Cybersecurity Awareness Training Student Guide for

NAL GROUP

Customer Solutions, Simplified.

COPYRIGHT NOTICE

CONFIDENTIALITY NOTICE

Revision History

Revision Date	Effective Date	Description of Change
11/2019	11/01/2019	Initial Release

References

NAL Group Cybersecurity Plan, release date 1/31/2019

Center for Internet Security (CIS) Controls 20: a guidance document that provides recommendations and actions for globally accepted best security practices. This work is licensed under a Creative Commons Attribution Non-Commercial-No Derivatives 4.0 International Public License (https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode)

Table of Contents

Welcome

We are all in this together!

Companies in this age of electronic information are under siege by dishonest and unscrupulous entities who benefit from acquiring the nonpublic information we use and maintain in our business.

Cybersecurity refers to protecting our networks, programs, and electronic data against attack, as well as preventing access to corporate hardware and software, and we need **YOUR** help to make our program a success.

About the Course

This course provides the awareness training needed to protect the information that has been entrusted to NAL Group by clients, employees, and customers.

This course includes:

- An overview of the cybersecurity program
- An explanation of the cybersecurity policies
- The cybersecurity best practices and responsibilities for you to follow

Duration

Although each learner should proceed at his or her own pace, it takes approximately two and a half hours to complete the course.

Terminology

Each section has words or terms that were used in the previous topic and the associated meaning.

Self-Checks

Once you have completed a topic, you will take a short Self-Check. You will be able to enter the Self-Checks answers directly into the training.

Course Assessment

Once you have completed the course, you will complete a course assessment in order to test your understanding of the cybersecurity concepts and company policies that you covered in the course.

The course assessment is integrated into the NAL Group learning management system (LMS) and will be made available to you by the Training Department.

Sign-Off

You are required to provide a signed copy of the Cybersecurity Awareness Training Acknowledgment of Completion form to your HR representative. A copy of this form is included at the end of this document for you to print and sign.

Cybersecurity Awareness

Information security is a vital part of business operations and is built into our business systems and processes to ensure the integrity and confidentiality of our information systems and network data.

Our security activities are designed to be helpful and practical and are aimed at preventing an intrusion instead of reacting to one after an attack. The plan for information security considers the type of business NAL Group has, our requirements and organizational processes, and the risks to our information assets.

NAL Group has taken the necessary protections to safeguard the information systems and the nonpublic information of our clients, employees, and customers by providing them with confidence that the confidentiality, integrity, and availability of their data is ensured. These protections enhance our positive reputation for taking proactive steps to mitigate cybersecurity risks.

This course is meant to get you up to speed on the NAL Group cybersecurity plan and policy, while teaching you how to identify threats and what to do about the threats, from damage caused by the most common events that compromise a system to the most advanced network attacks.

Goal and Objectives

The goal of this course is to provide you with a basic understanding of our cybersecurity program, policies, and what you can do to assist in protecting our nonpublic information.

GOAL

Upon completion of this course, you should be able to demonstrate a basic understanding of:

- The NAL Group cybersecurity program.
- Risk assessment and the threats we face.
- The purpose of our cybersecurity policy.
- The nonpublic information that we must protect.
- Our network and systems security.
- Our device management, data control and access, physical access, and disaster recovery policies.
- Your importance to cybersecurity.
- Your cybersecurity responsibilities and best practices.
- How to recognize and report a cybersecurity event.

OBJECTIVES

Course Checklist

- ☑ Receive the email announcement from the Training Department.
- ☑ Receive the email notification about the training schedule with access instructions.
- ☑ Cybersecurity Program module.
    - ☑ Complete the self-checks.
- ☑ Cybersecurity Policy module.
    - ☑ Complete the self-checks.
- ☑ Employee Responsibilities and Best Practices module.
    - ☑ Complete the self-checks.
- ☑ Course Summary module.
- ☑ Complete the course assessment with a passing score.
- ☑ Provide a signed copy of the acknowledgment of completion form to your HR representative.

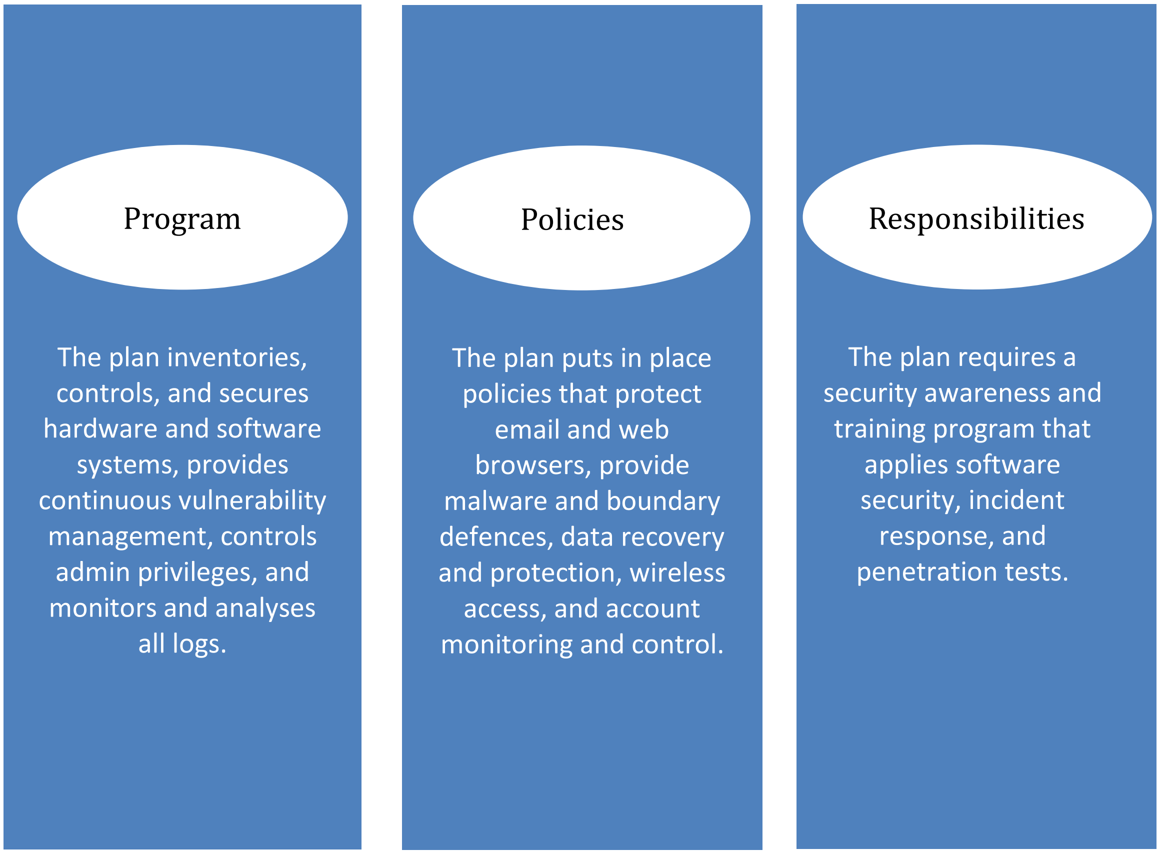
Cybersecurity Program

This section provides an overview of our cybersecurity awareness program and explains what it is that we are protecting and why we are vulnerable to threats and attacks.

Purpose

Our cybersecurity awareness program is designed to protect the confidentiality, integrity, and availability of the nonpublic information stored in our information systems.

Our cybersecurity awareness program evolved from the NAL Group Cybersecurity Plan, which is based on the Center for Internet Security (CIS) Top 20 Critical Security best practices as they apply to our business.



Program

The plan inventories, controls, and secures hardware and software systems, provides continuous vulnerability management, controls admin privileges, and monitors and analyses all logs.

Policies

The plan puts in place policies that protect email and web browsers, provide malware and boundary defences, data recovery and protection, wireless access, and account monitoring and control.

Responsibilities

The plan requires a security awareness and training program that applies software security, incident response, and penetration tests.

Terminology

Term	Definition
confidentiality	The condition that information is not made available or disclosed to unauthorized individuals, entities, or processes.
cybersecurity event	An attempt to disrupt, misuse, or gain unauthorized access to an information system.
cybersecurity risk	The potential that a given threat will exploit vulnerabilities of an information system and thereby cause harm to the organization.
information system	A set of electronic information resources that are established for the collection, processing, maintenance, use, sharing, dissemination, and/or disposition of electronic information.
integrity	The condition of accuracy and completeness.
nonpublic information	Electronic information that is not publicly available.

Self-Check

Test your understanding of our cybersecurity program and general cybersecurity concepts.

What is a computer network?	
Select the box with the correct answer.	
□	A super-computer owned by the government.
□	A web of connected computers and devices.
□	Internet service providers.
□	A security threat.

