

# Annual Cyber Security Education and Awareness Argonne National Laboratory Training Course ESH 223

## I. Introduction

The cyber security program at *Argonne National Laboratory* promotes the safe use of information technology. *Argonne* plays a key role in America's continued leadership in computing sciences. However, the Laboratory must balance the expansion of computing technology with the need to protect its information infrastructure.

## II. ***“Accountability for Cyber Security extends from the Laboratory Director to every employee and user.”***

## III. Objectives

After you complete your annual cyber security refresher, you will be able to:

1. Recognize your role in the cyber security program.
2. Recognize your responsibilities in the cyber security program.
3. Prevent intrusions to your computer system by selecting a good password.
4. Prevent email viruses and worms from entering your system.
5. Prevent computer theft.
6. Report computer incidents properly.
7. Identify the importance of backing your data regularly.
8. Protect the firewall.
9. Identify critical and sensitive information.
10. Prevent computer misuse.

**NOTE:** Because Argonne has distributed computing, cyber security must be a shared responsibility. Players include Laboratory management, the Cyber Security Program Office, various system administrators and the end user.

## IV. Your Role

- Prevent intrusions to your computer
- Detect intrusions on your computer
- Handle and report incidents properly
- Verify that your data is backed up
- Prevent computer misuse

## V. Preventing intrusions

Intrusion prevention includes actions that will prevent an intruder from accessing any data that belongs to you or the Laboratory. Several critical intrusion prevention tactics rely on you.

### 1. Choose a good password that meets DOE guidelines

- Eight (8) non-blank characters
- A combination of :
  - Letters (preferably a mixture of upper and lowercase)
  - Numbers
  - At least one special character in first 7 positions
  - First and last characters must be non-numeric
  - Must not contain your name or username

#### So, what does this mean to you?

- No common words such as dog, cat or mom
- Don't use numerals in the first or last position
- No simple pattern of letters or numbers such as xyz123
- Make your password be at least 8 characters
- Letters Are Upper And Lower Case
- Combo of letters, numbers & special characters (@#%&\*)!
- Not written on paper or post-it notes
- Not imbedded in computer files
- **Do not** share your password
- Change it at least every 180 days

System or network administrators should **never** ask you for your password

Notify your [local CSPR](#) of requests for passwords

For more information check out <http://www.anl.gov/ECT/access/checkpw.html> or simply use your **Password Rules Cube!**

[\\*Check out your choice for a password](#)

[\\*Additional password advice](#)

### 2. Watch out for email viruses and worms

- Forward unsolicited emails to [spam@anl.gov](mailto:spam@anl.gov).
- Do not open or email attachments from unknown sources.
- Do not execute software from unknown sources; the software may contain a virus.
- Do not execute unknown software from known sources; the other individual's computer may be infected with a virus.
- Use virus protection software.

#### What to do if you detect a virus or worm on your system

- quarantine the system (that means, leave it on but put a sign on the monitor to warn against further use)
- call your [local cyber security rep](#)
- wait for a technical support person to come and clean up your system

Far more damage to systems results from users trying to eradicate viruses and worms themselves than from anything else.

**NOTE:** The unusually high number of viruses and worms that have been spreading over the Internet makes it more likely your Windows system will become infected at some time. If it happens, you may receive a message from a virus checking program telling you that it has removed a virus or worm from a message that you sent. Sometimes the message confuses users because they haven't sent a message at the time the virus program has indicated. You should know that many viruses and worms often act independently of the user; they are programmed to send out messages from an infected machine without the user even knowing about the message or that his or her machine is infected. Examples include incidents where Argonne employees were embarrassed because they knowingly and unknowingly broadcast emails with titles such as: "ILOVEYOU", "Here you have, ;o)" (*AnnaKournikova*), "Manwanella".

3. **Employ a password enabled screen saver**
4. **Only accept computer instructions from reputable sources like your system administrator or [CSPR](#). Ignore and do not pass on hoaxes**

## VI. Deter computer theft

Argonne buildings with large common areas regularly experience the theft of components such as keyboards and mice.

### 1. For desktop computers

- Use simple key locks with strong surface mount adapters to prevent equipment theft.
- Lock your office or lab when your computer is unattended for a significant amount of time.

### 2. For laptop computers

Notebook users must be particularly careful on travel. Airports and hotel lobbies are notorious venues for computer theft.

- Purchase [Kensington](#) and [Kryptonite](#) lock down cables.
- Personalize your notebook. (Use mounted identification tags, which can't be removed without damaging the computer.)
- Do **not** save passwords that allow automatic login to systems/websites/intranet sites. (This prevents unauthorized access to these areas in the event of computer theft.)

