time bomb?
A program that is written so that it occurs on a specific date, and/or time. For example: The Y2K bug, a virus written to execute on the January 1, 2000.

What is a Trojan horse?
Trojan horse programs are named for the giant wooden horse that concealed Greek soldiers who used it to invade the ancient city of Troy. Like that famous trick, a Trojan horse program conceals hidden programming. The hidden function may just be a joke, or something annoying, but vandals often use Trojan horse programs to destroy other people's data, knowing that some people will run any program that has an interesting file name, or promises to perform a useful function. A Trojan horse is a program that appears to be one thing, but is something entirely different. Many people use the term to refer only to non-replicating malicious programs, thus making a distinction between Trojans and viruses.

The Anna Kournikova Bug

The worm tempts potential victims by posing as a picture of Kournikova. It arrives with the Subject line: "Here you have, ;o)". The message body reads "Hi: Check this!" and it arrives with an attachment named "AnnaKournikova.jpg. vbs." The bug is a so-called "mass-mailer." Like the Melissa virus, it sends copies of itself to e-mail addresses in the victim's address book.

Feb. 14, 2001 — Dutch police have arrested and released a man who admitted responsibility for writing the Anna Kournikova virus. The 20-year-old suspect turned himself in to local authorities early Tuesday, according the AP. In accordance with Dutch law his identity has been withheld. He faces up to four years in jail.

What is a virus?
A program that infects other programs by modifying them to include code that instructs other computers to replicate the virus to still more computers. Viruses are capable of mutating or changing while they are replicating themselves. This is one reason why fighting viruses is particularly difficult. Viruses can be benign or malignant. Malignant viruses seek to destroy your data, files, or system. Benign viruses seek to cause disruption, but not destroy.

What is a virus hoax?
Hoaxes are not viruses, but are usually deliberate or unintentional e-messages warning people about a virus or other malicious software program. Some hoaxes cause as much trouble as viruses by causing massive amounts of unnecessary e-mail.

Most hoaxes contain one or more of the following characteristics:

- Warnings about alleged new viruses and its damaging consequences,
- Demands the reader forward the warning to as many people as possible,
- Pseudo-technical "information" describing the virus,
- Bogus comments from officials: FBI, software companies, news agencies, etc.

If you receive an e-mail message about a virus, check with a reputable source to ensure the warning is real. Visit McAfee.com's Virus Hoax page (http://vil.mcafee.com/hoax.asp) or with Vmyths.com a website about virus hoaxes (http://www.vmyths.com) to learn about hoaxes and the damage they cause. Sometimes hoaxes start out as viruses and some viruses start as hoaxes, so both viruses and virus hoaxes should be considered a threat.

What is a worm?
As intranets and the Internet have grown in popularity, e-mail has evolved from a convenience to a necessity. Virus vandals know that, and they've invented new ways to use e-mail to spread viruses, and especially, worms. A worm program is similar to a virus. It is considered by some to be a subset of a virus in that it makes copies of itself but does so without needing to modify a host. Like viruses, worms may (or may not) do things other than replicate. A worm will eventually use all the memory in a computer or network.

What is in the wild?
In the wild is a term that indicates that a virus has been found in several organizations somewhere in the world. It contrasts the virus with one that has only been reported by researchers. Despite popular hype, most viruses are "in the wild" and differ only in prevalence. Some are new and therefore extremely rare. Others are old, but do not spread well, and are therefore extremely rare. Below is a list of those thought to be "in the wild".

The Inception of Computer Worms

On Nov 2nd 1988 Robert Morris Jr., a graduate student in Computer Science at Cornell, wrote an experimental self-replicating, self-propagating program called a *worm* and injected it into the Internet. He chose to release it from MIT, to disguise the fact that the worm came from Cornell. Morris soon discovered that the program was replicating and reinfecting machines at a much faster rate than he had anticipated - there was a bug. Ultimately, many machines around the country either crashed or became "catatonic". When Morris realised what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However because the network route was clogged, this message did not get through until it was too late. Computers were affected at many sites, including universities, military sites and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000. Robert T Morris was convicted of violating the Computer Fraud and Abust Act (Title 18), and sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision

Are all these programs harmful?
They waste disk space and memory, delay computer operations, and increase the likelihood of system crashes. They are often poorly written and may function erratically, overwrite data, and cause programs to run erratically. Many also have destructive routines to alter or overwrite data. In addition, the cost of antivirus software and the time recovering from virus damage is passed along to consumers by businesses at the cash register.