Why will cybersecurity always be a concern?	
Select the box with the correct answer.	
□	Because the Internet will never go away.
□	Because other countries want what we have.
□	Criminals need them to steal identities.
□	It is a side effect of Internet communication and linked systems.

The following terms are fundamental to any cybersecurity program. Can you match them to their corresponding definitions?
Place the definition letter in front of the correct term.

_____	Cybersecurity event	a. The potential that a given threat will exploit vulnerabilities of an information system and thereby cause harm to the organization.
_____	Cybersecurity risk	b. Electronic information that is not publicly available.
_____	Integrity	c. A set of electronic information resources that are established for the collection, processing, maintenance, use, sharing, dissemination, and/or disposition of electronic information.
_____	Nonpublic information	d. The condition of accuracy and completeness.
_____	Information system	e. An attempt to disrupt, misuse, or gain unauthorized access to an information system.

What are the CIS 20 best practices?	
Select the box with the correct answer.	
☐	A cybersecurity awareness program based on recommendations from employees.
☐	A series of 20 does and don’ts from Norton Security.
☐	A cybersecurity awareness program based on the Center for Internet Security (CIS) Top 20 Critical Security best practices.

Putting the CIS 20 Best Practices into Action

How do we go about putting the CIS 20 best practices into action?

By assessing our risk and providing guidance on how to avoid being vulnerable.

Risk Assessment

The first line of defense is risk assessment. Determining the vulnerability to our networks and identifying the potential for unwanted access to our nonpublic information.

Risk assessment is the overall process of risk identification, risk analysis, and risk evaluation.

Risk Identification	The process of finding, recognizing, and describing risks.
Risk Analysis	The process of comprehending the nature of risk and determining the level of risk.
Risk Evaluation	The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude are acceptable or tolerable.

What is involved with a risk assessment?

Understanding the cybersecurity threats that we face and the measures we can take to protect against, detect, respond to, and recover from those threats.

Risk Assessment	
Inventory Assets	We inventory all of our hardware and software systems and network assets to assess our potential for risk.
Threats	We understand the array of cyber threats that can be used to attack our networks and gain access to nonpublic information.
Protect Against Threats	We provide constant vigilance and management of our networks and assets and limit administrative privileges to protect against threats.
Detect Threats	We monitor our systems and network constantly through the use of logs, event notifications, and other methods to detect threats and vulnerabilities.
Respond to Threats	We analyze the event, assess its impact, and then mitigate any damage.
Recover from Threats	We restore networks and systems to normal operation, verify that the networks and systems are functioning normally, and then remediate vulnerabilities in order to prevent similar events.
Reporting	Our reporting obligations can vary depending upon the nature of the cybersecurity event.

Terminology

Term	Definition
administrative privilege	Restricted access granted to an administrator.
cybersecurity risk	The potential that a given threat will exploit vulnerabilities of an information system and thereby cause harm to the organization.
inventory	A complete list of items.
mitigate	Lesson the gravity or severity of an offense or mistake.
obligations	A course of action to which a person has a duty or commitment.
remediate	Provide a remedy or restore or reverse damage.
restore	Return to a previous state.
vulnerability	The state of being exposed to attack or harm.

Self-Check

Test your understanding of risk assessment.

When a cybersecurity event occurs, we have to respond quickly. Can you sequence our actions into their correct order?	
Place the order numbers (1 – 5) in front of the correct sequence of actions.	
______	Analyze the event in order to determine which information systems are affected, who originated the event, and how the event is occurring.
______	Assess the impact of the event on our business reputation, business functionality, information, and ability to recover.
______	Mitigate the event by containing the damage and then eliminating the components of the event.
______	Report the event to the appropriate authorities, if necessary.
______	Restore information systems to normal operation, verify that they are functioning normally, and then remediate vulnerabilities.

The following terms are fundamental to any Risk Assessment. Can you match them to their corresponding definitions?

Place the definition letter in front of the correct term.

______	Recover from threats	a. We inventory all of our hardware and software systems and network assets to assess our potential for risk.
______	Protecting against threats	b. We restore networks and systems to normal operation, verify that the networks and systems are functioning normally, and then remediate vulnerabilities in order to prevent similar events.
_____	Threats	c. We provide constant vigilance and management of our networks and assets and limit administrative privileges to protect against threats.
______	Respond to threats	d. We analyze the event, assess its impact, and then mitigate any damage.
______	Inventory	e. An attempt to disrupt, misuse, or gain unauthorized access to an information system.

Which of these groups exploits cyber vulnerabilities?

Select the box with the correct answer.

□	Criminals
□	Hackers
□	Foreign governments
□	All of the above

Inventory Assets

What is included in the inventory of assets?

Inventorying hardware and software assets provides important information about our assets that need to be protected.

Hardware assets include:

- Hard copy information on paper.
- Hard copy files stored in cabinets, filing room, or employee desks.
- Computers, servers, mobile communication devices.
- Internal networks.

Software assets include:

- Data displayed or stored electronically, including removeable media.
- Data transmitted by electronic means internally and externally.

Threats

What are the cybersecurity threats to our information systems?

While a system failure caused by malfunctioning hardware or software can certainly cause problems, for the purpose of this training, we will consider that a cybersecurity threat is ultimately attributable to a human root cause.

Your understanding of common cybersecurity threats, all of the devious and sneaky ways that our systems can be attacked, is vital to protecting our assets.

Threat	Description
Account Takeover	A form of identity theft in which the attacker obtains access to a user's account, typically via a backdoor, malware, or phishing, and then makes unauthorized transactions.
Backdoor	A secret method of bypassing the normal authentication or security controls; for example, use of a default password that has not been changed.

Threat	Description
Data Exfiltration	The unauthorized transfer of data from a computer.
Denial of Service (DoS) Attack	An attack where the originator seeks to make a network or system unavailable to its intended users by disrupting its services; for example, by flooding the targeted network or system with an excessive number of illegitimate requests that overloads the network or system, preventing legitimate requests from being fulfilled.
Eavesdropping	The act of secretly listening to a private conversation between systems on a network.
Insider Threat	A malicious threat to an organization that comes from people within the organization who have inside information concerning the organization's security practices, computer systems, or information; for example, the theft of confidential or commercially valuable information.
Phishing	An attempt to obtain sensitive information by disguising as a trustworthy source in an electronic communication; for example, an email or instant message that directs a user to enter details at an illegitimate website that looks and functions in an identical manner to the legitimate site.
Privilege Escalation	A situation where a user with a level of privilege or access is able to increase his or her level of privilege or access; for example, a user fools the system into giving him or her access to restricted data.
Ransomware	A type of malicious software that blocks access to the victim's data or threatens to publish or delete it until a ransom is paid.
Social Engineering	The psychological manipulation of people into performing actions or divulging sensitive information; for example, the impersonation of a trusted contractor or customer.

Threat	Description
Spoofing	A situation in which a person or program successfully masquerades as another by falsifying data; for example, the creation of an email message with a forged sender address.
Tampering	A malicious modification of software or information.

*In 2017, the Nigeria-based **Business Email Compromise (BEC) attack** hit over 50 countries, targeting more than 500 businesses, predominantly industrial companies. The **phishing scam** prompted recipients to download a **malicious file**. When the file was downloaded, **malware** would gain authorized access to business data and networks.*

Source: Small Business Trends: *10 Phishing Examples in 2017 that Targeted Small Business*

*On May 12, 2017, **WannaCry exploited** a weakness in Microsoft's operating systems to deliberately infect computers. When the worm was infiltrated, it encrypted the infected operating systems, rendering them unusable. The hackers subsequently demanded a ransom for unlocking the encryption. Small businesses with a void of up-to-date IT infrastructure were particularly exposed to the WannaCry attack.*

Source: Small Business Trends: *10 Phishing Examples in 2017 that Targeted Small Business*

Terminology

Term	Definition
attack	To take aggressive action against a person or cyber network.
attributable	Regarded as being caused by.
identity theft	The act of stealing identifying information to gain unauthorized access to assets.
malfunctioning	A process or piece of equipment fails to perform satisfactorily.
malicious	Intending to do harm.
originator	A system or someone who creates or initiates something.
removeable media	Portable means of transferring data, such as a flash drive or external hard drive.
system failure	A set of things working together as part of an interconnecting network that is no longer functioning.
transfer	The act of moving data from one place to another.
transmitted	Passed on from one person or place to another.
trustworthy source	Person or network that provides reliable and honest information.
unauthorized	Not having official permission or approval.

Self-Check

Test your understanding of threats.

Eavesdropping is the act of secretly listening to a private conversation between systems on a network.	
True or false?	
□	TRUE
□	FALSE

Backdoor is a term that refers to a secret meeting of thieves behind the building.	
True or false?	
□	TRUE
□	FALSE

Select four types of cybersecurity threats to our information systems.	
Click the boxes with the correct answers.	
□	Tampering
□	Electricity failure
□	Spoofing
□	VPN ware
□	Ransomware
□	Malfunction of a server with data
□	DoS Attack
□	All of the above

Protection from Threats

What measures have we put into place to protect us from these threats?

