



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Overview

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Introduction

Welcome to Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

This briefing will satisfy the requirement for initial access and mandatory annual training for all persons involved in management, use, or operation of federal computer systems. Users will be required to repeat this course every 12 months. It should take about 30 minutes to complete.

Appropriate use of LLNL's computer resources applies to all users and includes use of Laboratory-owned computers, computer systems, networks, storage, printers, copiers, and portable/mobile devices, as well as all methods of access, whether local or remote.

Internal links are not accessible from the Internet and may not be applicable to all users; these internal links are available from the LLNL network.

A [printable pdf](#) version of this course is available.



Before you begin this course, be sure you are using a **Lab Supported Browser**.

Please use **ONLY** the following browsers:

- **PC:** Internet Explorer or Firefox
- **Mac:** Firefox



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Overview

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Overview

The objective of this briefing is to ensure and promote a safe and secure computer usage environment at LLNL in compliance with DOE requirements.

Topics include:

- Computer, Network, & Peripheral Usage
- Portable Electronic Devices On Site
- Protection of LLNL Computers, Networks, & Peripherals
- How to Prevent & Report Incidents

Direct any questions to the Cyber Security Hotline at +1 925 422 4655 or to your immediate supervisor.

Users must read the following briefing and attest to the agreement before access is allowed to computers. Violations can result in consequences including, but not limited to, loss of access (to computers, networks, peripherals, and media) and administrative disciplinary action.

The acknowledgement will be recorded as a completion in the LTRAIN database for this course.





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Computer Usage at LLNL

Non-Employee Usage

Software & LLNL Computer/Laptop Usage

Computer Access Usage Policies

Do You Know?

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Computer Usage at LLNL

Non-Employee Usage

Software & LLNL Computer/Laptop Usage

Computer Access Usage Policies

Do You Know?

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Computer Usage at LLNL

Computer resources are provided to support the Laboratory's official business on site or off site.

LLNL personnel, contractors, and visitors **may not**:

- Connect personally-owned peripherals to their computers (e.g., speakers, mouse, trackball, usb stick).
- Create, download, view, store, copy, transmit, or retransmit:
 - Unauthorized mass mailings (e.g. chain letters)
 - Sexually-explicit or sexually-oriented materials or images
 - Materials that support gambling, illegal weapons, terrorist operations, or criminal activities
- Infringe on or violate copyright, intellectual property, or software/data export laws.
- Reveal your account password or allow use of your account by others, including family or household members.
- Use LLNL equipment to:
 - Perform intentional circumvention of security rules
 - Cause destruction, denial of service, or unauthorized alteration of software, hardware, or information
 - Cause congestion, delay, or disruption of service to any LLNL system or network (e.g., peer-2-peer transfers)





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Computer Usage at LLNL

Non-Employee Usage

Software & LLNL Computer/Laptop Usage

Computer Access Usage Policies

Do You Know?

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Non-Employee Usage

Non-employees are authorized to use government-owned equipment to perform only the work which has been assigned; only work-related use is allowed.

The Incidental Personal Use Policy does **not** apply to non-employees.

Non-employees must receive authorization before using any LLNL computers or networks. This authorization must be granted by the host program or identified in the contract between LLNL and the person's employer.

[See related policies](#)





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Computer Usage at LLNL

Non-Employee Usage

Software & LLNL Computer/Laptop Usage

Computer Access Usage Policies

Do You Know?

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Software & LLNL Computer/Laptop Usage

LLNL site-licensed software must be used in accordance with software licensing agreements. The system's ISSO may approve the use of public-domain software if such software is required or needed to enhance system operation.

Computer systems, whether off-site or on-site, must be protected using host-based virus and malicious code detection software configured with current virus profiles. Consult your OISSO/ISSO or System Administrator for proper configurations on your computer.

Laptops and media containing sensitive unclassified information **leaving the site must have full disk encryption** (see your ISSO or System Administrator for requirements). Laptops on foreign travel (LOFT) must be loaned from the Institutional LOFT pool: loft@llnl.gov or call 4-Help desk (+1 925 424 4357).

Use discretion when taking laptops and information off site—be aware of carrying sensitive information and don't take anything you don't need.

On a periodic, random, or "for cause" basis, LLNL computers and networks, including other LLNL local area networks (LANs), are monitored and inspected by CSP personnel and their designees--this includes monitoring of electronic mail and instant messaging —**there is no expectation of privacy**.





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Computer Usage at LLNL

Non-Employee Usage

Software & LLNL Computer/Laptop Usage

Computer Access Usage Policies

Do You Know?

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Computer Access Usage Policies



All authorized users (employees, non-employees, and collaborators) must read and abide by the following CSP computer usage policies:

- CSP [Policy 2329](#), Proper Use of LLNL Computers and Networks, describes authorized actions, privacy, software, password, setting, encryption, and protection requirements in order to be granted access.
 - **LLNL employees who are U.S. citizens** are granted access to use LLNL computers;
 - **Non-employees who are U.S. citizens** must receive host/contractual authorization before using any LLNL unclassified computers;
 - **Foreign Nationals (FNs)**, obtain access to LLNL cyber systems from the Visitor Tracking System & CyberTrak which provides Blue Network access through the LLNL Institutional Unclassified System Security Plan hosted by an LLNL employee.
 - FN's are allowed remote access (VPN-B) to the Blue network.
 - Sensitive Country Foreign Nationals (SCFNs) may NOT have remote access to the LLNL Restricted (Yellow) network. See CSP [Policy 2311](#) and CSP [P2021](#) for FN cyber access instructions.



Remote Access

- CSP [Policy 2028](#), Protecting LLNL Employee Remote Computer Systems, reminds us:
 - The security of remote computers is increasingly important to the overall security of LLNL's computer networks.
 - [Symantec Endpoint Protection](#) is available for home use at no charge to employees & collaborators.
 - Unprotected home and travel computers (particularly those with broadband, "always-on" links) are easy targets for viruses, worms, and hackers.
 - The HSPD-12 badge contains Personally Identifiable Information (PII) of the person to whom the card was issued. If the badge holder chooses to put their HSPD-12 badge into a non-government computer, the badge holder assumes responsibility for their PII read by the computer. The security of the non-government computer is the user's responsibility, and failure to maintain security of their system could result in the loss of PII.
 - If a remote system is discovered to be out of compliance with this policy, the user's remote access to the Yellow Network will be suspended and both the employee's Associate Director and the Laboratory's Chief Information Officer (CIO) will be notified.