**Remember:** A thief is less likely to walk off with a computer with someone else's name all over it. Plus, if your laptop is stolen and recovered, it will be that much easier to return it to you.

## VII. Protect Argonne's firewalls

In the past few years the Laboratory has worked very hard to secure its network perimeter against outside intruders. This work includes deploying firewalls, installing electronic intrusion detection systems, and providing strong configuration management guidance. This work has greatly reduced Argonne's external exposure.

### 1. So, what does that mean to me?

Everyday thousands of Argonne employees have direct access to their desktops. This type of access increases the individual user's responsibility for cyber security.

### 2. What could compromise these security measures?

- Bringing in software on diskettes
- Installing unauthorized local modems
- Enabling new software features that bypass the Laboratory's common defenses such as peer to peer file sharing services (Kazaa)
- Downloading software from web or ftp sites
- Installing a wireless access point

These changes can affect not only your local host but also the computers of neighbors.

**NOTE:** Consider carefully your need for a unique screen saver, network file sharing, or electronic mail graphics. In all cases contact your [CSPR](#) before making configuration changes that affect the security posture of all of us.

### 3. Could my home computer be a back door?

**Absolutely!** Argonne incidents are often the result of infected home computers. Many employees use their home computers for work related to the Laboratory.

- Install virus protection software.
  - Pc-cillin is available for free from the CIS Help Desk at 2-9999.
- Maintain your computer.
  - Visit <http://windowsupdate.microsoft.com> monthly.
- Install a home firewall. Use either:
  - A software firewall such as the Windows Firewall available in Microsoft XP or ZoneAlarm, or
  - A network firewall such as a Linksys router behind your cable modem or DSL service.
- Implement home wireless networks with caution!

Obtain a copy of the [Cyber Security for Your Home Machine](#) guide from the Cyber Security Program Office.

## VIII. General Information Protection

Most people readily recognize that their computers store confidential information that is vital for their daily work and for the operation of the Laboratory. Many computers users, however, overlook the fact that confidential data may be exposed as a result of routine activities:

- Paper print outs
- Portable media such as floppy disks, CD-ROMs, memory sticks
- Computers being discarded.

All computers users must take precautions to insure that these low-tech avenues to information exposure are closed.

- Confidential documents should be shredded; not simply placed in a recycling container.

- Electronic media should be erased before being destroyed or submitted to CIS's electronic media destruction program. Please contact your [CSPR](#) or the CIS Help Desk at 2-9999 - Option 2 for guidance.
- Unneeded computers must be sanitized prior to disposal. You must deliver unneeded computers and hard disks to your [CSPR](#) for sanitization and disposal.

## IX. What is Critical/Sensitive Information?

Information or services that must be specially protected from alteration or disclosure because of:

- Financial risk
- Legal risk
- Privacy act
- Official Use Only (OUO)
- Operations Security (OPSEC)
- Unclassified Controlled Nuclear Information (UCNI)
- Essential for day to day operation
- CRADA

These types of information require additional protection. You should contact your [Cyber Security Program Representative](#) if your work involves critical/sensitive information.

## X. How do I identify and report “potential” computer incidents?

You are Argonne's best identification and reporting mechanism. Although system attacks can be identified by monitoring capabilities built into Argonne's computing architecture, the most accurate monitoring capability is yours.

1. The best way to detect intruders is to prepare beforehand. Recognize what is normal behavior of your computing system and then identify the abnormal behavior. You will be aware of “strange and unexplained” things that might happen. These include:

- Unexpected disk accesses
- Unexpected new files
- Unexplained increased disk space usage
- Unexplained open applications
- Unexplained printouts
- Unexplained sluggishness on your system

These things might be the result of normal operation or they may signal an intruder. Intruders and intruder software can operate, if attempted by a skillful attacker, with little consumption of resources. Learn how your computer system generally reacts and identify abnormal behavior

### 2. EXAMPLES

As an example, a user begins to notice that her system is operating very slowly and applications are incapable of working correctly. This may be completely normal behavior due to system maintenance occurring within the computer environment; or this could be an attacker who is now unwisely using her system's resources. This simple identification is not enough information to believe that her system has been compromised. However, during a standard reload of the application, a message appears stating that the computer currently has two users logged in. Simple math tells us that there should only be one user operating this computer because she knows that she is the only registered individual. Now, a series of events have been identified

which may have identified abnormal activity and the [local CSPR](#) should be contacted immediately.