We have basic safeguards in place that are appropriate for the size of our organization to improve our cybersecurity.

Preparation is Essential

At NAL Group, preparation is essential for the protection of our networks and nonpublic information, we:

- ❖ Know how our network is structured, what systems we are running, and what data we are storing.
- ❖ Focus on implementing and improving the security controls that are most effective for our specific needs and resources.
- ❖ Create and maintain regular and systematic backups of important information.
- ❖ Plan for the unexpected.

Prevention is Critical

Prevention is critical to the safekeeping of our network and always better than trying to recover after an attack.

- ❖ Implement and maintain strong access controls.
- ❖ Patch network, system, and application vulnerability.
- ❖ Educate our employees about cybersecurity threats and security policies and practices.
- ❖ Create security-conscious policies and procedures.

By the way, we also require our third-party service providers that have access to or are provided with our nonpublic information to have the same requisite preventive measures in place for their networks and systems.

Controls

Let’s examine the difference between access controls and security controls.

Access Controls refer to the selective restriction of access to networks, systems, software, data, or physical areas; for example:

- ➢ Single-department access
- ➢ Single-person access
- ➢ Limited use of administrative privileges
- ➢ Limited number of users with remote network access
- ➢ Locked doors and entry control

Security Controls refer to safeguards or countermeasures to avoid, detect, counteract, or minimize cybersecurity threats; for example:

- Strong passwords
- Antivirus software
- Data encryption
- E-mail filters
- Firewalls
- Intrusion detection systems
- Network and application logging
- Virtual private networks (VPN)

Detecting a Cybersecurity Event

How do we detect a cybersecurity event?

We monitor our networks and systems for any act or attempt—successful or unsuccessful—to gain unauthorized access to, disrupt, or misuse our information systems or the nonpublic information stored on them. This includes the implementation of hardware, software, and procedural mechanisms that record and report activity on our networks and systems.

Responding to a Cybersecurity Event

How do we respond to a cybersecurity event?

We analyze the event, assess its impact, and then mitigate any damage.

Analysis

- Which networks, systems, or applications are affected?
- Who or what originated the event?
- How is the event occurring (the attack method and the vulnerabilities that are being exploited)?

Impact Assessment

Impact	Critical Questions that Determine the Level of Risk
Business Reputation	• Do we need to notify a regulatory company? • Do we need to notify the public or our clients?
Business Functionality	• How will the event impact the existing functionality of the affected systems? • What is the likely future functional impact of the event if it is not immediately contained?
Confidentiality, Integrity, and Availability of Information	• How will the event impact our overall mission? • How will the event affect other organizations, if any of the affected information pertains to an affiliate organization?
Recoverability from the Event	• What amount of time and resources are required to recover from the event? • Does the event require more resources than what we have available? • Does it make sense to spend time and resources on a drawn-out resolution effort? • Would a drawn-out resolution effort ensure that a similar event does not occur in the future? • Is the effort necessary to recover from the event worth the value of the required time and resources? • Is it possible to recover from the event? For example, if the confidentiality of sensitive information has already been compromised.

Mitigation

First, we limit the damage caused by the cybersecurity event and prevent any further damage from happening. This containment provides us with time to develop a specific recovery strategy.

Second, we eliminate components of the event, such as deleting malware or disabling breached user accounts, as well as identifying and mitigating all of the vulnerabilities that were exploited.

Recovering from a Cybersecurity Event

How do we recover from a cybersecurity event?

We restore networks and systems to normal operation, verify that the networks and systems are functioning normally, and then remediate vulnerabilities in order to prevent similar events.

The road to recovery can include any of the following actions:

- Rebuilding systems from scratch.
- Restoring systems from clean backups.
- Replacing compromised files with clean versions.
- Installing patches.
- Changing passwords.
- Strengthening network security.
- Implementing higher levels of network monitoring or system logging.

Recovery can be performed in a phased approach so that remediation steps are prioritized:

- Early phases increase the overall security with relatively quick, high-value changes to prevent future events.
- Later phases focus on longer-term changes and ongoing work to keep us as secure as possible.

Reporting Obligations

What are our reporting obligations?

Our reporting obligations can vary depending upon the nature of the cybersecurity event and only undertaken by management. When an event occurs, we might take any of the following actions:

- Consult our legal counsel.
- Review the reporting requirements of applicable state laws and regulations.
- Notify the carriers whose policyholders might have been affected by the event.
- Notify individuals, regulatory agencies, and/or law enforcement, if required.
- Inform the public, if required.

When notification is required, we provide a report to the appropriate entity as soon as possible but no later than 72 hours from the qualifying event.

Terminology

Term	Definition
access	A means of approaching or entering a restricted area.
antivirus	Designed to detect and destroy computer viruses.
backups	A reserve version.
countermeasures	An action taken to counteract a danger or threat.
encryption	The process of converting information or data into a code, especially to prevent unauthorized access.
firewall	A part of a computer system or network which is designed to block unauthorized access while permitting outward communication.
mitigation	The act of reducing the severity or seriousness of something.
patch network	A small piece of code inserted into a program to improve its functioning or to correct an error.
preparation	To make ready for use or consideration.
prevention	The act of stopping something from happening.
safeguards	A measure taken to protect someone or something or to prevent something undesirable.
security conscious	Taking reasonable measures to ensure networks are not vulnerable to threat or attack.
systematic	Done or acting according to a fixed plan or system, methodical.
vulnerability	The quality or state of being exposed to the possibility of being attacked or harmed.

Self-Check

Test your understanding of risk assessment.

We create and maintain regular and systematic backups of important information.	
True or false?	
☐	TRUE
☐	FALSE

At NAL Group, preparation is essential for the protection of our nonpublic information.	
Select the actions that are part of preparation.	
□	a. We patch network, system, and application vulnerability.
□	b. We know how our network is structured, what systems we are running, and what data we are storing.
□	c. We plan for the unexpected.

Can you spot the difference between an access control and a security control? Identify which of the following are access controls and which are security controls.	Access Control	Security Control
Single-department access	□	□
Antivirus software	□	□
Limited use of administrative privileges	□	□
Data encryption	□	□
Email filters	□	□
Limited number of users with remote network access	□	□
Firewalls	□	□
Locked doors and entry control	□	□

Risk assessment is the overall process of risk ____________________, risk ____________________, and risk ____________________.	
Select the three correct terms to complete the statement.	
□	Protection
□	Identifying
□	Detection
□	Analysis
□	Authorization
□	Evaluation

Optional Learning Activities

In this topic, you learned about the cybersecurity threats to our information systems. Refer to the following resources where you will find some interesting articles about how some of those threats have played out in the real world. Check them out at your leisure.

- From Marketplace®: *A new form of ID theft: account takeover* (audio).
- From Small Business Trends: *10 Phishing Examples in 2017 that Targeted Small Business*.
- From The Guardian: *DDoS attack that disrupted Internet was largest of its kind in history, experts say*.
- From Tripwire: *The 5 Most Significant DDoS Attacks of 2016*.
- From Wikipedia: A screenshot of the WannaCry ransomware screen.

Cybersecurity Policy

This topic describes the cybersecurity policies that all employees must follow.

Purpose

Our cybersecurity policy sets forth our policies and procedures for the protection of our information systems and nonpublic information stored on those systems.

It is based on our cybersecurity risk assessment and addresses the following areas, most of which we will discuss in this section:

- Nonpublic information
- Network and Security Systems
- Device Management
- Data Control and Access
    - Internet Control and Access
    - External Control and Access
- Disaster Recovery and Business Continuity

Nonpublic Information

Why is nonpublic information so important?

As you learned in the last section, nonpublic information is electronic information that is not publicly available. Nonpublic information shall be accorded the highest level of security and confidentiality by all of us at NAL Group.

You are required to report all actual or potential unauthorized access to, use of, or disclosure of nonpublic information to the Help Desk immediately.

The examples provide an idea of the harm disclosing nonpublic information can cause and the potential consequences.

Nonpublic information is all electronic information that is not publicly available and is:

- Business-related information that the unauthorized access to, disclosure of, or use would cause an adverse material impact to our business, operations, or security.

  Example – Debbie works in the legal department and is working on a contract to enable her company to take over a large account from a competitor, but it is not public information yet. Repeating this information to someone who would buy stock on the assurance that it will go up when the announcement is made would constitute an SEC violation of an unfair advantage in the investment world, known as insider trading. Highly illegal and punishable by incarceration. Ask Martha Stewart!