Incidental Personal Use

- Allowable [incidental personal uses](#) include travel, shopping, medical, or special interest sites. The Laboratory supports the business use of social media technologies such as Facebook, Twitter, LinkedIn and YouTube. ([more information](#))
- LLNL employees must read and abide by the Incidental Personal Use of Unclassified IT Resources section in the [LLNL Personnel Policies & Procedures Manual](#).
- Personal use of LLNL classified computing resources is prohibited.



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Computer Usage at LLNL

Non-Employee Usage

Software & LLNL Computer/Laptop Usage

Computer Access Usage Policies

Do You Know?

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Do You Know?



1. Click on the items below that you as an LLNL employee under the Incidental Use policy **are permitted** to download, view, store, copy, transmit, or retransmit?

Gambling site

Cooking site

Travel site

Chain letter

Social media site

(i.e., Facebook, LinkedIn, Twitter & YouTube)

Shopping site

Pornography site

Medical site

2. Laboratory employees may make incidental personal use of LLNS IT resources if that use meets **all** of the following criteria:
 - Does not involve resources designated for classified systems;
 - Does not involve personal gain;
 - Does not directly or indirectly interfere with Lawrence Livermore National Security, LLC's operation of electronic communications resources;
 - Does not interfere with the employee's work assignment at Lawrence Livermore National Security, LLC;
 - Does not burden Lawrence Livermore National Security, LLC with noticeable incremental costs [de minimus expense];
 - Does not bring discredit to Lawrence Livermore National Security, LLC or cast significant doubt on the employee's reliability or trustworthiness or otherwise affect an employee's ability to work effectively or harmoniously with others; and
 - Does not support outside business activities,
 - Does not involve the creating, downloading, viewing, storing, copying, or transmitting of sexually explicit or sexually oriented materials; or images or materials related to gambling, illegal weapons, terrorist operations, or criminal activities, and
 - Does not violate other laws, or otherwise constitute an unauthorized use under this or other Lawrence Livermore National Security, LLC policies or guidelines.
- a. True
b. False





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

PED Overview

On-Site PED User Privileges

Rules for Limited Area Use of PEDs

Portable Electronic Device Usage when Meeting in Limited Area

Connecting Non-U.S. Government-Owned PEDs

Bring Your Own Device

Do You Know?

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement



[Privacy & Legal Notice](#)
LLNL-WEB-466551

Last updated November 7, 2013

For questions about this course, contact [Brenda Janiro](#).



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

PED Overview

On-Site PED User Privileges

Rules for Limited Area Use of PEDs

Portable Electronic Device Usage when Meeting in Limited Area

Connecting Non-U.S. Government-Owned PEDs

Bring Your Own Device

Do You Know?

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Portable Electronic Devices Overview



Bringing non-government-owned devices into Limited Area buildings is a significant change for LLNL with significant responsibility. Protection of employee and LLNL information assets is paramount to accepting the freedoms and risks that come along with mobility and the communication tools we use.

This segment will present those responsibilities relative to portable electronic devices (PEDs) on site along with related information for employees, hosts, and visitors to LLNL.

Become familiar with the PED stickers, signs, and rules in the likely event you or a visitor carries one!

If there is any question regarding usage, please contact your Organizational Information System Security Officer (OISSO) or Information System Security Officer (ISSO) for guidance.

Please click on the video to hear Sue Marlais, Deputy Chief Information Officer's message.

To set the stage for this mobility connection change, we must understand the LLNL environment, intended use, and restrictions due to the nature of the work we do in the national interest.





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

PED Overview

On-Site PED User Privileges

Rules for Limited Area Use of PEDs

Portable Electronic Device Usage when Meeting in Limited Area

Connecting Non-U.S. Government-Owned PEDs

Bring Your Own Device

Do You Know?

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

On-Site Portable Electronic Device User Privileges

Extension of on-site user privileges for portable electronic devices (PEDs) is associated with responsibilities depending on device, location, and purpose of use.

LLNL requirements for use of electronic devices fall under two categories:

1. U.S. government-owned
2. Non-U.S. government-owned

The [LLNL Controlled Articles and Electronic Equipment Permitted Use Matrix](#) defines which electronic devices may be used on site. Non-U.S. government-owned devices are allowed on site in [Property Protected Areas](#) (PPA), [General Access Areas](#) (GAA), and [Limited Area](#) (LA) buildings. Some devices will have embedded microphones, cameras, wireless, and Bluetooth.

PEDs may not be used for classified information. Stickers ([see the sticker chart](#)) and signs ([see the signage chart](#)) will indicate which devices can be present at on-site locations and during classified discussions.

See [Cyber Security Policy 2026](#) for guidance and [PED Rules & Regulations](#).

Be aware: Employees can connect LLNL computers to their home networks, monitors and printers; LLNL data shall not be stored/transmitted to personal electronic devices with the capability to store/transfer data **unless** the PED is under the Bring Your Own Device program.





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

PED Overview

On-Site PED User Privileges

Rules for Limited Area Use of PEDs

Portable Electronic Device Usage when Meeting in Limited Area

Connecting Non-U.S. Government-Owned PEDs

Bring Your Own Device

Do You Know?

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Rules for Limited Area Use of Portable Electronic Devices

- While inside a Limited Area building, government and non-government-owned portable electronic devices (PEDs) must maintain proper separation from classified computing. For questions about separation, consult your local [Organizational Information System Security Officer](#) (OISSO).
- Security rules require 'stationary' computers and electronic devices to maintain proper separation distance from classified processing. 'Stationary' means the device is on the person while seated at a desk or table, or in its cradle.
- Separation requirements do not apply to incidental, brief proximity occurring while the device is being used in transit.
- Bluetooth headsets and handsets are **NOT** allowed in Limited Area buildings.
- Foreign Nationals (FNs) may **NOT** bring PEDs into a Limited Area building.