Who creates these programs - and why?
Virus writers range from researchers, to pranksters, to malicious vandals. The typical virus writer is an otherwise intelligent male, between 15 and 23 years old. He may be bored, curious, or intent on doing forbidden things, just to frighten others. Some belong to organized virus-writing groups (usually short-lived), and those in the group often respond to peer pressure, trying to outdo the others. Whether in a group or not, some get satisfaction from the challenge, while others think of themselves as rebels against the "system."

How do they spread?
Viruses and Trojans spread from one computer to another by using one or more methods, all of which depend on user carelessness. Some people never have a problem, but others who are not as careful (or lucky) infect their hard disk by running downloaded files, or after placing a newly-obtained floppy disk in a drive. Viruses and worms spread fastest among computers networked on a LAN, especially when e-mail file attachments are involved.

Is sharing files a problem?
Sharing certain types of files with others always involves some certain risk. The medium is irrelevant; files from a LAN server, downloaded from Internet sites, from a floppy (even from shrink-wrapped software). Riskiest of all are files posted on Internet newsgroups, because there is no control or accountability. Many people have become the first victims of brand-new viruses and worms, by downloading executable files that were posted deliberately by vandals.

What about e-mail?
Before the growth of the Internet, viruses used to spread more slowly, from user to user, and anti-virus vendors were usually able to distribute a remedy before things got out of hand. That's all changed, especially with worms, because some people will click on any e-mailed file that they receive. Vandals have seized their opportunity, and created programs designed to spread to all those who correspond with careless users. Because of this threat, the only 100 percent safe e-mail file attachment is a deleted e-mail file attachment.

Can a cookie contain a virus?
Some Web sites store information on your computer, in small text files called cookies, that can be used when you re-visit that site. Examples include items you've selected for purchase, registration data, or your user name and password, for Web sites that require them. Since cookies are text files, they are not executable, and this fact eliminates the possibility of viruses, because they must be hosted by an executable file. It is theoretically possible to include UUencoded or MIME comments, but decoding a UUencoded or MIME file and executing it is not possible.

How can you tell whether your computer is infected?
Because some viruses cause strange things to happen, an odd or unexplained event may lead a user to conclude a virus must be responsible, without bothering to explore other possible causes. On the other hand, many viruses are carefully programmed to do nothing to betray their presence. The solution to this dilemma is not to assume anything, but to rely upon anti-virus software as a diagnostic tool.

How can you protect your data?
If you have files you can't afford to lose, make sure you have more than one copy of them. Programs may already be backed up on their original installation disks, but what about the files that you create? Business records, spreadsheets, manuscripts, and other important files can be lost in an instant to a virus, or to other causes, hard disk failure among them. If no other copy of your files exists, make copies of them, before it's too late.

Do you need to worry?
Worrying will get you nowhere. Instead, take sensible precautions, to avoid losing data should you be affected by a program that was designed to cause problems. Many people are fortunate never to encounter one, but a vandal's program could be concealed in the next file you download, or in a file attached to an e-mail message. Or the threat could be on the next floppy you insert in a disk drive, especially one obtained from a friend, a co-worker, or a fellow student.

Software Security Fundamentals

So, what can YOU do to secure yourself from untrusted software? There are many things that you can do, some of them we already talked about, so they are mentioned very briefly here. The good news is that most of these preventive measures are relatively easy to do.

1. Do not download executable programs from bulletin boards. Bulletin boards are a launching pad for untrusted software.

2. Do not accept or use unlicensed software. Legitimate businesses are just that, legitimate….for the most part, they are on the up and up.

3. Do not share software disks with other users freely.

4. Do not allow access to your computer by people whom you do not trust.

5. Do not leave your disks unattended.

6. Do not ignore abnormal functioning of your computer…..it might be symptoms of a virus or other malicious software.

7. Back up essential files. Keep a log of what you do to learn which applications are most important to you. Although you can restore them from their installation CDs, that does not mean they'd work the way they do now. So if you have re-configured any, you'd need to find out how and where they store that data, in order to back it up.

