

Computer Security Awareness



**Information Technology Division
and
National Employee Development Center
November 2001**



Student Manual

The United States Department of Agriculture (USDA) prohibits discrimination in its programs on the basis of race, color, national origin, sex, religion, age, disability, political beliefs, and marital or familial status. (Not all prohibited bases apply to all programs.) Persons with disabilities who require alternative means for communication of program information (Braille, large print, audio tape, etc.) should contact the USDA's TARGET Center at (202) 720-2600 (voice and TDD).

To file a complaint, write the Secretary of Agriculture, U. S. Department of Agriculture, Washington, D. C. 20250, or call 1-800-245-6340 (voice) or (202) 720-1127 (TDD). USDA is an equal employment opportunity employer.

Acknowledgements

The following individuals contributed to the design and development of this training program.

Mario Phillips, Deputy National Security Officer, NRCS, Beltsville, Maryland

Luis C. Gamboa, Telecommunications Specialist, NRCS, Ft. Collins, Colorado

Stuart N. Keil, Information Systems Security Program Manager, NRCS, Ft. Collins, Colorado

Dana Kuiper, Computer Specialist, National Water and Climate Center, NRCS, Portland, Oregon

Timothy Patton, Computer Specialist, NRCS, Juneau, Wisconsin

Kevin Reynolds, Computer Specialist, NRCS, Syracuse, New York

Georgia Spiller, Employee Development Specialist, National Employee Development Center, NRCS, Ft. Worth, Texas

Table of Contents

| Section | Page |
|---|-------------|
| Overview | 7 |
| Course Objectives | 7 |
| Lesson 1 – Policy, Responsibility, and Accountability | 9 |
| Lesson 2 – Threats and Vulnerabilities | 15 |
| Lesson 3 – Passwords | 23 |
| Lesson 4 – Data & Software | 27 |
| Lesson 5 – Communications Security | 33 |
| Lesson 6 – Physical Security | 39 |
| Conclusion | 43 |
| Answers to Self-Study Questions | 47 |
| References | 51 |
| Self-Certification | 53 |

Computer Security Awareness

Course Overview

NRCS depends on computer systems to perform many of its functions and responsibilities. These systems contain a wealth of information resources. The purpose of this training is to generate computer security awareness and concern among its readers and to ensure an understanding of our roles in protecting this valuable resource.

This training provides readers with practical information on computer security that users should immediately implement in all their daily activities. The following topics are addressed.

- Laws, Policy, and Responsibility
- Threats and Vulnerabilities
- Passwords
- Data/Software
- Communications
- Physical Security

The NRCS Information Systems Security Program Manager has determined that this training meets the requirements as outlined in the Computer Security Act of 1987.

Course Objectives

After completing this training, the participant will be able to protect Federal Information Processing (FIP) equipment and data by:

- identifying security risks and responsibilities, and
- implementing security principles routinely.

Who is required to take this training?

- All NRCS employees
- All NRCS volunteers using NRCS computer systems
- District Partners
- Other Partners
- Non-NRCS individuals with authorization to use NRCS computer systems
- Contractors officially located where NRCS computer systems reside

Lesson 1

Laws, Policy, and Responsibility

Overview

This lesson defines some of the terms associated with computer security. It explains the user's responsibility for the security of NRCS computer systems. A brief overview of the laws and policies of Federal information processing as well as some of the penalties for abuse of those laws is provided.

Goals of This Lesson

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

- define the term computer security.
- briefly explain the USDA computer security policy.
- explain the NRCS computer security policy.
- state who is specifically responsible for computer security.
- define the term — classified and sensitive information.
- list the correct procedures to follow in the event of a security breach.
- relate an understanding of the consequences for violation of security policy.

Computer Security: What is it?

Computer security is the protection of the integrity, availability, and confidentiality of automated information and the resources used to enter, store, process, and communicate it. Good security practices provide this protection.

Why is it needed?

Inadequately controlled or protected information systems can have some very serious consequences, including:

the inability to perform our mission and provide the public with our services,

the waste, loss or misappropriation of funds, and

the loss of credibility or embarrassment to our agency.

Consequently, laws were passed to mandate this protection. Computer security laws hold users and managers responsible for the security of the computer systems and the information they contain. Since computers and electronic access is available to almost everyone, this responsibility is necessary to address security in current information technology environments.

The Computer Security Act of 1987 requires Federal agencies to provide all persons involved in the management, use or operation of computer systems initial and periodic training in information systems security. The Office of Management and Budget (OMB) gave direction to all federal agencies by further interpreting the intent of Congress. OMB

developed and distributed OMB Circular A-130, Appendix III which enforces such mandatory training by requiring its completion prior to granting users access to the system.

The Government Information Security Reform Act requires an agency to develop and implement an information program and to provide information security for the operations and assets of the agency. The following describes USDA's and NRCS's policies and guidelines.

USDA Policy

USDA Policy, DR 3140-1—this regulation establishes departmental policy and assigns responsibility for safeguarding the Department's ADP resources and sensitive information resident on Departmental automated information systems to each agency.

USDA Policy, DR 3140-2—this regulation establishes security requirements for the use of the Internet by U. S. Department of Agriculture employees.

USDA Policy, DR 3300-1—this regulation establishes policies and assigns responsibilities for the management and use of telecommunications services, equipment, and resources within the U.S. Department of Agriculture.

USDA Policy, DM 3440-1—this manual is designed primarily for use by Agency Classified Material Control Offices and USDA personnel specialists.

USDA Policy, DN 3140-6—this notice establishes policy for implementing secure Internet protocol from USDA networks to non USDA networks.

USDA Policy, DN 3140-8—this notice establishes policy for securing information on computers in the USDA networks.

NRCS Policy

NRCS security policy is a result of additional policy developed by USDA and NRCS managers emphasizing the protection of systems and data critical to our agency's operation. This policy is primarily found in Section 508 of the National Information Resources Management Manual (NIRMM). States may supplement the policies and procedures in the NIRMM and the National Information Security Handbook (NISH).

The NRCS policy states the importance and value of computer and information resources and the need to preserve and protect its integrity, confidentiality, and availability. All employees and contractors are required to protect Government resources from accidental or deliberate unauthorized access, use, modification, or disclosure by employing adequate security measures through cost-effective technical and managerial controls. All employees and contractors shall be personally accountable for Government resources entrusted to them to perform official Government business.

Additional information on information security policies can be found in the following:

National Instruction No. 270-307 — IRM-NRCS Internet & World Wide Web User Policy—which discusses Internet use by employees and contractors.

General Manual (GM) 270-IRM Circular No. 2 (Part 403): IRM Security - Electronic Mail (E-MAIL) System— which discusses e-mail use by employees and contractors.

National Information Security Handbook, IRM-270-VI—which discusses security practices, procedures, and responsibilities to be followed by employees and contractors.

General Manual (GM) 270-IRM Part 400: Information Technology (IT) – Roles and Responsibilities which discusses security practices to be followed by information technology employees and contractors.

Responsibility

One fundamental question that arises in discussions of computer security is “Whose responsibility is it?” A simple answer is “Computer Security is Everyone’s Responsibility.”

All users have the responsibility of being familiar with the NRCS computer policy and guidelines and are required to implement the policy. Managers, supervisors and IRM personnel have additional responsibilities as defined in the NIRMM. After you receive authorization to use any Federal computer system, you become personally responsible and accountable for your activity on the system. Accordingly, your use should be restricted to those functions needed to carry out job responsibilities.

Individual responsibility includes:

Ensuring that user identification codes and passwords are held in strict confidence and are properly safeguarded from unauthorized access, use, and disclosure.

Understanding and complying with all security requirements pertaining to Federal laws, USDA and NRCS policies.

Refraining from exploiting any hardware, software, communications, or automated information system weakness, such as intentionally modifying, destroying, reading, or transferring data and information in an unauthorized manner.