REMINDER

No Classified Discussions



Portable Electronic Devices Permitted in this area

Sample reminder sign.
[View additional signs.](#)





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

PED Overview

On-Site PED User Privileges

Rules for Limited Area Use of PEDs

Portable Electronic Device Usage when Meeting in Limited Area

Connecting Non-U.S. Government-Owned PEDs

Bring Your Own Device

Do You Know?

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Portable Electronic Device Usage when Meeting in Limited Area

- If you are hosting a meeting in a Limited Area building, you must ensure proper signage ([see the signage chart](#)) is in place before the meeting begins and remind participants that PEDs may be present and/or specify which PEDs may be present.
- Devices with microphones enabled (not physically disabled) are never allowed during classified discussions.
- LLNL-owned devices with the microphone physically disabled and camera covered may be allowed in classified discussion rooms.
- Cameras must be covered when classified is processed. Software disablement is not sufficient for a camera to be considered disabled. Cameras must be physically disabled or lenses covered with an opaque material.
- LLNL-owned computers and PEDs without approved stickers ([see the sticker chart](#)) are assumed to have wireless, microphone, and/or camera enabled.

Computers and electronic devices with wireless are not allowed inside Top Secret (TS) areas, Sensitive Compartmented Information Facilities (SCIFs), and Special Access Program Facilities (SAPFs).



Sample reminder sign.
[View additional signs.](#)



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

PED Overview

On-Site PED User Privileges

Rules for Limited Area Use of PEDs

Portable Electronic Device Usage when Meeting in Limited Area

Connecting Non-U.S. Government-Owned PEDs

Bring Your Own Device

Do You Know?

Protection of LLNL Computers, Networks, & Peripherals

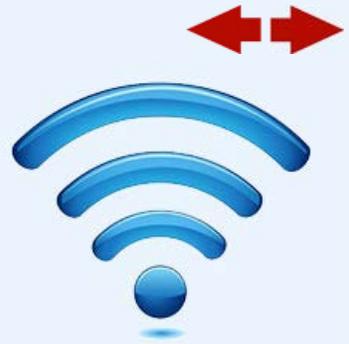
How to Prevent & Report Incidents

Acknowledgement

Connecting Non-U.S. Government-Owned PEDs

Personal Electronic Device On-site Rules

- Non-LLNL-managed computers and portable electronic devices are prohibited from connecting to the restricted network (yellow) and LLNL equipment.
- Non-LLNL-managed computers and portable electronic devices are allowed to connect to the LLNL Guest network (See [Guest Wireless Access Portal](#)) and to non-networked equipment with no storage capability (e.g., standalone projectors). There should be no expectation of privacy while connected to the LLNL network.
- Non-U.S. Government-owned portable electronic devices are prohibited in Vault-type Rooms (VTRs) or Closed Areas (CAs).
- **Employees** may use LLNL-owned computers on the Employee Wireless Network ([Employee Wireless Access Portal](#)) by logging on with an Active Directory (AD) logon.



[Privacy & Legal Notice](#)
LLNL-WEB-466551

Last updated April 9, 2014

For questions about this course, contact [Brenda Ianiro](#).



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

PED Overview

On-Site PED User Privileges

Rules for Limited Area Use of PEDs

Portable Electronic Device Usage when Meeting in Limited Area

Connecting Non-U.S. Government-Owned PEDs

Bring Your Own Device

Do You Know?

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Bring Your Own Device



LLNL has a Bring Your Own Device (BYOD) program in effect providing employees the convenience of using their personal-owned device for official business under these conditions.

- o Voluntary participation.
- o BYOD device is an LLNL employee's personally-owned device that is part of the BYOD program.
- o Tablets and smartphones are the only devices presently in the BYOD program.
- o Personally-owned devices part of the BYOD program are required to store LLNL data in the Mobile Device Management (MDM) container—this means the device is "LLNL managed."
- o BYOD camera or audio recording features may not be used on site except through the MDM container.
- o Participant agrees/signs LLNL usage requirements, policies, and awareness statements (see [BYOD web pages](#) and CSP [Policy 2026](#)).
- o BYOD program follows all other Personal Electronic Device (PED) rules on site.



[Privacy & Legal Notice](#)
LLNL-WEB-466551

Last updated November 7, 2013

For questions about this course,
contact [Brenda Janiro](#).



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

PED Overview

On-Site PED User Privileges

Rules for Limited Area Use of PEDs

Portable Electronic Device Usage when Meeting in Limited Area

Connecting Non-U.S. Government-Owned PEDs

Bring Your Own Device

Do You Know?

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Do You Know?



1. All of the devices below are allowed in General Access Areas, Property Protected Areas, and Limited Areas; which of these devices may remain in a room where a classified discussion is taking place? (check the boxes beside the pictures)



Personal phone



LLNL iPhone or Smartphone



Personal iPhone or Smartphone



LLNL laptop



Personal iPad

2. Non-U.S. government owned devices may be connected to the LLNL "restricted" (yellow) network without prior approval from an OISSO.
 - a. True
 - b. False
3. Computers and electronic devices (cell phones, iPhones, Smartphones, tablets, peripherals) are allowed in Limited Area buildings except in areas and buildings that are posted as prohibited.
 - a. True
 - b. False
4. LLNL-managed iPhones and Smartphones are allowed in classified discussions.
 - a. True
 - b. False



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

Protection of LLNL Computer Systems

What Do You Think?

Think it Through #1

Think it Through #2

How to Prevent & Report Incidents

Acknowledgement



Protection of LLNL Computers, Networks, and Peripherals





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

- Introduction
- Computer, Network & Peripheral Usage
- Portable Electronic Devices On Site
- Protection of LLNL Computers, Networks, & Peripherals
- Protection of LLNL Computer Systems
- What Do You Think?
 - Think it Through #1
 - Think it Through #2
- How to Prevent & Report Incidents
- Acknowledgement

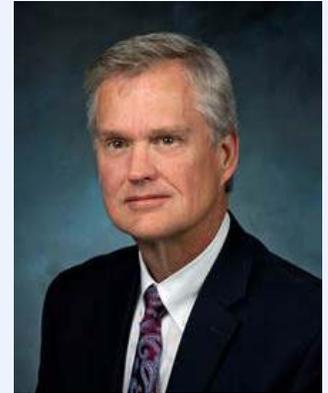
Protection of LLNL Computer Systems



Message from the CIO

LLNL and its employees (YOU) are constantly under attack by hackers and cyber criminals. There is always a balance between how much risk we take versus how secure we make the environment—and it must be a conscious choice!