- Personal identification information which can be used to identify an individual:
  - First initial/name and last name
  - Social Security Identification number (SSI)
  - Passport number
  - State-issued identification card number
  - Driver's license number
  - Non-driver identification card number
  - Financial account number
  - Credit or debit card number
  - Any security code, access code, or password that permits access to a financial account
  - Biometric record

  Example – Jim works in the copier room. One day he noticed that a repair man working on one of the copiers was making copies of the data stored in the machine, including documents from Human Resources with employee names and SSI numbers.
  This is an example of the theft of electronic nonpublic information. Remember, it could be your identity that is stolen and impacts your financial status.

- Protected health information (PHI), in any form or medium created by or derived from a health care provider or an individual and that relates to:
  - The past, present, or future physical, mental, or behavioral health or condition of any individual or a member of the individual's family.
  - The provision of health care to any individual.
  - Payment for the provision of health care to any individual.

  Example – Mary works in the Human Resources department and is privy to all the employee files. One day Mary was sending information to an insurance provider and accidentally included an employee's health records file that she had sitting on her desktop.
  Although Mary didn't do it deliberately, the results are the same, the insurance provider now has information it is not entitled to about an employee. This is a violation of the Health Insurance Portability and Accountability Act (HIPAA) laws and could result in a limitation or lack of coverage for the employee, a violation of the company policy on handling nonpublic information with repercussions for Mary, and a fine for the company.

Network and System Security

What is meant by network and system security?

For the purpose of this training, a network is the set of servers, computers, and other devices that are interconnected in the company called an intranet. The intranet is connected to the external Internet. The system is the software running on those servers, computers, and other devices that allow the devices to input, output, process, and store data. The network and system security are the defense put into place to protect the network and software from intrusion, threat, and attack from the Internet.

Our cybersecurity policy defines how we protect our information systems and the nonpublic information stored on them:

- We ensure that only licensed software applications or operating systems are added to the NAL Group authorized software inventory.
- Our boundary monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- Deploy network-based Intrusion Detections Systems (IDS) sensors to look for unusual attack mechanisms and detect compromise of these systems at each of the NAL Group network boundaries.
- Unauthorized software is either removed or the software asset inventory is updated as soon as possible.
- Ensure that network engineers use a dedicated machine for all network administrative tasks or tasks requiring elevated access that is segmented from the primary network and not allowed Internet access.
- We physically or logically segregate systems to isolate and run software that is required for business operations but might incur higher risk for the NAL Group.
- A Secure Sockets Layer (SSL) provides communications security over our computer network, which is used when entering passwords or exchanging nonpublic information.
- Email filters remove spam and computer viruses.
- Operating systems (OS) and antivirus applications on our servers, desktops, laptops, and mobile devices are kept up to date.
- Backups are encrypted and password protected.

As mentioned, we monitor our networks and systems for any act or attempt to gain unauthorized access to disrupt or misuse our information systems or the nonpublic information stored on them. We require the same of our third-party service providers.

Users (That’s You!)

Users (That’s You!) need to follow these network and system policies:
Exercise caution in your communications: ❖ Especially outgoing email and attachments. ❖ Ensure that nonpublic information absolutely needs to be sent by email. ❖ Send using secure email in accordance with our policies and procedures.
When you access any system or nonpublic information from a remote location, you must: ❖ Use the SSL connection ❖ Use a VPN connection using an encrypted address that provides a secure connection.
Do not access any of our system or nonpublic information using noncompany equipment, such as your home computer, unless: ❖ It is authorized and provided with appropriate firewalls ❖ It has virus protection ❖ The connection is done through the SSL connection
Only authorized individuals should have access to protected information based on their need to access the information as a part of their responsibilities.
We enforce detailed audit logging for access to sensitive data or changes to sensitive data, for the purpose of accountability.

Device Management

Depending on your role in the company, devices such as laptops, smart phones, tablets, and digital storage media are provided by the NAL Group for business use. They help you do your job.

Laptops	Mobile Devices	Digital Storage Media

Chances are you own one or more devices for your personal home use. In accordance with our Cybersecurity Policies in this training, email may only be accessed on a personal device with permission from management.

Management must be informed immediately of any lost or replaced company or personal device that has been granted access to the company email system.

You are responsible for managing both company and personal devices according to these policies:
❖ Keep laptops, mobile devices, and digital storage media with access to nonpublic information in your possession or in a secured location at all times.
❖ If you must secure the computer in a locked vehicle, do not leave the computer in view in your car, since this could invite theft. Place the computer out of sight or in the trunk.
❖ Extreme heat and cold can damage a computer. Extreme heat can damage the hard drive. A computer that has been in extreme cold can produce condensation within the computer when brought into a warmer temperature, which can cause damage.

You are responsible for managing both company and personal devices according to these policies:

- Unless authorized by the company, DO NOT put any company data on:
  - Laptops
  - Mobile devices
  - Universal Serial Bus (USB) flash drives (aka flash drive, jump drive, memory stick, pen drive, thumb drive)
  - Other portable digital storage media
- Any authorized devices must be password protected and encrypted.
- Do not store any nonpublic information on any noncompany equipment or device.
- DO NOT share passwords or other access information.

Former Employees

Employees that no longer work for NAL Group must return all laptops, mobile devices, other digital storage media, and any nonpublic information (digital and hardcopy). They must also return all company identification and keys that allow physical access to our facilities.

Former employee access to information systems, nonpublic information, voicemail, and other protected data will be immediately disabled and transferred to other staff members in order to assure continuity of work, and inactivated when it is determined to be appropriate.

Terminology

Term	Definition
biometric record	A distinctive, measurable, physiological characteristic that can be linked to a specific individual; for example, Deoxyribonucleic acid (DNA), face recognition, fingerprint, palm print, iris recognition, and retina scan.
boundary	Detect, prevent, and correct the flow of information transferring between networks of different trust levels with a focus on security-damaging data to prevent and detect malicious and unauthorized communication.
confidentiality	The state of keeping or being kept secret or private.
encrypted	To convert information into a cipher or code to conceal data and unauthorized access.
HIPAA	Health Insurance Portable and Accountability Act enacted in 1996 by the United States legislation that provides data security and security provisions for safeguarding medical information.
network traffic	The amount of data moving across a network.
protected health information (PHI)	Any information about health status, provision of health care, or payment for health care that is created or collected by a healthcare insurer, health care professional, hospital, or their business associates, and can be linked to a specific individual. PHI includes any part of a patient's medical record or payment history. Under the United States (US) Health Insurance Portability and Accountability Act (HIPAA), PHI that is linked to an identifier must be treated with special care.
publicly available information	Any information that we reasonably believe is lawfully made available to: • The general public from federal, state, or local government records. • Widely distributed media. • disclosures to the general public that are required to be made by federal, state, or local law.
segregate	To set apart, isolate or divide from others.
spam	Irrelevant or inappropriate messages sent on the Internet to a large number of recipients.
virus	A piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.

Self-Check

Test your understanding of our cybersecurity policies.

A network is a set of servers, computers, and other devices that are interconnected in the company called an intranet.	
True or False?	
□	TRUE
□	FALSE

Our cybersecurity policy sets forth our policies and procedures for the protection of our information system and our nonpublic information stored on them.	
True or false?	
□	TRUE
□	FALSE

Access to information systems is controlled in order to protect the confidentiality, integrity, and availability of nonpublic information.	
Select two things you should do to safeguard that information.	
□	a. We use Secure Sockets Layer (SSL) to provides communications security over our computer network.
□	b. We use Email filters to remove spam and computer viruses.
□	c. We use DSL for a fast and safe connection.

Can you select the nonpublic information from the following list?	
Select all the correct answers.	
□	Business related information
□	Any security code, access code, or password that permits access to a financial account.
□	Driver's license number
□	Credit or debit card number
□	Passport number
□	Social Security Identification number (SSI)
□	Financial account number
□	Protected health information
□	All of the above

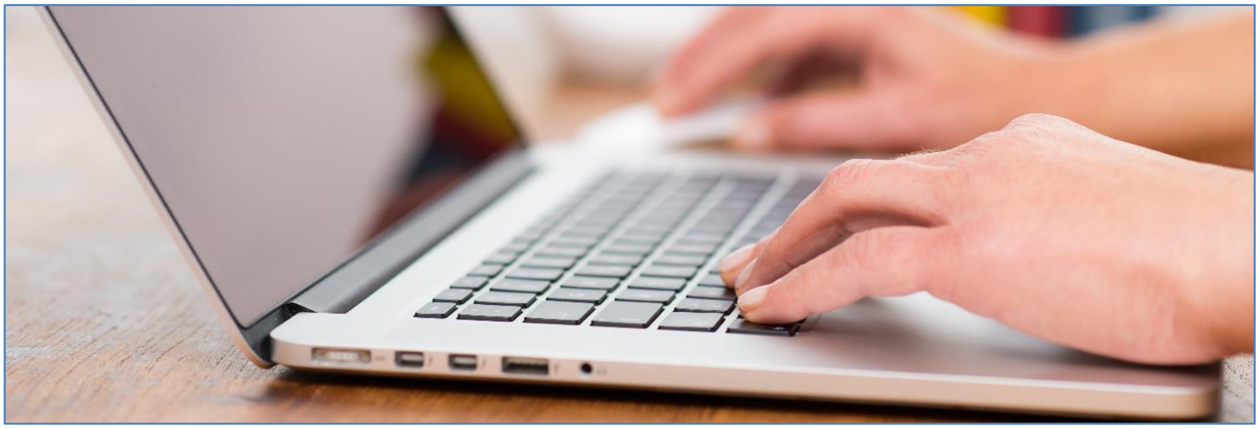
Laptops, smart phones, tablets, and digital storage media are provided by the company to help you do your job.	
Select all the things you should do to manage these devices in a secure manner.	
□	Leave your device on the seat in your car.
□	DO NOT share passwords or other access information.
□	Any authorized devices must be password protected and encrypted.
□	You can store nonpublic information on any noncompany equipment or device.