Providing correct user identification codes and using only approved authorized computing environments, automated information systems, data,

and information resources as authorized by your immediate supervisor.

Securing and logging off from any computing environment when processing is completed. Always logging off at the end of each workday.

Performing regular backups of data, software, applications, and information on computer resources using the fixed disk drive, tapes, and diskettes for disaster recovery purposes.

Refraining from introducing any unauthorized software, data, hardware, or telecommunication devices or modifying any configuration without proper approval from the Information Resources Management Coordinator.

Classified and Sensitive Information

It is the duty and responsibility of all NRCS employees and contractors with access to classified or sensitive information to protect this information against unauthorized disclosure in the interest of national security.

Classified and sensitive information can be defined as information that is personal in nature, proprietary, financial, National Security-related, or critical to agency plans and operations and for which loss, unauthorized modification, or unauthorized disclosure would be detrimental to National Security or agency operations.

People often forget to lock up sensitive reports and computer media containing sensitive data when they leave their work areas. Information carelessly left on top of desks and in unlocked storage can be casually observed, or deliberately stolen.

While working, be aware of the visibility of data on your personal computer or terminal display screen. You may need to reposition equipment or furniture to eliminate over-the-shoulder viewing. Be especially careful near windows and public areas.

Label all sensitive diskettes and other computer media to alert other employees of the need to be especially careful. When no longer needed, sensitive information should be deleted or discarded in such a way that unauthorized individuals cannot recover the data. Printed reports should be shredded, while data on magnetic media should be overwritten. Files that are merely deleted are not really erased and can still be recovered.

Personal computers used for storing or processing sensitive or classified information shall have approved security measures, such as removable hard disks, and secure telephone units for secure telecommunication (if applicable).

Security Breaches

Each and every user across the country may introduce a risk to all other users in some manner. Because computer systems are no longer isolated and are connected by way of networks, a single breach of security anywhere can affect systems everywhere.

A security breach can be defined as an incident where a person obtains access to printed information or a secured area that he/she is not authorized to see. Also, a security breach is an incident where a computer program or computer user gains access to computer systems that he/she is not authorized to use.

In recent years, NRCS has had several major security incidents. Some examples of those breaches follow.

The "Love" virus corrupted many users' computer hard drives.

An international hacker tried to copy password files from many USDA machines and succeeded in some cases.

Some offices have had their computers stolen.

Procedures to follow when NRCS security has been comprised may vary slightly from location to location but generally, the following should be used.

1. Immediately record how the incident was discovered and your actions leading up to the discovery.

2. Back up your system and data files.

3. Notify your supervisor and/or the IT Security Coordinator for your location.

4. Supply information as requested to the Information Technology Security Coordinator.

Many losses could be avoided if computer users would report any circumstances that seem unusual or irregular. Warning signals could include such things as *unexplainable system activity that you did not perform, data that appears to be of questionable accuracy, and unexpected or incorrect processing results.*

Ultimately, computer security is the user's responsibility. The user must be alert to possible breaches in security and adhere to the established security regulations and procedures.

Security Laws and Penalties

The Computer Fraud and Abuse Act of 1986 provides for punishment of individuals who *access federal computer resources without authorization; attempt to exceed access privileges, abuse Government resources, and/or conduct fraud on Government computers.*

The following will show you just how seriously the Government considers abuse of computer security laws.

Federal law, NATIONAL SECURITY INFORMATION - 18 U.S.C. SECTION 1030(a)(1), prohibits accessing a computer with/without or in excess of authority,

thereby obtaining National Security Information that could be used to injure the United States.

If convicted of this offense, the maximum penalties are 10 years in prison for the first offense and 20 years in prison and \$250,000 fine for the second offense.

Federal law, Protecting Information 18 U.S.C. SECTION 1030(a)(2) prohibits intentional accessing a computer with/without or in excess of authorization and obtaining information in a financial record or a credit report on U.S. Government owned computers.

If convicted of this offense, the maximum penalties are 1 year in prison and \$100,000 fine for the first offense and 10 years in prison and \$250,000 fine for the second offense.

Federal law, TRESPASS IN GOVERNMENT - 18 U.S.C. SECTION 1030(a)(3) prohibits intentional accessing any nonpublic computer of a Federal agency if not authorized to access any computer of that agency.

If convicted of this offense, the maximum penalties are 1 year in prison and \$100,000 fine for the first offense and 10 years in prison and \$250,000 fine for the second offense.

Federal law, ACCESS IN ORDER TO DEFRAUD - 18 U.S.C. SECTION 1030(a)(4) prohibits the intent to defraud by accessing a "protected computer" without or in excess of authorization and obtain anything of value over \$5000.

If convicted of this offense, the maximum penalties are 5 years in prison and \$250,000 fine for the first offense and 10 years in prison and \$250,000 fine for the second offense.

Federal law, 18 U.S. Code Section 1030(e)(8) prohibits any impairment to the integrity or availability of data, a program, system, or information that causes a loss of \$5,000 or more in a 12-month period, or causes personal physical injury.

Federal law, TRAFFICKING IN PASSWORDS - 18 U.S.C. SECTION 1030(a)(6) prohibits an intent of defrauding or trafficking affects interstate or foreign commerce on a U.S. Government computer.

If convicted of this offense, the maximum penalties are 1 year in prison and \$100,000 fine for the first offense and 10 years in prison and \$250,000 fine for the second offense.

Federal law, THREATS TO DAMAGE A COMPUTER - 18 U.S.C. SECTION 1030(a)(7) prohibits any electronic communication containing any threat to cause damage to a protected computer or the intent to extort money or anything of value from any person, firm, or entity.

If convicted of this offense, the maximum penalties are 5 years in prison and \$250,000 fine for the first offense and 10 years in prison and \$250,000 fine for the second offense.

Federal law, WIRE FRAUD - 18 U.S.C. 1343 prohibits using the wires in furtherance of a scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises.

If convicted of this offense, the maximum penalty is 5 years in prison and \$250,000 fine.

Federal law, WIRETAP STATUTE - 18 U.S.C. 2511 prohibits the intentional endeavoring to intercept any wire, oral, or electronic communication and disclose the

contents of a communication that was obtained through an illegal wiretap.

If convicted of this offense, the maximum penalty is 5 years in prison and \$250,000 fine.

Federal law, UNLAWFUL ACCESS TO STORED COMMUNICATIONS - 18 U.S.C. 2701 prohibits intentional accessing a facility through which an electronic communication service is provided and obtaining, altering, or preventing authorized access to a wire or electronic communication.

If convicted of this offense, the maximum penalty is 6 months in prison.

The above prohibitions and punishments apply to mere attempts, even if

unsuccessful, to commit the listed crimes. Multiple accesses or multiple attempts constitute multiple offenses for the purpose of determining punishment.

Summary

With the increased use of computers and computer networks to conduct official business, more emphasis must be placed on security. The security of your information is dependent on you and your peers following good security principles and practices.

You are a partner with the Information Resources Management staff in ensuring Federal Information Processing security. Everyone is responsible for computer security.

Questions for Self-Study—Lesson 1

1. State the definition of computer security.

2. Whose responsibility is computer security?
“Computer Security is _____.”
_____.”

3. What is a security breach?

4. Some Federal laws carry a penalty of 10 years in prison and a \$250,000 fine if convicted of a computer security offense.
A. True
B. False

Lesson 2

Threats and Vulnerabilities

Overview

There are many software and hardware security vulnerabilities that are inadvertently created by new software releases, upgrades to the operating system and application software. This lesson will explain some of the reasons and methods to protect the information on your computer hard drive.