Doug East, Chief Information Officer (CIO) at LLNL, suggested, “Protect yourself and your information . . . outside world personal information, LLNL classified and unclassified information, intellectual property, export controls . . . you’re helping us protect and defend that data from the hands of those who shouldn’t have it.” Despite our good internal defenses, we are still vulnerable and bad guys can still get into our networks. It takes a long time and many assets to recover from an attack.



Doug East, Chief Information Officer (CIO), LLNL

Pay Special Attention to spear phishing attacks:

- **Email sender** information that mimics the real thing.
- **What it is asking the user to download** or what type of information is solicited.
- **Executable meant to look like a PDF document** which can download malware on your system.

The Cyber Security Program provides a defensive computer posture at LLNL. For assistance, contact the 4-HELP desk at 424-4357 or consult the [RightAnswers](#) knowledge database.

Some of the tools and measures are:
(Click on menu bars below for definitions.)

Authentication

At LLNL, computer users are asked to authenticate using institutionally-managed credentials to keep cyber thieves and hackers from stealing protected information or compromising networks and to provide assurance that the user is authorized and identified when accessing LLNL computer networks.

LLNL institutionally-managed credentials include:

- Official User Name (OUN) and [Personal Access Code](#) (PAC)
- Active Directory (AD) login
- One Time Password (OTP) tokens for remote access
- Multi-Factor Authentication (MFA)

Warning banner

Institutional protection services

Password protection

Encryption/anti-virus protection

Web proxy

Email protection

Information protection - PII

Information protection - UCI and Classified

Physical Protection Measures

We make the environment—and it must be a conscious choice. Doug East, Chief Information Officer (CIO) at LLNL, suggested, “Protect yourself and your information . . . outside world personal information, LLNL classified and unclassified information, intellectual property, export controls . . . you’re helping us protect and defend that data from the hands of those who shouldn’t have it.” Despite our good internal defenses, we are still vulnerable and bad guys can still get into our networks. It takes a long time and many assets to recover from an attack.



Doug East, Chief Information Officer (CIO), LLNL

Pay Special Attention to spear phishing attacks:

- **Email sender** information that mimics the real thing.
- **What it is asking the user to download** or what type of information is solicited.
- **Executable meant to look like a PDF document** which can download malware on your system.

The Cyber Security Program provides a defensive computer posture at LLNL. For assistance, contact the 4-HELP desk at 424-4357 or consult the [RightAnswers](#) knowledge database.

Some of the tools and measures are:
(Click on menu bars below for definitions.)

Authentication

Warning banner

The warning banner warns users at access point of proper use, monitoring, and consequences.

****WARNING**WARNING**WARNING**WARNING**WARNING****

This is a Department of Energy (DOE) computer system. DOE computer systems are provided for the processing of official U.S. Government information only. All data contained within DOE computer systems is owned by the DOE, and may be audited, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DOE computer systems to appropriate authorities. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS AUDITING, INTERCEPTION, RECORDING, READING, COPYING, CAPTURING, and DISCLOSURE OF COMPUTER ACTIVITY.

****WARNING**WARNING**WARNING**WARNING**WARNING****

- Peripherals
- Protection of LLNL Computer Systems
- What Do You Think?
- Think it Through #1
- Think it Through #2
- How to Prevent & Report Incidents
- Acknowledgement

Doug East, Chief Information Officer (CIO) at LLNL, suggested, "Protect yourself and your information . . . outside world personal information, LLNL classified and unclassified information, intellectual property, export controls . . . you're helping us protect and defend that data from the hands of those who shouldn't have it." Despite our good internal defenses, we are still vulnerable and bad guys can still get into our networks. It takes a long time and many assets to recover from an attack.



Doug East, Chief Information Officer (CIO), LLNL

Pay Special Attention to spear phishing attacks:

- **Email sender** information that mimics the real thing.
- **What it is asking the user to download** or what type of information is solicited.
- **Executable meant to look like a PDF document** which can download malware on your system.

The Cyber Security Program provides a defensive computer posture at LLNL. For assistance, contact the 4-HELP desk at 424-4357 or consult the [RightAnswers](#) knowledge database.

Some of the tools and measures are:
(Click on menu bars below for definitions.)

Authentication
Warning banner
Institutional protection services

Preventative protection measures include:

- Vulnerability scanning
- Firewalls
- Intrusion Prevention System (IPS) tools
- Intrusion Detection System (IDS) tools

Contact CSP's Network Security Team: nst@lists.llnl.gov

Computer Systems

What Do You Think?

Think it Through #1

Think it Through #2

How to Prevent & Report Incidents

Acknowledgement

information. It could be your personal information, LANE classified and unclassified information, intellectual property, export controls . . . you're helping us protect and defend that data from the hands of those who shouldn't have it." Despite our good internal defenses, we are still vulnerable and bad guys can still get into our networks. It takes a long time and many assets to recover from an attack.

Pay Special Attention to spear phishing attacks:

- **Email sender** information that mimics the real thing.
- **What it is asking the user to download** or what type of information is solicited.
- **Executable meant to look like a PDF document** which can download malware on your system.

The Cyber Security Program provides a defensive computer posture at LLNL. For assistance, contact the 4-HELP desk at 424-4357 or consult the [RightAnswers](#) knowledge database.

Some of the tools and measures are:
(Click on menu bars below for definitions.)

Authentication

Warning banner

Institutional protection services

Password protection

Password protection includes:

- User awareness of password policies
 - Do not share passwords.
 - Create strong passwords using phrases & symbols.
- Automated rules on creation of passwords that contribute to the effectiveness of password protection
- Consider the following when creating strong passwords:
 - First, select a short phrase. It can be from a favorite song, movie, or book, anything you'll remember.
 - For an example, use "Choosing a strong password is *Easy*."
 - Use only the first letter of each word in the phrase. In the example, this yields "CaspiE."
 - Second, select a single-digit number. Use the last digit of the year you were born, or of your home phone number, or zip code.
 - Finally, select a non-alphanumeric character from the keyboard. (! @ # \$ % & * + ?)
 - One possible example is: **Cas3piE#**



Doug East, Chief Information Officer (CIO), LLNL

What Do You Think?