Our networks and systems are protected from and monitored for any attempt to gain unauthorized access to, disrupt, or misuse our information systems or the nonpublic information stored on them.	
Select all the things that we do to protect our systems and networks:	
□	Our boundary monitors and controls incoming and outgoing network traffic based on predetermined security rules.
□	Unauthorized software is either removed or the software asset inventory is updated as soon as possible.
□	Email filters remove spam and computer viruses

Data Control and Access

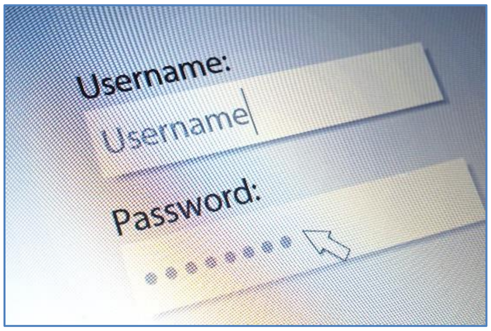
As part of our cybersecurity policy, we limit user access privileges to information systems that provide access to nonpublic information. We periodically review those access privileges to ensure that they are still applicable.

- We use automated tools to maintain a comprehensive inventory of administrative accounts to ensure only authorized people have access.
- We change default passwords before deploying any new asset.
- Accounts will use passwords that are unique to that system.
- We use dedicated machines for all administrative tasks that are segregated from the primary intranet.



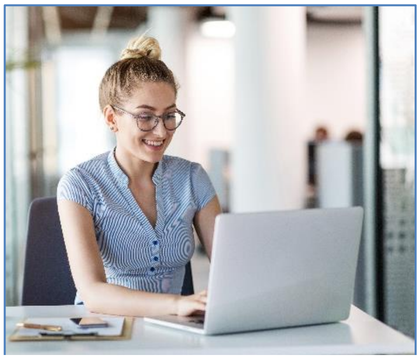
Internal Control and Access

In order to protect the confidentiality, integrity, and availability of nonpublic information, we have implemented the following measures:



- Our systems require a username and password. Mobile devices require a password. Employee usernames and passwords are appropriately strong, with a minimum number of characters and other elements.
- Controls have been implemented in order to terminate computer sessions and/or lock computers after a predetermined period of inactivity.

- Log off or lock your computer when you leave it unattended; for example, when you go on a break, to lunch, to a meeting, or out of the office.
- If there is a file containing nonpublic information open on your computer, lock the screen anytime you leave your computer unattended, even briefly.

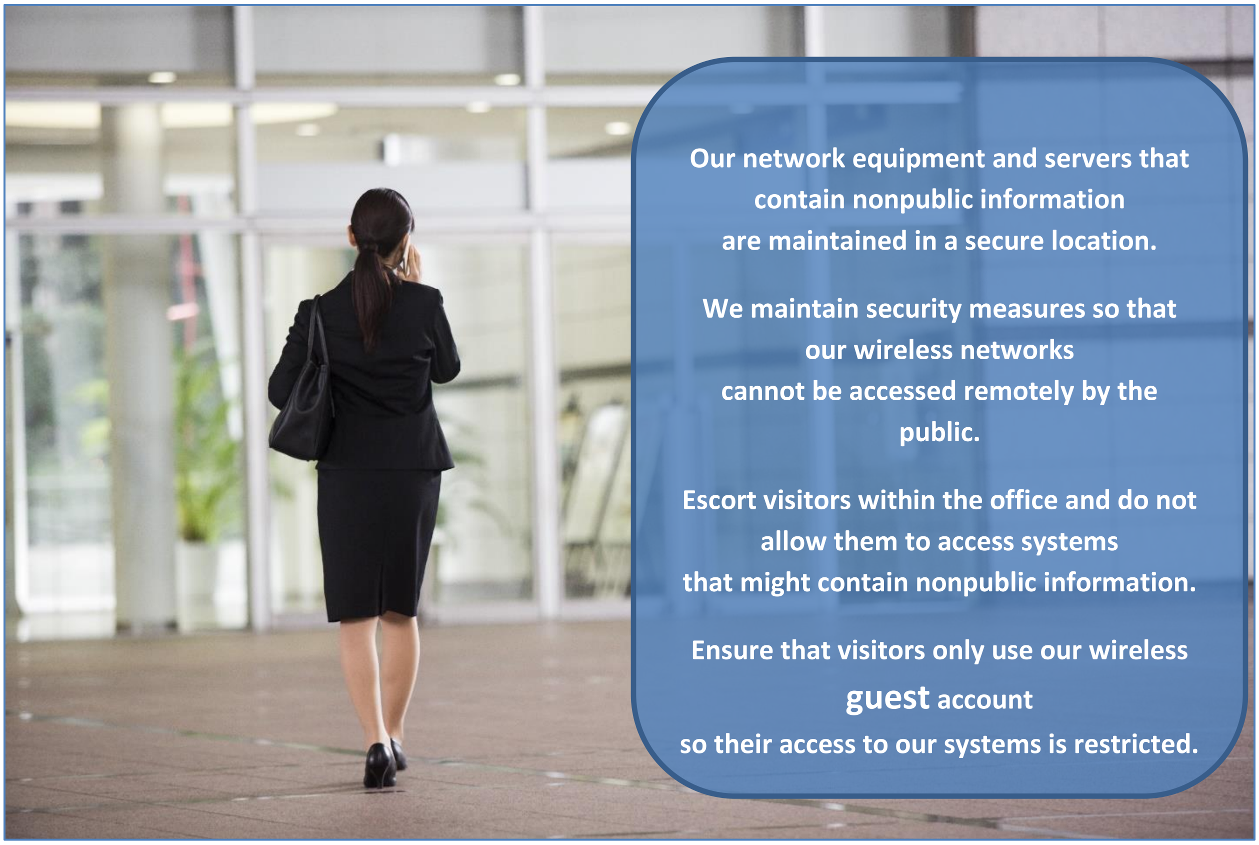


- Software can only be downloaded and installed by members of our IT team.

- We retain checks and bank account information. Adhere to the company document retention schedule. When it is appropriate to destroy this information, paper and electronic records shall be destroyed in a manner which ensures that they cannot be read or reconstructed.

External Control and Access

In addition to the measures taken to reduce internal risks, we take measures to minimize external risks to the confidentiality, integrity, and availability of nonpublic information.



Our network equipment and servers that contain nonpublic information are maintained in a secure location.

We maintain security measures so that our wireless networks cannot be accessed remotely by the public.

Escort visitors within the office and do not allow them to access systems that might contain nonpublic information.

Ensure that visitors only use our wireless **guest** account so their access to our systems is restricted.

Disaster Recovery and Business Continuity

In the unlikely event of total destruction or damage beyond repair to our facilities or information systems, you will be notified of the disaster and whether or not to report to work.

Depending upon the level of the disaster, operations might be suspended for a period of hours or days, operations might be moved to a temporary sight, or a new facility might be required.

Terminology

Term	Definition
automated	Operated by systems and processes that are prescheduled to act.
confidentiality	The state of keeping or being kept secret or private.
dedicated	Exclusively allocated to or intended for a particular service or purpose or task.
predetermined	Planned or decided in advance.
primary	Of chief importance.
segregated	Set apart, isolated or divided.
terminate	To bring to an end.

Self-Check

Test your understanding of data control and access.

As part of our cybersecurity policy, we limit user access privileges to information systems that provide access to nonpublic information.	
True or false?	
□	TRUE
□	FALSE

It is OK to leave your computer unlocked if you are just leaving it unattended for a few minutes.	
True or false?	
□	TRUE
□	FALSE

It is OK for you to download software onto your computer if your supervisor thinks you need it.	
True or false?	
□	TRUE
□	FALSE

You should report all actual or potential unauthorized access to, use of, or disclosure of nonpublic information to the Help Desk.	
Ture or false?	
□	TRUE
□	FALSE

Learning Activity

Review the *NAL Group Cybersecurity Plan*. Look through the document and identify the policies we have discussed in this topic. If you have any questions about these policies, make a note of your questions and contact the Help Desk for answers.