Goals of This Lesson

Upon completion of this training, the participant will be able to

- define the terms threats and vulnerabilities as related to computer security,
 - recognize the various types of threats and vulnerabilities that can damage computer equipment, data and applications stored on computers.
 - minimize threats and vulnerabilities to computer hardware and software.
-

Introduction

With the increased number of personal computers, laptops, and peripheral equipment at employees' desks and the increased use of networks, threats and vulnerabilities to computer equipment and the data and software stored on the equipment have multiplied. In this lesson, we'll introduce you to common threats to your computer system. We'll also show you how a computer system is vulnerable to common threats. With this in mind, our goals for this lesson are to enable you to define the terms, threats and vulnerabilities, as related to computer security. You should also recognize the various types of threats and vulnerabilities that can damage computer equipment, data and applications stored on computers, and adopt measures to minimize threats and vulnerabilities.

Definitions

Threats and vulnerabilities are terms that are often used interchangeably but refer to two separate concepts.

A computer security threat is anything that can harm or damage your information or computer assets (hard drives, CDs, tapes, software, etc.)

A computer vulnerability is defined as a weakness or flaw that allows a threat to harm or damage your computer system.

Threats

Threats can be divided into four basic categories:

- manmade
- technical
- environmental
- natural

Manmade Threats

Manmade threats are threats produced by people. We'll discuss manmade threats in two categories.

Internal Manmade Threats

Internal threats are those that come from within the organization. Personnel who

come in contact with the computer system on a daily basis are often responsible for these threats.

Internal threats may be intentional or unintentional. Personnel who pose unintentional threats are usually uninformed or careless. Personnel who intentionally cause harm to computers are usually extremely knowledgeable of computers, security systems and countermeasures.

Following are some examples of internal threats:

Improper use of password (sharing passwords, writing it down on a piece of paper on or near your computer)

Improper media handling

Improper disposal of media

Eating, drinking or smoking near computer equipment

Malicious data alteration

Operator error

Disgruntled employee access

Employee sabotage

Theft of hardware, software or data

Unauthorized access

Snooping/Browsing/Eavesdropping

Sifting through discarded waste to obtain information including user ids, personal addresses or telephone numbers, etc.

External Manmade Threats

External manmade threats are those that come from people outside the organization. External threats are almost always intentional.

Following are some examples of external threats:

Hackers

Theft of hardware, software or data

Former employee access

Unauthorized access

Snooping/Browsing/Eavesdropping

Civil Disorder

Vandalism

Sifting through discarded waste to obtain information including user ids, personnel addresses or phone numbers, etc.

Industrial espionage

Technical Threats

Technical threats are manmade, but deserve their own separate heading because of the pervasive problems they can cause. Technical threats are threats that manipulate software programs and data.

The more common ones include:

Software bugs

Data diddling (a change in the data without the owner's awareness) system component and leaves no obvious signs of its presence.

Scanning computers and network devices.

Snooping/Browsing/Eavesdropping

Malicious Software

– *Virus* - Self-replicating, malicious program segment that attaches itself to an application program or other executable. A virus may contain a Logic Bomb or Trojan horse.

- *Worm* – a program designed to propagate through a network rather than just a single computer.
- *Trojan Horse* - A worm that pretends to be a useful program or a virus that is purposely attached to a useful program prior to distribution.
- *Time Bomb* - A virus or worm designed to activate at a certain date/time.
- *Logic Bomb* - A virus or worm designed to activate under certain conditions.
- *Rabbit* - A worm designed to replicate to the point of exhausting computer resources.
- *Bacterium* - A virus designed to attach itself to the operating system and exhaust computer resources, especially central processing unit cycles.
- *Spamming* - Overloading a system with incoming message or other traffic to cause system crashes.
- *Tunneling* - Any digital attack which attempts to get under a security system, by accessing very low level system function (e.g., device drivers or operating system kernels).

Environmental Threats

Environmental threats are conditions in a facility that can cause harm or damage to sensitive information and all information technology at your work site.

Environmental threats include:

Heat

Water damage

Power failure

Magnetism

Natural Threats

Natural threats are threats from nature. They include the following:

Airborne particles (dust, smoke, hair, etc.)

Earthquakes

Fires

Floods

Electrical storms

High winds

Static electricity

Vulnerabilities

A *computer vulnerability* is defined as a weakness or flaw that exposes computer equipment, software or data to the threats mentioned previously. Different types of vulnerabilities can include:

Software/data

Hardware

Human

Network

Software

Software is vulnerable because many people within an office have access to it and because it is easy to modify. Software may be vulnerable to:

Theft

Data alteration

Technical threats (Trojan horses, viruses, etc.)

Unrestricted access (By not restricting access to data, others can modify that data either intentionally or unintentionally. In some cases it may be a subtle change

which the “owner” of the data does not notice (data diddling) but which can have serious consequences. It could also be more noticeable, but still difficult and time-consuming to correct.

Software bugs

Illegal duplication

Viruses and Trojan horses

Unwanted modification (includes loading single license software on more than one computer, invalidating the license agreement)

Downloading unapproved software and files from Internet sites

Hardware

Like software, hardware is vulnerable to a number of threats. Hardware may be vulnerable to:

Theft

Vandalism

Natural or environmental threats

Denial of Service attacks

Human

Human vulnerabilities include:

Untrained Users

Operator Error

Disgruntled employee

Unauthorized access

Improper use of passwords

Disposing printouts of sensitive information without shredding.

Sharing sensitive or private information with people who do not have a need to know the information.

Failure to backup important files onto diskettes

Trusting the validity of software received from unknown companies and known acquaintances

Network

Computers are no longer used only in a “stand-alone” mode. They are often connected to other computers in the office in local area networks; or with telephones and modems, connected to computers and information worldwide. Linking computer allows software and data to be transferred from one computer to another. Linking computers also makes your computer systems vulnerable to security threats.

Network vulnerabilities include the following:

Improper backups

Not following password procedures

Unauthorized software

Malicious e-mail attachments to spread viruses

Spamming (e-mail flooding)

Exposure to multiple users

Shared file systems

Another method to distribute viruses

Remote logons from home as a privileged user

Case Studies and Exercises

Please review the case studies below and write your answers in the spaces provided. The correct answers can be viewed later in this lesson.

Case Study 1

Natasha, a hydrologist, has logged onto a remote computer. She suddenly remembers she has a meeting and leaves her desk without logging off. Susan comes into Natasha's area and notices Natasha is logged in. Being curious, Susan sits down at Natasha's computer.

Question: What kind of threat is Susan at this point? What part of the threat does Natasha play in this scenario? What is the solution to this problem?

Case Study 2

Boris, an engineer, has spent the last two hours entering data for a high priority project. An electrical storm disrupts the power in his building. His computer is damaged and the data lost.

Question: What has happened in this scenario? How could this damage have been avoided?

Case Study 3

Rocky, a wildlife biologist, received a diskette from a friend on the habitat requirements of moose in the Rocky Mountains. He took this diskette to the office and loaded the data onto his PC. Before long, several of his PC applications quit working the way they should. Some files are missing as well.

Question: What has happened to Rocky's PC?

Case Study 4

Kristen's password has expired and she needs to pick a new one. Kristen picks kristen1 as her password.

Question: Are there any vulnerabilities involved with selecting a password such as this? What threats has Kristen left herself open to?

Case Study 5

On Wednesday, Charles borrowed a laptop computer to use over the weekend. Since he does not need to take it home until Friday, he left it on his desk overnight.

Question: What's at risk here?

Questions for Self-Study—Lesson 2

1. Doing periodic backups of files can protect the user from which of the following computer security threats:
 - A. Power outage
 - B. Operator error
 - C. A virus
 - D. Fire
 - E. All of the above
2. An example of a natural threat is:
 - A. High winds
 - B. Magnetism
 - C. Viruses
 - D. Trojan horses
 - E. All of the above
3. It's okay to leave your computer logged into a remote computer if:
 - A. you will only be away for a few minutes.
 - B. you have a screen saver.
 - C. you are meeting with someone just a few cubicles away.
 - D. None of the above.
4. If your area is being threatened by a severe storm (electrical, hurricane, etc.), the following steps should be taken.
 - A. Unplug all computer equipment.
 - B. Move all computer equipment, CD's, diskettes and/or tapes away from the windows.
 - C. Cover all computer equipment
 - D. If there is time, perform a backup of your system.
 - E. All of the above.