Think it Through #1

Think it Through #2

How to Prevent & Report Incidents

Acknowledgement

defend that data from the hands of those who shouldn't have it." Despite our good internal defenses, we are still vulnerable and bad guys can still get into our networks. It takes a long time and many assets to recover from an attack.

Pay Special Attention to spear phishing attacks:

- **Email sender** information that mimics the real thing.
- **What it is asking the user to download** or what type of information is solicited.
- **Executable meant to look like a PDF document** which can download malware on your system.



Doug East, Chief Information Officer (CIO), LLNL

The Cyber Security Program provides a defensive computer posture at LLNL. For assistance, contact the 4-HELP desk at 424-4357 or consult the [RightAnswers](#) knowledge database.

Some of the tools and measures are:

(Click on menu bars below for definitions.)

Authentication

Warning banner

Institutional protection services

Password protection

Encryption/anti-virus protection

Entrust is the Institutional standard encryption for email and documentation.

Symantec Endpoint Protection (SEP) is the Institutional standard anti-virus and malware protection software.

Bitlocker for Windows and **FileVault** for Mac are also used for full disk encryption.

takes a long time and many assets to recover from an attack.

Pay Special Attention to spear phishing attacks:

- **Email sender** information that mimics the real thing.
- **What it is asking the user to download** or what type of information is solicited.
- **Executable meant to look like a PDF document** which can download malware on your system.



Doug East, Chief Information Officer (CIO), LLNL

The Cyber Security Program provides a defensive computer posture at LLNL. For assistance, contact the 4-HELP desk at 424-4357 or consult the [RightAnswers](#) knowledge database.

Some of the tools and measures are:
(Click on menu bars below for definitions.)

Authentication

Warning banner

Institutional protection services

Password protection

Encryption/anti-virus protection

Web proxy

The Web proxy:

- Insulates users from the Internet by blocking access to many inappropriate sites, users are still responsible to insure that unblocked inappropriate sites are not accessed.
- Logs all Web traffic.
- **Palo Alto Networks** next-generation firewall provides a secure perimeter for LLNL networks.

Contact CSP's Network Security Team: nst@lists.llnl.gov

Pay Special Attention to spear phishing attacks:

- **Email sender** information that mimics the real thing.
- **What it is asking the user to download** or what type of information is solicited.
- **Executable meant to look like a PDF document** which can download malware on your system.



Doug East, Chief Information Officer (CIO), LLNL

The Cyber Security Program provides a defensive computer posture at LLNL. For assistance, contact the 4-HELP desk at 424-4357 or consult the [RightAnswers](#) knowledge database.

Some of the tools and measures are:
(Click on menu bars below for definitions.)

Authentication
Warning banner
Institutional protection services
Password protection
Encryption/anti-virus protection
Web proxy
Email protection

Email protection includes:

- Anti-spam
- Anti-virus
- Attachment blocking

The Laboratory's policy on incidental personal use of government owned computers allows employees to purchase personal items to be shipped to their home address.

When buying items on-line, it is recommended that employees provide their personal email instead of their LLNL email.

With the prevalence of database hackers, it is important to protect information that identifies you as an LLNL employee, or mistakenly identifies you as a government employee by virtue of your email address ending in ".gov". Using your LLNL email could make you viewed as a valuable asset by adversaries and potentially make you a target.

THERE IS NO RIGHT OF PRIVACY ON LLNL SYSTEMS, this includes monitoring of electronic mail and instant messaging.

Pay Special Attention to spear phishing attacks:

- **Email sender** information that mimics the real thing.
- **What it is asking the user to download** or what type of information is solicited.
- **Executable meant to look like a PDF document** which can download malware on your system.



Doug East, Chief Information Officer (CIO), LLNL

The Cyber Security Program provides a defensive computer posture at LLNL. For assistance, contact the 4-HELP desk at 424-4357 or consult the [RightAnswers](#) knowledge database.

Some of the tools and measures are:
(Click on menu bars below for definitions.)

Authentication

Warning banner

Institutional protection services

Password protection

Encryption/anti-virus protection

Web proxy

Email protection

Information protection - PII

LLNL has standards regarding transmittal, storage, and destruction of data and media.

[Personally Identifiable Information](#) (PII)

- Report loss or unauthorized disclosure of PII immediately to your supervisor, program manager, Information System Security Officer (ISSO), or Organizational Information System Security Officer (OISSO).
- Seek permission of your manager or other authorized manager as required to take electronic or documented personal data off site.
- Encrypt PII when taken off site. Contact your Supervisor, ISSO, or System Administrator for guidance.
- PII must be removed from mobile devices, laptop computers, or the Mobile Device Management (MDM) application(s) on mobile devices when no longer required for current business purposes. A supervisor must approve PII stored on mobile devices for more than 90 days.

Acknowledgement

- **What it is asking the user to download** or what type of information is solicited.
- **Executable meant to look like a PDF document** which can download malware on your system.



Doug East, Chief Information Officer (CIO), LLNL

The Cyber Security Program provides a defensive computer posture at LLNL. For assistance, contact the 4-HELP desk at 424-4357 or consult the [RightAnswers](#) knowledge database.

Some of the tools and measures are:

(Click on menu bars below for definitions.)

Authentication

Warning banner

Institutional protection services

Password protection

Encryption/anti-virus protection

Web proxy

Email protection

Information protection - PII

Information protection - UCI and Classified

Unclassified Controlled Information (UCI)

Your security responsibilities include:

- Guard classified and unclassified controlled information (UCI) from unauthorized access or disclosure
- Do not leave your office or workspace unlocked during off-hours or when it is unattended—log off your computer when not in use
- UCI information must be encrypted on all computers, electronic devices, and ESM taken off-site. Refer to CSP [Policy 2029](#), Encryption of Computers, Electronic Devices, and Electronic Storage Media (ESM) Off-Site.

Classified Information

- Anyone working with classified information must take the online course, CS0115-W, Training for Users of Classified Information Systems
- Employees contact your [OISSO](#), ISSO, or System Administrator; non-employees contact your host for instructions.