Employee Responsibilities and Best Practices

This topic describes your responsibilities and the best practices that can empower you to tackle evolving cybersecurity threats.

Your Importance to Cybersecurity

Never underestimate your importance to cybersecurity.

You may think that cybersecurity events are mainly caused by outsiders hacking into a company's information systems. While that scenario is the one that makes the headlines, the fact is that employee error, such as a lost or stolen computer or mobile device, or downloading malicious software, can also lead to data loss or a data breach incident.	Employee responsibility is critical to the protection of our information systems and nonpublic information. We have legal obligations to respect and protect the privacy of nonpublic information and its confidentiality, integrity, and availability to authorized users.

What if you make a mistake?

Let the Help Desk know immediately!

Laptop Usage

Reviewing Your Responsibilities

DO

Keep laptops and digital storage media in your possession or in a secured location.

DO NOT

Do not put any company data on laptops or digital storage media unless authorized by the company.

DO NOT

Do not share passwords or other access information.

Best Practices

In General

- When away from the office, keep your company laptop and company approved portable storage devices, such as a USB flash drive, secure—either locked up or in your personal possession.
- When you travel by car with your laptop, put it in the trunk of the vehicle, and take it with you when you arrive at your final destination.
- When away from your laptop (or desktop), lock the screen using the following key sequence: **CTRL+ALT+DELETE**
- Do not share your password.

Wi-Fi

Public Wi-Fi networks can be found almost everywhere and make it easy for you to connect to the Internet wherever you are. Although these public networks are convenient, they are not always secure and do not encrypt information that you send over the Internet, potentially exposing you to cybersecurity threats and presenting an opportunity for others to steal sensitive information. Always avoid conducting sensitive activities through public networks.

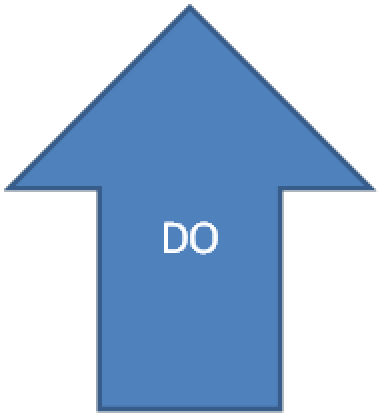
If you plan to work on sensitive information:

- Turn off features on your laptop that allow you to connect automatically to Wi-Fi.
- Once you have finished using the public network, be sure to log out.

If it is included in your mobile plan, use your mobile network connection (also known as your wireless hotspot) when working on sensitive information, instead of using the public network. Your mobile network connection is generally more secure than a public wireless network. Note: there can be additional costs associated with using a hotspot. Check with your mobile service provider for cost information before using a hotspot.

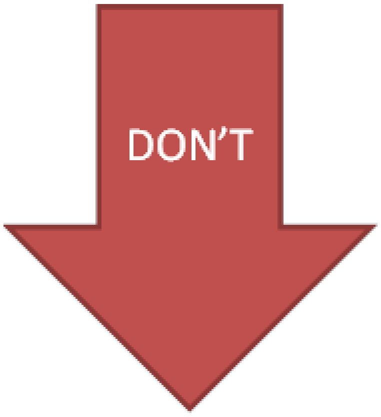
Passwords

When it comes to cybersecurity, the best first step is a strong password. Most people do not put a lot of thought into creating passwords beyond their birthday or pet's name, but as the number of cybersecurity breaches continues to rise, it is critical to have passwords that are difficult to break.



- Use eight characters or more.
- Use a combination of upper- and lower-case characters, numerals, and symbols.
- Make your password cryptic so that it cannot be easily guessed, while ensuring it is something you can remember.

- Use complete words.
- Use personal information such as your name, birthdate, family or pet’s names, or the company name.
- Reuse passwords.



Password Hints:

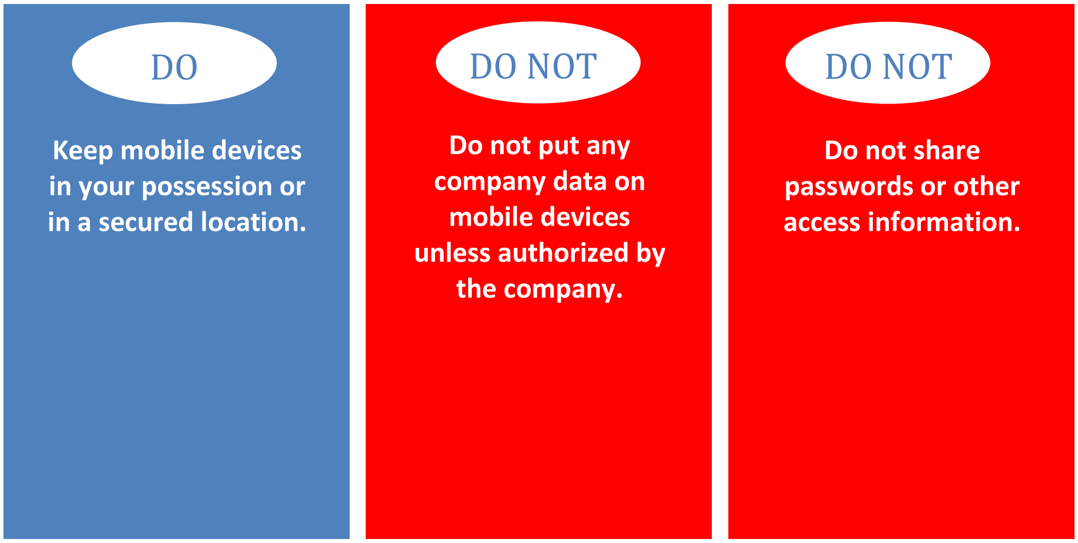
- Create a unique acronym for a sentence or phrase, substituting alphanumeric or phonetic replacements for words, and adding some punctuation.
- Change common words by substituting letters with numbers and punctuation marks or symbols; for example, replace the letter "A" with an ampersand (@) or replace the letter "I" with an exclamation point (!).
- Use phonetic replacements; for example, replace "F" with "PH."
- Make deliberate but obvious misspellings; for example, replace "engine" with "enjin."
- Make up a formula that helps you remember your passwords, for example, <your initials><where you are><year>, which could look like "JJPwork19".

Password Security

- Be aware of your surroundings when logging in to secure systems while in public places so that others cannot see your username and password. Shoulder surfing is prevalent in public places like coffee shops and libraries.
- Choose different passwords for all of your accounts.
- Because it can never be said too many times – **NEVER SHARE YOUR PASSWORDS WITH ANYONE**.

Mobile Device Usage

Reviewing Your Responsibilities



DO

Keep mobile devices in your possession or in a secured location.

DO NOT

Do not put any company data on mobile devices unless authorized by the company.

DO NOT

Do not share passwords or other access information.

Sound familiar? Your responsibilities for the use of laptops and mobile devices are the same. Keep these devices—and the nonpublic information that they contain or have access to—safe and secure.

Best Practices for Personally Owned Devices

With the increased capabilities of consumer devices, such as smart phones and tablets, it has become easy to interconnect these devices to company networks and systems. Use of these devices to interconnect to company email, calendars, and other services can blur the lines between company controls and consumer controls.

Policy

There is a formal process in place for gaining access to our systems from your personally owned mobile device. This process helps ensure that mobile devices are secure and used appropriately.

Passwords and Passcodes

You are responsible for protecting your devices from theft and maintaining password protection in accordance with our password policy minimum requirements. The first level of mobile device security is locking your device with a passcode or touch ID.

Lost or Stolen Devices

Mobile devices contain a wealth of personal information, including email messages, contacts, calendars, and access to apps. When your mobile device is lost or stolen, your personal information goes with it, resulting in data and access vulnerabilities that can be exploited.

In case your phone is ever lost or stolen, make sure that you know how to use any features that allow you to remotely locate, lock, or wipe data from your device. These features might be built into the OS, provided by your mobile carrier, or available via a desktop application. Management must be informed immediately of any lost, stolen, or replaced company or personal device that has been granted access to the company email system.

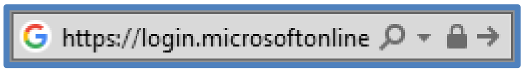
Software Updates

Install updates for your device OS and apps as soon as they are available. Keeping the software on your mobile device up to date can prevent the exploitation of known vulnerabilities.

Internet Usage

Most people use the Internet without a thought to the harm that can ensue. Employee misuse of the Internet can place us in an awkward, or even illegal, position.

Best Practices



https://login.microsoftonline

When entering company or nonpublic information on a website, make sure that the website is encrypted. Encrypted websites use addresses that begin with **https://** (not **http://**). Look for this on every page, not just the login or welcome page.