Answers to Case Study Exercises

Case Study 1

Answer:

Susan's actions are an example of an internal man-made threat. She could be snooping through sensitive files, deleting or damaging files. Her actions could be intentional or unintentional. Natasha has left both her system and the remote system vulnerable. The solution for protecting against this type of computer security threat and vulnerability is to always log off whenever you leave your PC unattended.

Case Study 2

Answer:

This is an example of a natural threat. A counter measure for avoiding this threat is for Boris to plug his PC and peripheral equipment into a power strip with a surge protector. Periodic saves to a floppy disk, CD-ROM or some other type of removable media would have minimized the loss of data.

Case Study 3

Answer:

The diskette contained a virus that contaminated his PC. Rocky should have run the diskette through a virus checker before loading it onto his PC. Since he had recent backups, his loss of data was minimized. This is an example of a technical threat.

Case Study 4

Answer:

Since this is such an easily guessed password, anyone else could gain access as Kristen almost immediately. This type of password is widely used and places your system at great risk. Kristen has left her system open to any number of threats. (Passwords are the subject of the next lesson.) Kristen should not have used a name of a person, place, or thing as a password.

Case Study 5

Answer:

Laptops are easy to steal. To protect it, Charles should have locked it in a desk drawer, in a locked computer room or another locked area. Some laptops connect to docking stations. They should be locked to the docking station when possible to keep them secure.

Lesson 3

Passwords

Overview

This lesson explains the purpose of passwords and introduces you to the proper techniques for selecting a password. It describes practices and procedures that enable you to protect your passwords.

Goals of This Lesson

Upon completion of this training, the participant will be able to

- explain why we use passwords.
 - describe a proper password and its structure.
 - protect passwords by keeping them private and concealed.
-

Introduction

If a stranger were to tell you that he wants you to give him all of your cash, it's unlikely that you would comply. You'd probably call the police. On the other hand, a computer would probably not only give the stranger its cash, but also ask if the credit cards are needed, too. Why? Because the computer has no common sense. The computer does not know that it should not be giving away credit cards or credit card numbers!

Luckily, we can construct barriers between the world and your computer to minimize the chances of this happening. One of these barriers is the password.

When you have completed this lesson, you will be able to explain why we use passwords, describe a proper password and its structure, protect passwords from being stolen and used by other people.

What is a password?

A password is a set of letters and numbers that you type into a computer that allows access to the computer system or designated data files. It's a

method of authenticating a unique user. It is used in conjunction with your computer identification normally called the user id.

The objective when choosing a password is to make it as difficult as possible for someone to make educated guesses about what you've chosen. If chosen carefully and protected, the password can be an effective barrier to unauthorized access. A large number of computer security incidents can be traced to poorly chosen passwords. For most of us, the single most effective thing we can do to contribute to the security of NRCS data is to properly select and properly protect our password.

By using good passwords, we protect

- valuable data,
- computer resources and services,
- sensitive information,
- and fulfill our responsibility to others utilizing shared systems.

Password Characteristics

Passwords should have a complex format and minimum length and should be

changed periodically and not repeated. Characteristics of a good password include:

- a minimum of 8 characters.
- includes numbers and/or punctuation marks within the password.
- capital and small letters.
- no obvious number/letter substitutions e.g. zero for the letter.
- no personal information e.g. names or birth dates.

Guidelines and Suggestions

The following will help you when composing a password.

Do not use your login name in any form.

Do not use your first or last name in any form.

Do not use your spouse or child's name.

Do not use other information easily obtained about you.

Do not use a password of all digits, or all the same letter.

Do not use a word contained in (English or foreign language) dictionaries.

Do not use a password shorter than eight characters.

Use a password with mixed-case alphabetic characters.

Use a password containing non-alphabetic characters, e.g. digits or punctuation.

Use a password that is easy to remember, but not easy for someone else to guess or construct.

Use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Choose a line or two from a song or poem, and use the first letter of each word.

Alternate between one consonant and one or two vowels.

Choose two or more short words, link them together and include punctuation characters.

Pick random characters out of a hat.

Examples of Good And Bad Passwords

| | |
|---------------------|---|
| rA\$sc2al | is good |
| fluffy | is bad |
| \$contribute | is bad |
| good4u | is bad |
| jrs123 | is bad, (especially if the initials of your name are jrs) |
| WRR_314 | is bad (if this is your license plate) |
| ObviOus | is bad |
| feDer\$\$8al | is good |
| tOyb%oxx | is good |
| b5Y;u99G%p | is good but not practical |

How can you protect your password?

The following guidelines will help protect your password:

Do not share your password with anyone.

Do not write your password down.

Change your password at least every 90 days.

Do not let anyone observe you typing in your password.

Do not include your password in any data file.

Do not use “remember password” features.

Do not attempt to reuse an expired or invalid password.

Summary

In this lesson, we have learned the definition of a password, the characteristics of a good password,

and some guidelines and suggestions for composing a password. We have also learned what to do to protect your password.

We must remember that the first and most important link in the security chain is the password. If the link is weak, then the whole chain is broke and no combination of security measures will keep your system secure.

Implementation of the password security measures discussed in this lesson will enable you to develop a proper password and protect your data, hardware, and software.

Questions for Self-Study—Lesson 3

1. Which of the following is an acceptable password?
 - A. bunny
 - B. egbD_lf
 - C. kristen1
 - D. None of the above
2. How can you protect your password?
 - A. Don't tell it to anyone
 - B. Don't write your password down.
 - C. Don't use personal information
 - D. All of the above.
3. We use passwords:
 - A. to protect data
 - B. to protect computer resources and services
 - C. to fulfill responsibility to others utilizing shared systems
 - D. All of the above
4. Your local security officer may impose password requirements stricter than those described in this course.
 - A. True
 - B. False

Lesson 4

Data and Software

Overview

This lesson provides a brief overview of procedures to protect critical data and information that is processed by computers to support the mission of NRCS.

Goals of This Lesson

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

- state NRCS policy on copyrights and intellectual property rights.
- state policy for distributing NRCS developed software and data.
- state policy for allowable software on NRCS computers.
- describe the difference between shareware and public domain software.
- describe the problems associated with using unapproved software.
- describe sensitive data.

Introduction

By itself, computer hardware is useless. In order to function, the computer must have sets of instructions called software. There are two types of software: *operating systems software* and *applications software*.

Operating system software are the programs that coordinate communications between your computer's central processing unit and its other computer equipment, for example, the printer and scanner. These programs perform routine "housekeeping" activities such as, starting the computer, keeping track of the location of data, and placing data in storage.

Applications software are programs that contain instructions for specific tasks you want a computer to perform. For example, you may want to use a word processing program to prepare a memo or a spreadsheet program to manipulate numbers and formulas.

An applications software program may be purchased commercially, or it may be developed by NRCS to do a specific task that commercial software cannot do.

NRCS has millions of dollars invested in both kinds of software and data. Due to this large investment, users must be diligent in practicing security measures when installing, entering, storing or otherwise manipulating data and software. USDA and NRCS security policies have been developed to improve the security of computer directories, files, diskettes and compact disks that are used to help employees accomplish their work.

Definitions

An *intellectual property right* is the guarantee under law that originally-authored software, writings, music, etc. cannot be used by others without permission granted by the owner of the right.

Copyright is a form of legal protection of intellectual property.