Classified /Unclassified Information

- All systems must be protected with a password
- Use Screen Lock controls whenever your computer is unattended

- **What it is asking the user to download** or what type of information is solicited.
- **Executable meant to look like a PDF document** which can download malware on your system.



Doug East, Chief Information Officer (CIO), LLNL

The Cyber Security Program provides a defensive computer posture at LLNL. For assistance, contact the 4-HELP desk at 424-4357 or consult the [RightAnswers](#) knowledge database.

Some of the tools and measures are:
(Click on menu bars below for definitions.)

Authentication
Warning banner
Institutional protection services
Password protection
Encryption/anti-virus protection
Web proxy
Email protection
Information protection - PII
Information protection - UCI and Classified
Physical Protection Measures

Physical protection of LLNL computer systems is bound by location, type of equipment, and type of information processed. See your ISSO for guidance on placement, installation, or movement (e.g., ergonomic evaluation improvements) of any LLNL computer equipment on site.

Both unclassified and classified systems are built to automatically screen lock; however, screen lock controls can be overridden either by an application or unauthorized user action. If your computer does not automatically activate, contact your technical support to have it configured properly. See [Screen Lock Controls](#) for unattended computers/inactivity.

Classified computing components must be identified with a label that has a red and white striped border with black text on a white background. Movement of hardware with this label is restricted. Personnel are not to remove items with this label from their existing security environments. Movement of components with these labels must be completed with the ISSO.

This label is used for marking classified input/output devices (such as Central Processing Unit, drives, and printers). These labels are to be used as a conspicuous external label indicating the highest classification and most restrictive category of the information allowed to be processed by the system/components.

For more information on these labels see CSP IM4337. The Keyboard and Mouse devices do not require marking.

Notice of Classified Use	
Highest level of Data or Software:	Do not remove this item from existing security environment, alter its required security environment, or make any new connections without the permission of the appropriate ISSO/CSSO
<input type="checkbox"/> Secret	<input type="checkbox"/> Restricted Data
<input type="checkbox"/> Confidential	<input type="checkbox"/> National Security Information
Other: _____	
Responsible Organization: _____	Date: _____
Contact your ISSO/CSSO or LLNL Computer Security for questions, problems, or incidents. Ext. 2-4655	



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

Protection of LLNL Computer Systems

What Do You Think?

Think it Through #1

Think it Through #2

How to Prevent & Report Incidents

Acknowledgement

What Do You Think?

How many emails per month do you think LLNL receives? (click on your answer)

[~80,000](#)

[~2 million](#)

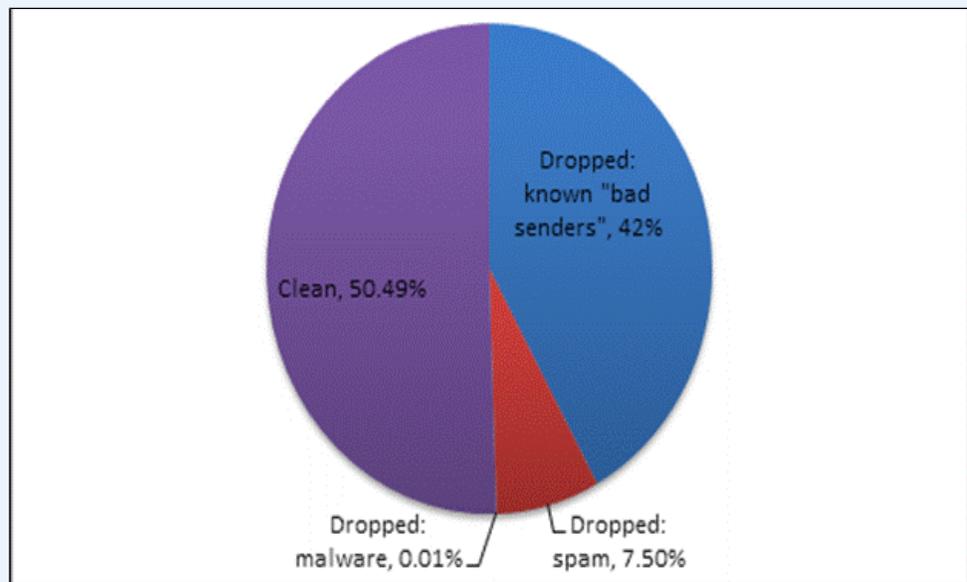
[~16 million](#)

[~53 million](#)



LLNL Email Statistics

Over a typical 30-day period, only about 50% of all emails received are "clean"; the remainder will be dropped by our perimeter defenses and are identified as either spam, known "bad senders", or containing malware.





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

Protection of LLNL Computer Systems

What Do You Think?

Think it Through #1

Think it Through #2

How to Prevent & Report Incidents

Acknowledgement

Think it Through #1



User's vigilance remains vital to the Lab's cyber security. Waves of highly-targeted e-mail attacks, often called spear phishing, are exploiting client-side vulnerabilities in commonly-used programs such as Adobe PDF Reader, QuickTime, Adobe Flash, and Microsoft Office. This is currently the primary initial infection vector used to compromise computers that have Internet access.

Those same client-side vulnerabilities are exploited by attackers when users visit infected Web sites.

Would You Click on This Email?

Why This Email is Suspicious

Date: Tue Feb 26 21:42:53 2008 +0000

From: "James Miller" <miller250@llnl.gov>

Subject: salary information???

To: namenotshown@llnl.gov

Hey,

I thought that salary information was no longer being shared? For some reason the following site has a copy. It seems some one posted it on the net. Check it out <http://blogsphere.mozilla.com>

James



Privacy & Legal Notice
LLNL-WEB-466551

Last updated November 7, 2013

For questions about this course,
contact [Brenda Janiro](#).



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

Protection of LLNL Computer Systems

What Do You Think?

Think it Through #1

Think it Through #2

How to Prevent & Report Incidents

Acknowledgement

Think it Through #1



User's vigilance remains vital to the Lab's cyber security. Waves of highly-targeted e-mail attacks, often called spear phishing, are exploiting client-side vulnerabilities in commonly-used programs such as Adobe PDF Reader, QuickTime, Adobe Flash, and Microsoft Office. This is currently the primary initial infection vector used to compromise computers that have Internet access.

Those same client-side vulnerabilities are exploited by attackers when users visit infected Web sites.