   Make backup copies of files on your hard disk. All hard disk files would be best. Some files may already be backed up (in effect) on original installation disks, but most important are the files you create with your applications. Business records, spreadsheets, manuscripts, and other important files that take tremendous work to produce can be lost in an instant--if no other copy exists. Do not take that risk--make copies of them.

8. Delete e-mail file attachments. The only 100 percent safe e-mail file attachment is the one you delete. Clicking on everything, as some users do, is very unsafe, because an e-mailed virus or worm can send a copy of itself to everyone a user knows, often disguised as something innocent. If you open a file attached to an e-mail, even from someone you know, you are always taking a risk, however small.

   Since worms (like KAK) can be concealed in the body of an e-mail, close the preview pane of your e-mail program, because that is what opens the e-mail message (but not attachments) automatically. Also, turn the Windows 98 Scripting Host off:

1. Click on Settings, then Control Panel, then Add/Remove Programs
2. Then click on the Windows Setup tab, then Accessories and if it is checked,
3. Uncheck Windows Scripting Host and Click "OK" to save changes -- or click CANCEL if it was not checked.

Note: Web pages that use scripts may not load properly with the Windows Scripting Host disabled, or you may be redirected to alternative pages, that don't use scripts. If you find that inconvenient, you can put the check mark back later (you may need your Windows CD to do that). For Windows 95 and ME, instead of doing the above, locate winscript.exe and rename it, or delete it from the hard disk (after you first copy it to a floppy disk, in case you want to restore it later).

9. Block Word Macro viruses. Since only Microsoft Word can open (run) macros that might be embedded in an MS-Word DOC file, those who use Word can enhance their safety by viewing DOC files sent to them by others using a free Viewer, available by download from Microsoft's Web site. Another safety enhancement would be sharing Word files that are saved in Rich Text Format, instead of Word Document format, because files in RTF format do not contain macros, and thus cannot harbor a macro virus. Word 2000 users should also make sure that macro virus protection (under Tools/Macro/Security) is set to High.

   Word 97 users should make sure that macro virus protection (under Tools, Options, General) is turned on (checked), and consider password-protecting Normal.dot:
   1) Exit Word97, then delete Normal.Dot
   2) Start Word, then use Alt-F11 to start the VisualBasic editor
   3) Press Ctrl-R to open a window in the upper left corner (if necessary)
   4) Click Normal in that window
   5) From the Tools menu, select Normal Properties, then Protection
   6) Check "Lock project for viewing" and enter a password
   7) Click OK, then press Alt-Q to exit the editor

   Remember the password, because while this procedure protects Normal.dot from viruses, you will need the password if you want to modify Normal.dot, to record your own macros, for example.

10. Stop virus hoaxes.

Did a ***genuine*** **computer security expert send you the alert? If** your mother-in-law forwarded a chain letter alert, which came from her dentist, who got it from a podiatrist, who got it from his secretary's daughter, who supposedly received it at college directly from IBM's virus experts.

Does the email offer a link to an *authoritative* details page? Email alerts shouldn't go into detail about a computer virus. Rather, the alert should

summarize the threat and provide a link to a "for more info" page stored on a *well-known* computer security website. ***Beware:*** some hoax alerts include generic links to respected websites. The hoaxster wants you to **assume** the website has important information about the virus. A rule of thumb: the link to more information should take you *directly* to more information about the threat. If it doesn't, then you should **chide** the sender for failing to give you accurate information.

Does it urge you to forward the chain letter to everyone you know? Genuine virus alerts won't ask you to participate in a **chaotic** email distribution scheme. Forward it instead to Vmyths.com (see below) so we can study it.

For More Information, Suggestions, Feedback, Contact:

Melissa J. Dark, Ph.D.
Assistant Director for Educational Programs
CERIAS
Purdue University
Recitation Hall
656 Oval Drive
West Lafayette, IN 47907
765-496-6761
dark@cerias.purdue.edu