Shareware is software that is distributed by the author for a period of time for free trial use. If the user determines that he/she wants to keep the software, then the user is usually instructed to send the dollar amount requested to the developer. If the user determines not to purchase the software, then the software must be completely removed from the computer.

Public domain software is software placed in the public domain by the author and is free of charge for the use of the software. However, the author usually requires that he/she be acknowledged if the software is used to print reports or is part of another software system.

Maintenance

NRCS employees and contractors need to practice good procedures to reduce the security risks to information processed by computers.

To maintain data/software security, the user should:

Handle all portable media carefully.

Erase or destroy all portable media before disposal.

Protect storage media against vandalism, theft or environmental damage.

Secure external media when not in use.

Shred hard copy waste containing private information such as employee or client information.

Perform periodic system backups and store in a secure area.

Keep food or drink away from all storage media.

Ensure access to data is authorized.

Scan all media using virus detection software.

Position equipment, e.g. monitor, in a way that maximizes the protection of data.

NRCS Policy

The following statements explain methods to avoid any negative impact and publicity on NRCS' reputation concerning the use of commercial software.

NRCS users will honor intellectual property rights including copyright restrictions.

Copyrighted software will be installed and used in accordance with license agreements

Unauthorized copies of software will not be made for office or personal use.

Software may not be borrowed or removed from the workplace.

Only software that is officially released or approved by the appropriate NRCS management is to be used. (Applies to NRCS officially developed software and commercial software tested by the Common Computing Environment (CCE) team)

Proprietary Use

This section will state practices that discuss proper use of licensed software, which can be traced to a vendor, supplied serial number.

NRCS users will honor all copyright restrictions and intellectual property rights. Copyrighted software will be installed and used in accordance with licensing agreements.

Unauthorized copies of software will not be made for office or personal use.

Software may not be borrowed or removed from the workplace.

Only software purchased through NRCS procurement system or NRCS FIP released software is to be used on NRCS systems.

Permission must be obtained before NRCS software or data is placed on a personal home computer or a computer in a conservation district office.

NRCS data/software installed on a non-NRCS FIP computer must be protected at the same level as it would be on an NRCS system.

All users will ensure that the appearance of any data tampering, malicious software, or unauthorized access is reported immediately through your supervisor.

Sensitive Data

Sensitive data is:

“The loss, misuse, or unauthorized access to or modification of any information which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act of 1974), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.”

How do you protect sensitive data?

Use encryption if the sensitivity of the data warrants such protection. See your IRM coordinator for additional information on encryption. You can also protect sensitive data if you:

Shred paper documents

Restrict access to systems

Restrict access to tables within a database.

Setting appropriate permissions on files.

Put printouts with sensitive information in a secure file cabinet.

The screen of a workstation/laptop should be placed so that others cannot see the screen without explicit permission.

Media containing information essential to the mission of the organization should be duplicated and the duplicate should be stored in a secure off-site location.

Shareware or Public Domain Software

Shareware is software that is distributed by the author for a period of time for free trial use. If the user determines that he/she wants to keep the software, then the user is usually instructed to send the dollar amount requested to the developer. If the user determines not to purchase the software, then the software must be completely removed from the computer.

Public domain software is a computer program that can be obtained from bulletin boards, chat rooms, computer shows, computer user support groups.

NRCS, generally, does not approve the use of software or public domain software. NRCS, at the national level, works with the developers of public domain software if there is a need to use this software for NRCS business.

Unapproved Software

This section will discuss software, which is not purchased through your local procurement office or the Common

Computing Environment project. Some of the following problems could occur if unapproved software is used.

Your system administration may not be able to support or troubleshoot a problem on your system created by the unapproved software.

Unapproved software or unapproved versions of software may conflict with other software. This is especially true as computers are connected to local and wide area networks.

Unapproved software may contain bugs and/or viruses.

Game software obtained outside of official channels should not be used on NRCS computers.

Software obtained from bulletin boards and chat rooms should not be used on NRCS computers.

Software obtained from unknown sources should not be used on NRCS computers.

NRCS Policy for Distribution of Data

The commercial software that is distributed on the Common Computer Environment workstations and servers have been tested by personnel from NRCS, Farm Service Agency, Rural Development to ensure the software meets your immediate computing needs.

The management team of the three USDA agencies has approved the software that is distributed on the CCE computers. Any other software distributed to employees should be approved by the state or regional IT management.

Types of software that should be distributed within NRCS

Official Release of NRCS developed software

Commercial Off the Shelf acquired in hardware procurement

Other Commercial Off the Shelf procurement

Approval of the NRCS data owner and CIO for data distribution to the public.

Summary

In this lesson we have learned about NRCS policies concerning commercial software and the difference between shareware and public domain software. Also, we have learned the difference between appropriate software and inappropriate software to be executed on NRCS issued computers.

Questions for Self-Study—Lesson 4

1. Intellectual property rights and copyright laws do not apply nor have any bearing on computers housed in federal office buildings.
A. True
B. False
2. NRCS does not approve the use of shareware or public domain software.
A. True
B. False
3. NRCS encourages employees to use any software from any source that will enhance the work of the agency.
A. True
B. False
4. As a federal employee, you are entitled to make copies of software you use in the office for your personal use.
A. True
B. False
5. Unapproved software or unapproved versions of software may conflict with other software.
A. True
B. False

Lesson 5

Communications Security

Overview

This lesson will cover practices to prevent electronic communications equipment against authorized modification and destructive actions performed by internal and external sources.

Goals of This Lesson

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

- state four methods of safeguarding physical devices necessary for electronic communications.
 - state at least two methods each for using file transfer protocol, telnet, World Wide Web, and electronic mail in a secure fashion.
-

Introduction

Communications security involves how an individual computer user interacts with other computers. It is necessary to not only think about your computer individually (passwords, data/software security, etc.) but also its relationship with other computers. Your computer can provide services to other users and similarly, you often request services from other users' computers. It is important to understand how this makes your system vulnerable, not only from malicious users, but from seemingly innocent acts whose repercussions may not be readily apparent.

The following are examples of security breaches that resulted from a lack of communications security.

Robert Morris, a Cornell University student, constructed a program in 1987 based on a standard Unix service called *finger*, which displays information about users presently logged into a computer. He realized that a program based on *finger* could be used as a backdoor into

nearly all Unix computers. After releasing this program on the Internet, a bug in the code caused the program to malfunction, bringing down thousands of computers nationwide and causing millions of dollars in damage.

Teenagers in Denmark, using standard Unix services, gained access to several North Atlantic Treaty Organization computers and were selling classified information to several foreign governments.

NRCS has had its own security breaches. A database was broken into using an easily guessed password causing damage and embarrassment to the agency.

Why is this important to you?

One reason is the large investment that NRCS has made in the collection of technical material (in some cases, worth hundreds of millions of dollars in staff time) makes it vital that measures be taken to protect our resources.

Another reason is that using the communications capability of agency computers in an unsecured manner makes everyone in the agency, not just the individual computer, vulnerable. The previous reasons are very important but one additional reason that is important to you personally is that you, as an individual, can be held personally responsible for using communications technology in inappropriate ways.

Physical Devices and Network Services

Communications security encompasses both the physical devices that connect your computer to others and the different services that your computer offers once you are connected. Having the ability to communicate with other computers exposes NRCS and its computer systems to security risks. Communications security means that actual communications are secure and the ability to communicate is readily available. It is not enough to simply ensure that the actual communication is secure; making certain that the user has the means to communicate when desired is important as well. Denial of service, or keeping the user from communicating, is a popular attack on computers.

Physical Devices

Physical devices include *modems, routers, hubs, and other FIP equipment* used for electronic communications. The following guidelines should be considered when using these physical devices.

Modem installation requires IRM prior approval. Why?