Would You Click on This Email?

Why This Email is Suspicious

Date: Tue Feb 26 21:42:53 2008 +0000

A. From: "James Miller" <miller250@llnl.gov>

Subject: salary information???

To: namenotshown@llnl.gov

Hey,

I thought that salary information was no longer being
B. shared? For some reason the following site has a copy.
It seems some one posted it on the net. Check it out
C. <http://blogsphere.mozilla.com/C1/4.png>

James

A. Do you know the sender?

B. Is salary information shared in this fashion?

C. There is a hidden redirect address in the link that can be viewed if you hover over it with the mouse.

It should be reported using the
Anti-spam toolbox.



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

Protection of LLNL Computer Systems

What Do You Think?

Think it Through #1

Think it Through #2

How to Prevent & Report Incidents

Acknowledgement

Think it Through #2



Because users feel safe downloading documents from trusted sites, they are easily fooled into opening documents, music, and videos that exploit client-side vulnerabilities.

Some exploits do not even require the user to open documents. Simply accessing an infected Web site or opening the infected e-mail message is all that is needed to compromise the client software.

Your computer can be infected without downloading or installing anything - make sure systems are patched, and if something doesn't seem right, report it to your supervisor or use the references provided in the "How to Prevent & Report Incidents" section of this briefing.

Would You Click on This Email?

Why This Email is Suspicious

Date: Mon, 11 Aug 2008 10:57:37 -0700
To: E-line <e-line@lists.llnl.gov>
From: Public Affairs Office <pao@11n1.gov.net>
Subject: CYBER SECURITY REMINDERS

Employees are a key to helping the Laboratory recover from recent attacks as well as thwarting future cyber threats.

To allow Computer Security to ensure networks are secure, employees are asked to click on this link <http://pao-int.11n1.gov.net/patch.html>

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

Protection of LLNL Computer Systems

What Do You Think?

Think it Through #1

Think it Through #2

How to Prevent & Report Incidents

Acknowledgement

Think it Through #2



Because users feel safe downloading documents from trusted sites, they are easily fooled into opening documents, music, and videos that exploit client-side vulnerabilities.

Some exploits do not even require the user to open documents. Simply accessing an infected Web site or opening the infected e-mail message is all that is needed to compromise the client software.

Your computer can be infected without downloading or installing anything - make sure systems are patched, and if something doesn't seem right, report it to your supervisor or use the references provided in the "How to Prevent & Report Incidents" section of this briefing.

Would You Click on This Email?

Why This Email is Suspicious

Date: Mon, 11 Aug 2008 10:57:37 -0700
To: E-line <e-line@lists.llnl.gov>
A. From: Public Affairs Office <pao@11n1.gov.net>
Subject: CYBER SECURITY REMINDERS

B. Employees are a key to helping the Laboratory recover from recent attacks as well as thwarting future cyber threats.

To allow Computer Security to ensure networks are secure, employees are asked to click on this link
C. <http://pao.int.11n1.gov.net/patch.html>

A. Check the sender's address. Note the 11n1.gov.net - the "11n1" is actually numbers, also the domain ends with .net

B. Note the anonymity of the message.

C. Note URL: 11n1.gov.net - the "11n1" is actually numbers, also the domain ends with .net

It should be reported using the Anti-spam toolbox.



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

How YOU Can Help

Phishing

Unsolicited Phone Calls

Getting Help & Reporting Incidents

Acknowledgement



[Privacy & Legal Notice](#)
LLNL-WEB-466551

Last updated November 7, 2013

For questions about this course, contact [Brenda Janiro](#).



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

How YOU Can Help

Phishing

Unsolicited Phone Calls

Getting Help & Reporting Incidents

Acknowledgement

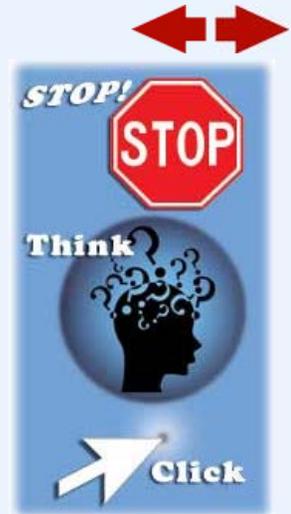
How YOU Can Help

The Internet offers a world of opportunities and is a way of life for us today; yet such convenience in the information age comes with risks. Practice online safety today and every day in your personal and professional life.

- Protect your personal information—it's valuable!
- Protect LLNL intellectual property and sensitive information appropriately—it's in the national interest and it's your job!
- Know who you're dealing with online—look up a physical address and a working telephone number of online vendors.
- Update anti-virus, anti-spyware, and firewall protection regularly.
- Set up your operating system and Web browser software properly and update them regularly—select high enough security to reduce your risk online.
- Protect your passwords—do not share passwords; create strong passwords by using phrases & symbols.
- Know who to contact if something goes wrong online.
- **STOP & THINK BEFORE YOU CLICK!**

Using Social Media and Internet — Be Aware

- Social media sites are common hunting grounds for cyber criminals to use social engineering for nefarious activity.
- Posting personal information (hobbies, vacations, affiliations, practices, opinions) or sensitive job duties can make you a target for social engineering attacks.
- Internet activities make it easy for adversaries to find information about you, your family, your routine or even location-based metadata embedded in mobile photos—remember what you post is public and permanent!
- When using government resources for incidental use, it is highly recommended employees provide their personal email instead of their LLNL email. With the prevalence of database hackers, it is important to protect information that identifies you as an LLNL employee, or mistakenly identifies you as a government employee by virtue of your email address ending in ".gov." Using your LLNL email could lead adversaries to see you as a valuable asset and potential target.
- See [Staying Safe on Social Networking Sites](#) for more security tips.