A pop-up blocker should be installed or provided as part of your web browser; however, pop-up blockers do not always block all pop-ups.

Do not respond to pop-ups while working online. Close them by clicking **X** in the upper right corner. If you click **OK** or **Cancel**, the pop-up might install spyware or other malicious code onto your computer.

Terminology

Term	Definition
c	Consisting of letters and numbers.
cryptic	A coded message.
hotspot	An ad hoc wireless access point that is created by a dedicated hardware device or a smartphone feature that shares the phone's cellular data.
interconnect	A device used to connect two things together.
obligation	An act or course of action to which a person is morally or legally bound; a duty or commitment.
phonetic	Related to speech sounds; sounds like.
pop-up	To appear without having been requested.
Wi-Fi	A trademarked term meaning IEEE 802.11x.

Self-Check

Test your understanding of laptop and mobile device usage.

Employee error, such as a lost or stolen computer or mobile device, or downloading malicious software, can lead to data loss or a data breach incident.	
True or false?	
□	TRUE
□	FALSE

What key sequence can you use to lock your screen when you step away from your computer?	
Select the box with the correct answer:	
□	**CTRL+ALT+DELETE**
□	**CTRL+ALT+SHIFT**

You should report all actual or potential unauthorized access to, use of, or disclosure of nonpublic information to the Help Desk.	
Ture or false?	
□	TRUE
□	FALSE

Select all the conventions that make for a strong password.	
□	Your pet’s name.
□	Change common words by substituting letters with numbers and punctuation marks or symbols.
□	Use phonetic replacements.
□	Make deliberate but obvious misspellings.
□	All of the above.

Why should you avoid conducting sensitive activities through public networks?	
Select all correct answers.	
□	They are not always secure and do not encrypt information that you send over the Internet.
□	They can expose you to cybersecurity threats.
□	They can present an opportunity for others to steal sensitive information.

You have a responsibility to lock your device with a passcode, touch ID, or other biometric.	
True or False?	
□	TRUE
□	FALSE

Social Media

All users of social media need to be aware of the risks associated with social media networking.

Best Practices

Social media is a place where people let their guard down. It's what you check on your lunch break. It's what you do when you get home from work and before you turn in for the night. On sites like Facebook and Twitter, where the atmosphere is casual, there is a greater tendency to let certain information slip, which brings possible risk to the company.	Publicly posting or tweeting about that business conference you just attended could be used to create a targeted phishing email containing a malicious link.	If your personal account is attached to a company account and your personal account is hacked, not only does this threaten our information security, but it also has the potential to threaten our brand image as well. If even a few incendiary tweets are perceived to have come from our corporate account, it could push clients away and lead to negative media attention.	Although they have implemented better security tools, the responsibility for security does not rest with social media companies. At the end of the day, it's your problem to own. The available security options only work as well as you use them.

Email Usage

Many data breaches are a result of email misuse that can result in the loss or theft of data and the accidental downloading of viruses or other malware.

Phishing emails can be used to target your identity, gain control of our networks and systems, or steal your password in order to access company information.

They often appear as if they come from a trusted source and can often include links that they ask you to click or attachments that they ask you to download.

In July 2017, Internet security company Comodo disclosed a new type of phishing scam specifically targeting small businesses. Phishing emails were sent out to more than 3,000 businesses, including the subject line 'Shipping Information'.

The email noted a forthcoming delivery by United Parcel Service (UPS) and included a seemingly innocent package tracking link. When the recipient clicked on the link it contained malware, potentially releasing a virus.

Source: Small Business Trends: *10 Phishing Examples in 2017 that Targeted Small Business*.

Best Practices

You should delete suspicious messages without opening them.

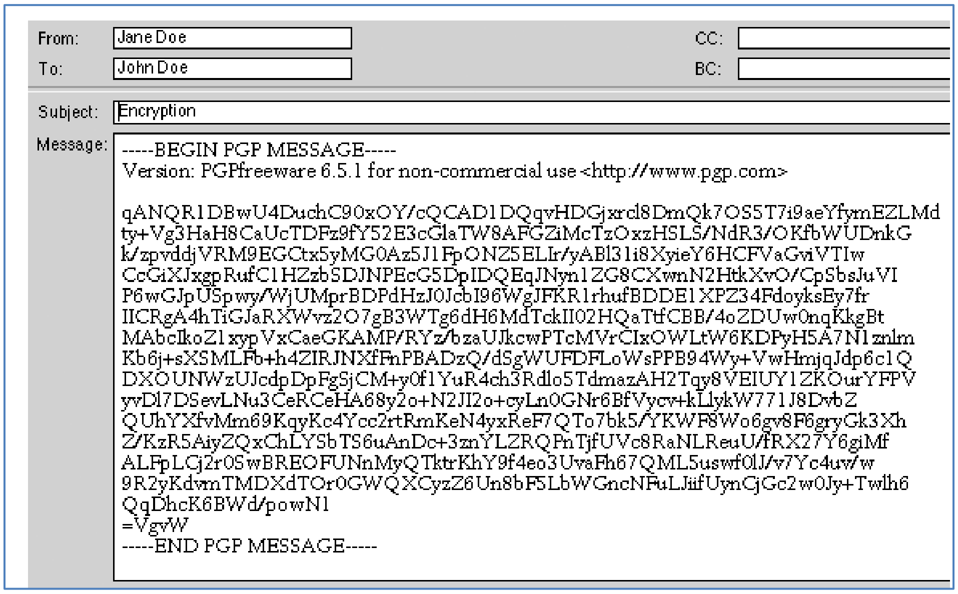
Before you open an email message or respond to requests to click on links or download attachments, confirm that the message:

- Comes from someone you know.
- Comes from someone who has sent you an email in the past.
- Is something you were expecting.
- Does not look out of the ordinary, with incorrect spelling or unusual characters.

Beware of links:

- Avoid clicking on links in email messages, especially if that is all that is in the email.
- Verify that a link is authentic before clicking on it.
  - Type the address directly into the address bar on your browser.
  - Check a link by hovering over it with the cursor to reveal the full address in the lower-left corner of the browser window.

Encryption works by applying a cryptographic algorithm and key to text that changes the readable text to what appear to be random letters and numbers but is actually code that will be unscrambled at the receiver's end. The sender and receiver must use the same key for encryption and decryption. In the event that management deems that certain communications must be encrypted, they will provide the rules around using encryption and a process for how to apply encryption.



From:	Jane Doe	CC:	
To:	John Doe	BC:	

Subject: Encryption

Message:

```
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.1 for non-commercial use <http://www.pgp.com>

qANQR1DBwU4DuchC90xOY/cQCAD1DQqvHDGjxrdl8DmQk7OS5T7i9aeYfymEZLMd
ty+Vg3HaH8CaUcTDFz9fY52E3cGlaTW8AFGZiMcTzOxzHSLS/NdR3/OKfbWUDnkG
k/zpvddjVRM9EGCtx5yMG0Az5J1FpONZ5ELIr/yABl31i8XyieY6HCFVaGviVTIw
CcGiXJxgpRufC1HZzbSDJNPEcG5DpIDQEqJNyn1ZG8CXwnN2HtkXvO/CpSbsJuVI
P6wGJpUSpwy/WjUMprBDPdHzJ0JcbI96WgJFKR1rhufBDDE1XPZ34FdoyksEy7fr
IICRgA4hTiGJaRXWvz2O7gB3WTg6dH6MdTckII02HQaTtfCBB/4oZDUw0nqKkgBt
MAbcIkoZ1xypVxCaeGKAMP/RYz/bzaUJkcwPTcMVrCIxOWLtW6KDPyH5A7N1znlm
Kb6j+sXSMLFb+h4ZIRJNXfFnPBADzQ/dSgWUFDFLoWsPPB94Wy+VwHmjqJdp6c1Q
DXOUNWzUJcdpDpFgSjCM+y0f1YuR4ch3Rdlo5TdmazAH2Tqy8VEIUY1ZKOurYFPV
yvDl7DSevLNu3CeRCeHA68y2o+N2JI2o+cyLn0GNr6BfVycv+kLlykW771J8DvbZ
QUhYXfvMm69KqyKc4Ycc2rtRmKeN4yxReF7QTo7bk5/YKWF8Wo6gv8F6gryGk3Xh
Z/KzR5AiyZQxChLYSbTS6uAnDc+3znYLZRQPnTjfUVc8RaNLReuU/fRX27Y6giMf
ALFpLCj2r0SwBREOFUNnMyQTktrKhY9f4eo3UvaFh67QML5uswf0lJ/v7Yc4uv/w
9R2yKdvmTMDXdTOr0GWQXCyzZ6Un8bF5LbWGncNFuLJiifUynCjGc2w0Jy+Twlh6
QqDhcK6BWd/powN1
=VgvW
-----END PGP MESSAGE-----
```

Protecting Company and Client Data

Information should only be accessed and used in ways that keeps customer identity and the confidentiality, integrity, and availability of company data and nonpublic information intact.