Installation of a modem provides an open door to your computer. Before we expose a computer to the outside world, it is important to secure the computer as much as possible. If a modem connection is made to a computer without local IRM's knowledge, that computer becomes a threat to other computers that

it can reach. It also exposes any data or software on that computer to potential harm. Further, modem connections can be used to breach a *firewall*—a combination of hardware and software that has as its sole purpose the protection and isolation of an interior network from outside threats. Modem connections bypass the firewall or any other security and are thus potentially serious breaches.

Users should not connect to any non-USDA contracted Internet Service Providers (ISPs) via modem from any NRCS system unless all data transmitted including login ids and passwords are encrypted. Why?

For the same reasons stated above. First, it is against regulations to use private ISP's for Government business. Second, it exposes the NRCS computers to a large amount of risk.

Modems will be configured to drop the line if the session is interrupted. Why?

If the line is not dropped, the next person calling the modem is allowed to pick up where the last person using the modem left off without a different username or password. The second user would be given a prompt allowing them to assume the guise of the last person.

Modems or routers will not be reconfigured by unauthorized users. Why?

Modems and routers are often configured with security features. Reconfiguring them by untrained users might result in the loss of some of those features.

Default router passwords issued by the vendor need to be changed by authorized users.

Modem phone numbers will not be given out by users without the authorization of IRM. Why?

If someone knows your modem's phone number, they may try to break into your

system. If the phone number is unknown, access is much more difficult.

Physical connections to the network hub will be added only by authorized personnel. Why?

Each computer added to the hub should be individually set up and secured properly.

Users must ensure proper disconnection of modem when dial-up connection is complete. Why?

Proper disconnection from the system means that the next user will be able to connect properly.

Access to physical communication devices will be restricted and when feasible, housed in a secure area. Why?

Protection of the means of obtaining communications is as important as communicating in a secure manner.

Network Services

Network services is system software that enables a networked computer to communicate with other networked computers including file transfer protocol (ftp), e-mail, telnet, World Wide Web access and browsing, and file sharing, etc.

Safeguard all logins and passwords. Why?

Constructing and protecting a good password will give you the biggest bang for your buck in securing network services. Methods for choosing a good password have already been covered.

Access to remote sites will be for government business and research purposes. Why?

Visiting inappropriate sites may cause embarrassment to the government and to you personally. Whenever you visit a site, by whatever network service you choose you leave behind a record of your visit. This record can be used to track down

the computer that was used to make the visit.

Users should not establish or reconfigure anonymous file transfer protocol (ftp) sites. Why?

Establishment of this service makes a computer vulnerable to attack from malicious users.

Users should not place inappropriate material on any NRCS computer, nor will they use NRCS resources to place such material on non-NRCS computers. Why?

Placing inappropriate material on an NRCS computer is at the very least embarrassing and at the most, theft of services. Some material may also be illegal, opening the user to criminal action. NRCS computer equipment can be used for limited personal use.

Users should not download unauthorized material using any NRCS computer. Why?

This is the flip side to the previous rule above. In the same way we do not want you to use an NRCS computer to place inappropriate material elsewhere, we do not want you to bring inappropriate material from other computers to NRCS computers. This constitutes a misuse of Government property.

Password-remembering features of ftp or telnet sessions will not be used.

Why?

If the password-remembering feature on your ftp or telnet client is turned on, you have effectively given away your username and password to anyone who sits down at your computer. This can place your own files in jeopardy as well as remote files that have been entrusted to you. The computer on the other end cannot tell that it is not really you sitting at the keyboard, so it relies on your username and password.

Users should not place hidden files or change permissions on files once they are posted to an ftp site without the Webmaster approval. Why?

Everything on an ftp site must be visible to ensure that no inappropriate material is being transmitted.

Web browsers, such as Netscape, will be used for business purposes and limited personal use. Why?

Government computers and their capabilities should not be used for commercial business or profit. This constitutes a misuse of government property.

Users should not post documents to the Web server nor establish home pages without the concurrence of the Webmaster. Why?

The Webmaster is the person who has overall responsibility and accountability for maintaining the Web site. Posting documents without the Webmaster's concurrence is risky for two reasons. Inappropriate material may be inadvertently posted. The person posting the document may do so in a manner that compromises security for the network and makes it vulnerable to attack.

Users should not alter World Wide Web documents on NRCS computers without the concurrence of the Webmaster, nor will they use NRCS equipment to modify WWW documents on non-NRCS computers. Why?

Users are required to obtain the Webmaster's concurrence before posting a document. If the document is altered, new concurrence must be obtained to ensure that the new document also conforms to regulations. Similarly, users should not alter documents on non-NRCS computers.

Users should not export file systems without authorization and will consult with your state IRM to establish the

level of access needed for exported file systems. Why?

When a file system is exported, the default format most often used results in making it readable and writeable universally. As a consequence, anyone on the Internet anywhere in the world can mount the file system on their own computer and make changes to your files without your knowledge or permission. They could use this access to gain further privileges on your computer. Even with file systems exported only to trusted computers, it is important that restricted privileges be granted.

Example: Suppose a database is exported. If a user only needs to read, not modify data, then the user should only be granted read privileges.

E-mail will not be used for the transfer of inappropriate material. Why?

It is illegal to use electronic communications for commercial purposes, to harass users, and to transfer inappropriate material.

A lockable screen saver program should be employed on personal computers. Why?

In both these instances, it is easy for someone to pretend to be you. A lockable screen saver will make this harder. When you get up from your computer, you should secure it. A lockable screen saver can do this fairly conveniently. It is not foolproof, obviously, but it makes it harder for others to pretend that they are you.

Users should not run executable programs received as e-mail attachments. Why?

The following example should suffice. In the spring of 1997, a bogus e-mail was circulated across the Internet. The message said that the attachment to the e-mail message, a file called AOL4FREE.COM, would give the user a free America On-Line account. All the

user had to do was execute the program. Instead of getting a free account, all files on the hard disk were deleted and a rude message informed the user of his gullibility.

used for communications, the file transfer protocol (FTP) and Telnet. The security practices discussed in this lesson should be understood to ensure good data communications security.

Summary

In this lesson, we learned of some vulnerabilities of physical devices

Questions for Self-Study—Lesson 5

1. You can access a World Wide Web site for personal monetary gain when:
 - A. you are working late.
 - B. on weekends.
 - C. on your lunch hour.
 - D. Never

2. Enabling the password-remembering features of your browser:
 - A. allows someone to more easily pretend they are you to other computers.
 - B. is permissible during business hours.
 - C. should be used when you cannot remember your password.
 - D. is not a big deal.

3. State four methods of safeguarding physical devices necessary for electronic communications.

4. State at least two guidelines each for securing File Transfer Protocol (FTP), Telnet, World Wide Web, and electronic mail.

Lesson 6

Physical Security

Overview

This lesson will cover practices that should be performed to ensure proper protection of computer equipment and software.

Goals of This Lesson

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

- provide physical security for NRCS hardware.
- provide physical security for NRCS media.
- recognize vandalism or theft of equipment and the procedure for reporting such acts.

Introduction

Until now, we have been emphasizing the aspects of Federal Information Processing (FIP) security but we must not overlook the fact that information processing is accomplished using physical supplies such as computer hardware, floppy discs, CD-ROMs, and paper documents. Their misuse can seriously compromise security.

This section is intended to make you more aware of the threats to NRCS hardware and media and the actions you should take to improve physical security. When you have completed this section, you will be able to provide physical security for NRCS hardware, provide physical security for NRCS media, and recognize vandalism or theft of equipment and the procedure for reporting such acts.

A secure environment for the physical protection of computer equipment, software, media, and data is essential. Physical security is the process of creating that secure environment. Protect your work area by challenging and

assisting people who do not belong in the area.