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

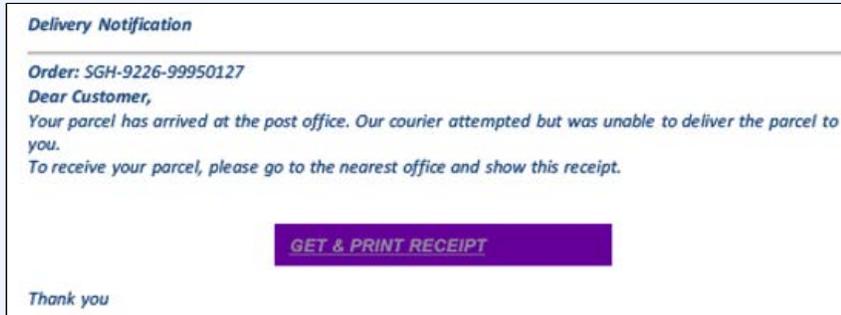
- Introduction
- Computer, Network & Peripheral Usage
- Portable Electronic Devices On Site
- Protection of LLNL Computers, Networks, & Peripherals
- How to Prevent & Report Incidents
 - How YOU Can Help
 - Phishing
 - Unsolicited Phone Calls
 - Getting Help & Reporting Incidents
- Acknowledgement

Phishing

“Phishing” is a virtual trap set by cyber thieves that uses official-looking e-mail to lure you to fake websites, trick you into revealing personal information, or take over your machine and infect a network.

An even more targeted type of phishing is known as “spear phishing” where authentic-looking e-mails are sent to targeted victims typically with some sense of urgency and legitimate explanations as to why they need your personal data or need for you to respond immediately.

On a periodic basis LLNL's Cyber Security Program runs targeted phishing exercises designed to test our training programs and is a method of testing considered a “best practice” in the industry. The email might look like this:



If an employee clicks on a link or attachment, he/she is sent to an educational page that says, “This has been an authorized simulation designed to teach you about spear phishing threats. Please take the time to learn how you can help prevent this type of attack.” The redirect information is kept confidential and may be used for statistical purposes. All SPAM or suspicious email should be reported to spam@llnl.gov

Don't take the bait — [see tips to avoid phishing scams.](#)



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

How YOU Can Help

Phishing

Unsolicited Phone Calls

Getting Help & Reporting Incidents

Acknowledgement

Unsolicited Phone Calls

Criminals making phone calls to lure victims into divulging personal and proprietary information with the intent to gain control of a computer and for monetary gain is a related cyber threat. Some even go as far as looking at company (or social networking) websites to gather background information leading you to believe they are legitimate.

While LLNL-owned and managed computers, peripherals, networks, and devices employ intrusion prevention tools and standards, receiving direct contact phone calls is also a threat.

Protect yourself, your information, and LLNL assets by exercising vigilance when receiving phone calls (at work, at home, and on travel) requesting information about your computer or any personal or proprietary information.

Should you receive a phone call that could be a scam, remember:

- Confirm the caller's identity — ask for a name and number to call back or investigate their web site.
- Never give passwords or information the caller should already have (like your account number).
- Be suspicious and don't trust an offer that's too good to be true, requires urgent action, or is calling at random.

Scenario

You arrive in your hotel room after a long day of travel and delays. The phone rings in your room, and you are greeted by the hotel receptionist who explains that there must have been some system problem when you checked in. He wants to verify your credit card number to guarantee payment of the room expenses.

What is the best action to take?

- a. Ask if this could wait until the morning.
- b. Get out your credit card and give him the number, expire date, and code on it.
- c. Hang up immediately and go to the front desk.





CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

How YOU Can Help

Phishing

Unsolicited Phone Calls

Getting Help & Reporting Incidents

Acknowledgement

Getting Help & Reporting Incidents



[Download this information in pdf format](#)

Incident:	Call:	Email/Web:
Questions or assistance	Cyber Security Program Hotline 925-422-4655	Cyber Security site IT Knowledgebase
Loss or suspected loss of PII	Cyber Security Program Hotline 925-422-4655, or 925-456-4759 (off hours) within 30 minutes of discovery	imt@llnl.gov
Inadvertently placed classified information onto an unclassified system	Your Organizational Information System Security Officer (OISSO)/Information System Security Officer (ISSO) or the Cyber Security Program Hotline 925-422-4655, Off hours: 925-456-4759 immediately	OISSO site
SPAM or Suspicious email	Cyber Security Program Hotline 925-422-4655	Report SPAM email
Clicked on a bad link on an LLNL computer	Cyber Security Program Hotline 925-422-4655 Laboratory personnel working during off-hours, may contact the IMT cell phone at 925-456-4759	imt@llnl.gov
Email specifically mentions LLNL, DOE, is threatening to National Security, or seems suspicious or targeted	Your OISSO/ISSO If you are unable to contact your OISSO, contact the Cyber Security Program Hotline 925-422-4655 Laboratory personnel working during off-hours, may contact the IMT cell phone at 925-456-4759	OISSO site _imt@llnl.gov
Potential security incident - It is the responsibility of all Laboratory employees to immediately report any potential security incident.	Security Incidents Reporting Office (SIRO) 24/7 424-SIRO (7476) PFD Sergeants Office (925-422-7225) during off hours	Security Incident Reporting Office site

See [OnGuard Online](#) for practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

See [Staying Safe on Social Networking Sites](#) for more security tips.



CS0149-W: Proper Usage of LLNL Unclassified Computers, Networks, & Peripherals

Introduction

Computer, Network & Peripheral Usage

Portable Electronic Devices On Site

Protection of LLNL Computers, Networks, & Peripherals

How to Prevent & Report Incidents

Acknowledgement

Acknowledgement



By attesting to this agreement, you are acknowledging that you have read, understand, and agree to comply with the above principles and related policies governing the use of Lawrence Livermore National Laboratory computers, networks, peripherals, and media.

Do you have an Official LLNL User Name (OUN) and Personal Access Code (PAC)?

(Off-site collaborators may select "No.")

Important Information

For help with your PAC, visit the [LLNL PAC Toolbox](#).

In order to complete the acknowledgement, receive a pass or fail confirmation email, and have your completion record in LTRAIN, you must use a **Lab supported browser**. Refer to the chart below to determine the appropriate browser.

In order to receive both the confirmation email and a course completion, you must also have your **pop-up blockers turned off**.

If you need help configuring your browser, contact your Desktop Support group or 4-HELP (424-4357).

Lab Supported Browsers

Platform	Minimum Browser
Windows	Internet Explorer 8.X Firefox 3.6X or greater
Mac	Firefox 3.6X or greater

* Acknowledgement will **not** work with Chrome or Safari.