**Another example**, a user receives an email containing an attachment from someone on the Internet. He opens the attachment, which you should never do if you don't know who the email is from, and nothing happens. Keep in mind that any type of attachment can contain a virus or other unsuspected software. His system may now be compromised at this point with either a simple script or an elaborate set of applications. For instance, 3 years ago a software executable was released on the Internet which played a game (a Bart Simpson game to be specific). This game contained a trojan horse which was another application embedded in the game. The user was not expecting the trojan horse when he opened the program. This trojan horse would monitor when the system was no longer attached to the Internet and was not in use. During these times, the trojan horse would call a phone number located in a foreign country that would bill at a rate of \$100 per hour. Understandably so, this person was quite surprised when his phone bill arrived.

### 3. What do I do if I suspect an intrusion?

Report the problem to your [local CSPR](#). Every minute that passes provides more opportunity for the intruder to damage your computer, to use your computer to damage other computers, or allow time for others to find and exploit your vulnerability.

1. Don't panic. Contact your [CSPR](#).
2. Leave the computer ON.
3. Do NOT modify any files.
4. Do NOT close any applications.
5. If you store sensitive or irreplaceable data, disconnect from the network now.
6. Start taking notes of your discoveries and activities. Do not use a possibly compromised system to take notes or communicate about the suspected break in.
7. Quarantine the system (that means, leave it on but put a sign on the monitor to warn against further use).

## XI. Backing up your data

Make sure that your environment and data are part of a regular and reliable backup strategy. Verify that backups are taking place and that your CSPR is aware of your computing environment and data needs. This may involve:

- A local backup of your computer.
- A general file system strategy for your organization.

The backup strategy for your data must consider:

- How quickly your environment must be restored.
- How long must your data be recoverable (i.e. do you need to be able to recover last week's, last month's, or last year's data?).
- Is the data or system critical or sensitive and so required to remain confidential or available?

**NOTE:** A critical part of cyber security is the ability to restore a user's environment and data.

## XII. Prevent computer misuse

The Laboratory provides its employees access to incredible computing and network resources. Many of these resources are generally unavailable to the public, industry, and academia. With that access comes the responsibility to use these resources professionally and in the best interests of the Laboratory. Laboratory computing and networking resources are to be used only for Laboratory-authorized activities. Argonne computer users must not engage in activities that are:

- Illegal
- Prohibited by Laboratory policy
- Likely to incur incremental costs that are not related to the overall missions of the Laboratory.

**NOTE:** Engaging in any of the above prohibited activities can result in disciplinary action up to and including dismissal. (see ANL Policy 6.11)

### 1. Examples of such activity include, but are not limited to:

- Accessing inappropriate internet web sites (for example, sexually explicit or gambling sites).
- Using Laboratory computers to receive, send, generate or store documents related to a personal business.
- Using ANL computers to attack other sites.
- Unauthorized sharing of your password with anyone.
- Violating software license agreements.
- Participating in activities that are illegal or that otherwise may cause disrepute or legal liability for the Laboratory (for example, sending or receiving sexually explicit or racially charged materials). See HR Policy 7400.

### 2. Monitoring

This is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. **By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use.**

Whenever you log in to your computer, you should see this banner. Contact your [CSPR](#) if you don't see it.

## XIII. Top 10 Security Tips

1. Know your local [Cyber Security Program Representative \(CSPR\)](#) and [system administrators](#).

2. Choose complex passwords (numerics, mixed case, special characters) AND keep them secret.
3. Run anti-virus software.
4. Report unusual computer behavior immediately to your [local CSPR](#). For example new pop-ups, programs running that you didn't expect, or suddenly poor performance.
5. Don't use software from unknown sources or open questionable email attachments.
6. Keep your computer physically secure, particularly laptops.
7. Recognize sensitive information, personnel, contractual, Official Use Only, patentable, and protect it.
8. Contact your [CSPR](#) before making configuration changes such as enabling file sharing, installing software, installing a modem, or setting up a wireless network access point. Comply with your divisional policy on making configurations.
9. Make sure your computing environment is part of a reliable backup strategy.
10. Ensure that your computing and networking resources are to be used only for Laboratory-authorized activities.

**XIV.** For more information on Cyber Security Policies & Procedures see Cyber Security Intranet home page at: <http://inside.anl.gov/safetysecurity/cybersecurity/index.html> and/or contact your [local CSPR](#).

## **XV. Computer-related injuries**

A substantial number of computer-related injuries can be prevented with proper knowledge and training, but many workers are unaware of the ergonomic risk factors they face while performing their jobs.

It's a good idea to review your computing work area annually to look at potential ergonomic risk factors.

Take a look at the OSHA website at, <http://www.osha.gov/SLTC/etools/computerworkstations/index.html> for an interactive review of your workstation.

## **XVI. Division specific information**

If you belong to one of the divisions listed below, please go to the appropriate website for more specific information.

**CMT** - <https://www2.cmt.anl.gov/training1/esh223/CST1.htm>