Physical Security

Physical security assures that equipment and media are available to all authorized users and protected from all unauthorized users. As we go through this lesson, we will emphasize the three classes of threats to equipment. They are:

- unauthorized access
- unintentional damage
- intentional damage or theft

Hardware

Computer equipment has become essential to the functions of NRCS and must be protected. Let's look at protection procedures in light of our threats.

Unauthorized access

All levels of NRCS deal with information that is sensitive. It may be subject to the privacy act; it may be procurement sensitive; it may be business sensitive. Just as we protect paper information from prying eyes, we must also protect

this information when it resides on a computer. We can help protect our data by denying unauthorized people access to our equipment.

The following precautions will minimize unauthorized access to NRCS equipment:

Restrict access to NRCS equipment to authorized users only. This can be accomplished by placing equipment, such as, network servers and routers in locations where unauthorized people cannot go.

Equipment in public areas should be placed in a way that minimizes the risk of unauthorized access. The screen of a workstation should be placed so that a customer cannot see the screen without your explicit permission.

Log off the computer, when you are not physically present. If you need to leave your workstation, either shut down the system or activate a password protected screen saver.

Unintentional Damage

NRCS probably loses more equipment to unintentional damage than it does by any other means. To minimize unintentional damage, observe the following guidelines:

Place equipment in a location that minimizes its vulnerability to accidental and/or environmental damage.

Protect equipment by using surge protectors or an uninterruptable power supply (UPS).

Ensure that the equipment is properly installed and ventilated.

Keep food, drink, and smoke away from your equipment.

Treat laptop computers with care.

When damaged, they are very expensive to repair.

Refrain from introducing any unauthorized hardware or telecommunication devices or modifying any configuration without proper approval from the Information Technology Manager.

Intentional Damage or Theft

Observing the following will decrease the susceptibility of intentional damage or theft.

Secure all laptops during non-business hours and when not in use.

When feasible, physically anchor all equipment that is located in public accessible areas.

Ensure there is no easy path of flight between the equipment and the exit. This will help deter impulsive thefts.

Be especially careful when traveling with a laptop computer. A laptop computer is very marketable. Do not leave your laptop turned on and unattended. There are many schemes, some ingenious, to separate you from your laptop.

Security Incident Handling Procedures

When an employee suspects an attack, the security coordinator with responsibility for the employee's location is to be informed.

The security coordinator will then inform the state information resource manager about the incident.

After that, the security coordinator or State Information Resource Manager will inform the security officer and one of the deputy security officers. The security officer or deputy security officer discusses with the agency's technical support personnel the appropriate actions to take.

When a course of action has been determined, the security officer or deputy security officer discusses the needed action with the state security coordinator.

The state security coordinator discusses the course of action with computer personnel in the office where the incident occurred.

The computer personnel in the office verify whether an actual security incident occurred. If an actual security incident occurred, the office computer personnel will perform the needed course of action to eliminate the intrusion or attack.

The office computer personnel inform the state security coordinator and the security officer that the corrective action was performed. If an actual security attack occurred, then the security officer or deputy security officer informs the System Network Control Center and writes and forwards an incident report to the Office of Cyber Security.

If no security attack or intrusion took place the security officer will inform the Office of Cyber Security that no harm to computer resources occurred.

Information Media

Information can physically reside on portable media, such as floppy disks, CD-ROMs, and magnetic tape. Such media is vulnerable to theft or damage. The consequences can be severe. The loss of a procurement sensitive file can jeopardize the completion of a major procurement. Let's look at media protection in light of our threats.

Unauthorized access

If I can get my hands on your media, I have a very good chance to access your data, no matter how sensitive. In order to minimize unauthorized access to NRCS media, the following precautions should be followed:

Lock up media containing sensitive information when not in use.

Destroy sensitive information before discarding or reusing the media. Note that the "delete" or "erase" commands are not sufficient for this purpose.

- Magnetic tapes must be degaussed (subjected to a strong magnetic field).
- Magnetic disks must be reformatted.
- Optical media (CD-ROMS) must be destroyed.

Store media in an environmentally suitable location.

Unintentional Damage

Do not leave media, including commercial software where it is vulnerable to damage and theft.

Keep media away from damaging conditions such as magnetic fields and heat.

Properly label media. Ensure that the labeling prominently displays the sensitivity of the data.

Handle media carefully to avoid damage. Do not write on media with an instrument that will damage media.

Media containing information essential to the mission of the organization should be duplicated and the duplicate should be stored in a secure off-site location.

Intentional Damage or Theft

NRCS sensitive information can be very valuable to outside organizations and can be a target for theft. The following precautions will minimize that possibility:

Lock up media containing sensitive information when not in use.

When using sensitive media, be careful not to leave the sensitive media unprotected where it can be stolen or damaged.

Consider using encryption if the sensitivity of the data warrants such protection. Then, even if the media is stolen, it still remains a problem to decipher the information on the media. See your IRM coordinator for additional information on encryption. Even if you take all reasonable precautions, there is still the possibility that you will experience theft or

vandalism to NRCS computer equipment or media. Always back-up files on your computer using tapes or diskettes for disaster recovery purposes.

Summary

In this lesson you were presented with examples of unauthorized access, unintentional and intentional damages and theft to computer equipment and media. We should be familiar with the security incident handling procedures for a computer suspected of being comprised.

Questions for Self-Study—Lesson 6

1. You can protect computer equipment by:
 - A. restricting access to authorized users only.
 - B. ensuring equipment is installed in an environmentally suitable location.
 - C. securing all equipment during non-business hours and when not in use.
 - D. All of the above.
2. Laptop computers are especially vulnerable to:
 - A. unauthorized access.
 - B. unintentional damage.
 - C. intentional damage and theft.
 - D. All of the above.
3. Report theft or vandalism to:
 - A. your supervisor.
 - B. your site security coordinator
 - C. Both A and B.
 - D. the national NRCS security officer.

Conclusion

Our computer systems and the information stored on them have great value and need to be managed to the same extent as our more traditional assets, such as vehicles. You would not park a government vehicle in a busy parking lot, go off and leave the vehicle unlocked, running and full of case files. This is basically what is being done with our computer systems.

It used to be that computer security could easily be handled by locking the computer room door. Decentralization of our information technology has placed the management of automated information and its technology directly into the hands of every agency employee, rather than into the hands of a few computer specialists.

As has been shown, our computer systems are subject to numerous threats, such as theft, natural disasters and hacker attack. We can do many things to eliminate threats and reduce our vulnerabilities.

First of all, we need to create an environment that ensures physical security. No equipment or data can be secure if it can be easily stolen or damaged. The communications services that your computer provides must also be protected. This involves using those services safely, as well as safeguarding the devices that allow communication.

Further, the data you put on your computer needs protection, and the software that manipulates it must be legally obtained.

One of the easiest things an individual can do to meet the many threats to our computing systems is to choose a good password and then protect it. Remember the guidelines for choosing and using passwords:

- Choose a password that is easy for you to remember, but difficult for others to guess.
- Don't write down your password or give it to others.
- Change your password every 90 days or at any time that you suspect it has been compromised.

Computer security ultimately depends on what we all do daily, as we use the equipment with which we have been entrusted. Good security practices must be followed at all times. The law requires us to do this and holds us responsible if we do not. Moreover, you have a responsibility to others since all systems can be put at risk by the actions of one careless individual.

Good security is essential and ongoing. You must ensure that the security of your computer system does not degrade over time, as the technology changes, and as staffing or procedures change. **We must never take computer security for granted.**

At this time, please view
“The Best Defense” video.

Answers to Self-Study Questions

Correct answers are in boldface type.

Lesson 1 – Laws, Policy, and Responsibility

1. State the definition of computer security.
Computer security is the protection of the integrity, availability, and confidentiality of automated information and the resources used to enter, store, process, and communicate it.
2. Whose responsibility is computer security?
“Computer Security is Everyone’s Responsibility.”
3. What is a security breach?
A security breach can be defined as an incident where a person obtains access to printed information or a secured area that he/she is not authorized to see, or where a computer program or computer user gains access to computer system that he/she is not authorized to use.
4. Some Federal laws carry a penalty of 10 years in prison and a \$250,000 fine if convicted of a computer security offense.
A. True
B. False

Lesson 2 – Threats and Vulnerabilities

1. Doing periodic backups of files can protect the user from which of the following computer security threats.
A. Power outage
B. Operator error
C. A virus
D. Fire
E. All of the above
2. An example of a natural threat is:
A. High winds
B. Magnetism
C. Viruses
D. Trojan horses
E. All of the above
3. It’s okay to leave your computer logged into a remote computer if:
A. you will only be away for a few minutes.
B. you have a screen saver.
C. you are meeting with someone just a few cubicles away.
D. None of the above.

4. If your area is being threatened by a severe storm (electrical, hurricane, etc.), the following steps should be taken.
 - A. Unplug all computer equipment.
 - B. Move all computer equipment, CD's, diskettes and/or tapes away from the windows.
 - C. Cover all computer equipment.
 - D. If there is time, perform a backup of your system.
 - E. All of the above.**

Lesson 3 – Passwords

1. Which of the following is an acceptable password?
 - A. bunny
 - B. egbD_if**
 - C. kristen1
 - D. None of the above.
2. How can you protect your password?
 - A. Don't tell it to anyone.
 - B. Don't write your password down.
 - C. Don't use personal information.
 - D. All of the above.**
3. We use passwords:
 - A. to protect data.
 - B. to protect computer resources and services.
 - C. to fulfill responsibility to others utilizing shared systems.
 - D. All of the above.**
4. Your local security officer may impose password requirements stricter than those described in this course.
 - A. True**
 - B. False

Lesson 4 – Data and Software

1. Intellectual property rights and copyright laws do not apply nor have any bearing on computers housed in federal office buildings.
 - A. True
 - B. False**
2. NRCS does not approve the use of shareware or public domain software.
 - A. True**
 - B. False

3. NRCS encourages employees to use any software from any source that will enhance the work of the agency.
 - A. True
 - B. False**
4. As a federal employee you are entitled to make copies of software you use in the office for your personal use.
 - A. True
 - B. False**
5. Unapproved software or unapproved version of software may conflict with other software.
 - A. True**
 - B. False

Lesson 5 – Communications Security

1. You can access a World Wide Web site for personal monetary gain when:
 - A. you are working late.
 - B. on weekends.
 - C. on your lunch hour.
 - D. Never**
2. Enabling the password-remembering features of your browser:
 - A. allows someone to more easily pretend they are you to other computers.**
 - B. is permissible during business hours.
 - C. should be used when you cannot remember your password.
 - D. is not a big deal.
3. State four methods of safeguarding physical devices necessary for electronic communications. (Any four of the following will suffice.)
 - A. Modem installation requires IRM prior approval.**
 - B. Users should not connect to any non-USDA contracted Internet Service Providers (ISPs) via modem from any NRCS system unless all data transmitted including login ids and passwords are encrypted.**
 - C. Modems will be configured to drop the line if the session is interrupted.**
 - D. Modems or routers will not be reconfigured by unauthorized users.**
 - E. Modem phone numbers will not be given out by users without the authorization of IRM.**
 - F. Physical connections to the network hub will be added only by authorized personnel.**
 - G. Users must ensure proper disconnection of modem when dial-up connection is complete.**
 - H. Access to physical communication devices will be restricted and when feasible, housed in a secure area.**

4. State at least two guidelines each for securing File Transfer Protocol (FTP), Telnet, World Wide Web, and electronic mail. (Any eight of the following will suffice.)
- A. **Safeguard all logins and passwords.**
 - B. **Access to remote sites will be for government business and research purposes.**
 - C. **Users should not establish or reconfigure anonymous FTP sites.**
 - D. **Users should not place inappropriate material on any NRCS computer, nor will they use NRCS resources to place such material on non-NRCS computers.**
 - E. **Users should not download unauthorized material using any NRCS computer.**
 - F. **Password-remembering features of FTP or Telnet sessions will not be used.**
 - G. **Users should not place hidden files or change permissions on files once they are posted to an FTP site without the Webmaster's approval.**
 - H. **Web browsers, such as Netscape, will be used for business purposes and limited personal use.**
 - I. **Users should not post documents to the Web server nor establish home pages without the concurrence of the Webmaster.**
 - J. **Users should not alter World Wide Web documents on NRCS computers without the concurrence of the Webmaster, nor will they use NRCS equipment to modify WWW documents on non-NRCS computers.**
 - K. **Users should not export file systems without authorization and will consult with your state IRM to establish the level of access needed for exported file systems.**
 - L. **E-mail will not be used for the transfer of inappropriate materials.**
 - M. **A lockable screen saver program should be employed on person computers.**
 - N. **Users should not run executable programs received as e-mail attachments.**

Lesson 6 – Physical Security

1. You can protect computer equipment by:
 - A. restricting access to authorized users only.
 - B. ensuring equipment is installed in an environmentally suitable location.
 - C. securing all equipment during non-business hours and when not in use.
 - D. All of the above.**
2. Laptop computers are especially vulnerable to:
 - A. unauthorized access.
 - B. unintentional damage.
 - C. intentional damage and theft.
 - D. All of the above.**
3. Report theft or vandalism to:
 - A. your supervisor.
 - B. your site security coordinator
 - C. Both A and B.**
 - D. the National NRCS Security Officer.

References

- Albitz, Paul and Cricket Liu, *DNS and BIND*, Sebastopol, CA, O'Reilly and Associates, 1992
- Chapman, D. Brent and Elizabeth Zwicky, *Building Internet Firewalls*, Computer Fraud and Abuse Act of 1986
- Computer Security Act of 1987 (Pub. L. 100-235)
- Costales, Bryan, with Eric Allman and Neil Rickert, *Sendmail*, Sebastopol, CA, O'Reilly and Associates, 1993
- Government Information Security Reform Act
- Garfinkel, Simon and Gene Spafford, *Practical Unix Security*, Sebastopol, CA, O'Reilly and Associates, 1991
- General Manual (GM) 270-IRM Circular No. 2 (Part 403): IRM - Security - Electronic Mail (E-MAIL) System
- Hunt, Craig, *TCP/IP Network Administration*, Sebastopol, CA, O'Reilly and Associates, 1992
- National Information Security Handbook, IRM-270-VI
- National Instruction No. 270-307 - IRM - NRCS Internet & World Wide Web User Policy
- National IRM Manual, Computer Security Section 508
- National IRM Manual, Part 2, Security
- NRCS Policy on Data Protection and Privacy
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources
- Privacy Act of 1974, Sebastopol, CA, O'Reilly and Associates, 1995
- USDA Departmental Regulation DR 3140-1, USDA Information System Security Policy
- USDA Departmental Regulation DR 3140-2, USDA Internet Security Policy
- USDA Departmental Regulation DR 3300-1, Telecommunications, Section 4, Appendix I
- USDA Departmental Manual DM 3440-1, Classification, Declassification, and Safeguarding Information
- USDA Departmental Notice DN3140-8 Securing Sensitive Information on Servers
- USDA Departmental Notice DN3140-6 Gateway and Firewall Policy and Technical Security Standards
- USDA Policy on Software Copyrights

Self-Certification

Computer Security Awareness Training

Directions: Once you have completed this mandatory training, you must document your completion. Please sign and date the form below, remove this page from the manual and forward it to your Human Resources Department. Please provide a copy to your State IRM Coordinator or the individual with those designated responsibilities.

I certify that I have completed the
Computer Security Awareness training.
I have read the Student Manual
and viewed “The Best Defense” video.

Print name: _____

Signature: _____

Date: _____

Location: _____