Reviewing Your Responsibilities

- Accord nonpublic information the highest level of confidentiality.
- Exercise caution in your communications, especially outgoing email and attachments, in order to ensure that the nonpublic information absolutely needs to be sent by email and, if so, that it is sent using secure email in accordance with our policy.
- Log off or lock your computer when you leave it unattended.
- If there is a file containing nonpublic information open on your computer, lock the screen anytime you leave your computer unattended, even briefly.
- Escort visitors within the office and do not allow them to access systems that might contain nonpublic information.
- Ensure that visitors only use our wireless **guest** account so access to our systems is restricted.
- Use a VPN connection when you access our systems from a remote location.
- Report all actual or potential unauthorized access to, use of, or disclosure of nonpublic information to the Help Desk.

Best Practices for Hardcopy Information

- Be aware of your surroundings when viewing hardcopy documents in an open setting. Shoulder surfing isn’t just for passwords.
- Clean up your materials after meetings.
- Immediately retrieve your documents after printing, copying, or faxing.
- Keep sensitive materials in a secure location.

Best Practices for Verbal Communication

Loose lips sink ships! Do not discuss company business outside of work. Even being excited about a success and telling someone outside of the company can be construed as sharing insider information.

A Nortel Networks employee complained about the challenges they were having with a new software release to a friend in a restaurant setting. Unbeknownst to the employee, the person at the next table was a journalist. The issues with the new software release were made public the next day, causing a drop in Nortel’s stock price.

Source: former Nortel Networks employee.

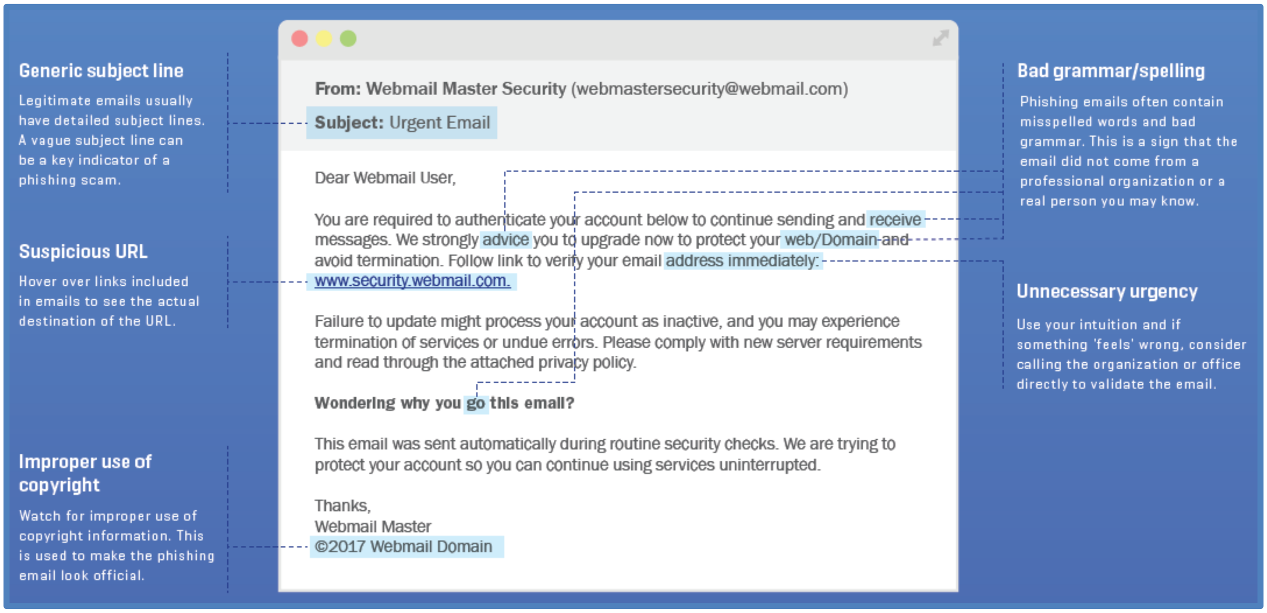
Recognizing Threats

Cybersecurity threats are becoming more sophisticated, realistic, and difficult to recognize. Phishing attacks are one of the most common threats.

Best Practices to Avoid Phishing Attacks

Phishing attempts can often get through email filters and security software, so stay vigilant and trust your instincts. Think twice about clicking a link or opening an attachment that seems suspicious. Double-check that webpage addresses are legitimate, especially those where you must enter a username and password. If anything raises doubt, delete or report the message. If in doubt—don't click on a link. The producers of phishing emails specialize in making them compelling.

What does a phishing email look like?



Generic subject line

Legitimate emails usually have detailed subject lines. A vague subject line can be a key indicator of a phishing scam.

Suspicious URL

Hover over links included in emails to see the actual destination of the URL.

Improper use of copyright

Watch for improper use of copyright information. This is used to make the phishing email look official.

From: Webmail Master Security (webmastersecurity@webmail.com)

Subject: Urgent Email

Dear Webmail User,

You are required to authenticate your account below to continue sending and receive messages. We strongly advice you to upgrade now to protect your web/Domain and avoid termination. Follow link to verify your email address immediately:
www.security.webmail.com.

Failure to update might process your account as inactive, and you may experience termination of services or undue errors. Please comply with new server requirements and read through the attached privacy policy.

Wondering why you go this email?

This email was sent automatically during routine security checks. We are trying to protect your account so you can continue using services uninterrupted.

Thanks,
Webmail Master
©2017 Webmail Domain

Bad grammar/spelling

Phishing emails often contain misspelled words and bad grammar. This is a sign that the email did not come from a professional organization or a real person you may know.

Unnecessary urgency

Use your intuition and if something 'feels' wrong, consider calling the organization or office directly to validate the email.

Source: Department of Homeland Security (DHS)

The following phrases are examples of what attackers might include in an email message when phishing for sensitive information:
"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."
"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."
"Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

Source: Federal Trade Commission (FTC) OnGuardOnline

Symptoms of Cybersecurity Events

Besides suspicious email messages, what else might alert you to the possibility that you have been the target of a cybersecurity attack?

- Your antivirus software detects a problem.
- Your computer reboots or shuts down by itself.
- Your computer's performance slows down.
- Disk space disappears.
- The cursor moves by itself.
- New icons or programs that you did not add appear on your desktop.
- Excessive pop-ups display in your browser or on your desktop.
- Your browser's homepage changes.
- You receive frequent firewall alerts about unknown programs trying to access the Internet.
- There seems to be a lot of network activity while your computer is not particularly active.

Reporting Threats

All employees should know how to report cybersecurity threats and events internally.

Report anything suspicious. If you experience any unusual problems with your computer or device, report it to the Help Desk.

When reporting the unusual activity, include the following details:

- The identity of the computer or device that is experiencing the unusual activity.
- A description of the symptoms.
- The date and time when you first noticed the symptoms.
- The task you were performing when you first noticed the symptoms.

Note: Only NAL Group management has the authority to determine if and when it is appropriate to disseminate information outside of the company.

New Threats

Cybersecurity risk assessment is an ongoing process. Security measures are monitored and reviewed in order to ensure that they work as planned and that changes to our network or systems haven't rendered them ineffective. Business requirements, new vulnerabilities, and new threats can change over time. Management will keep you apprised of any changes or updates in cybersecurity policies.

Terminology

Term	Definition
incendiary	Tending to stir up conflict.
malware	Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
phishing	The fraudulent practice of sending emails that appear to be from reputable companies in order to trick individuals into revealing personal information, such as passwords and credit card numbers.
shoulder surfing	The act of trying to view another person's laptop or mobile device screen for the purpose of acquiring passwords or nonpublic information.
vigilant	Watching out for possible danger or difficulties.

Self-Check

Test your understanding of your cybersecurity responsibilities in managing Social media, email usage, protecting company date, and recognizing threats.

You are visiting a website (for business purposes, of course) and a suspicious pop-up window appears.	
What should you do?	
☐	Click **Cancel**.
☐	Click **OK**.
☐	Click the close button (**X**).

Who is responsible for the security of your social media sites?	
Select all that apply.	
☐	Facebook
☐	Twitter
☐	You are
☐	YouTube

Before you open an email message or respond to requests to click on links or download attachments, what can you do to confirm that the message is safe?	
Select all that apply.	
□	The message comes from someone you know.
□	The message comes from someone who has sent you an email in the past.
□	The message is something you were expecting.
□	The message does not look out of the ordinary, with incorrect spelling or unusual characters.

If you experience any unusual problems with your computer or device, report it to:	
Select all that apply.	
□	Help Desk
□	Your mother
□	Your colleagues
□	A teammate

Because third-party companies work with us, they don't need to use the Guest access when they are onsite.	
True or false?	
□	TRUE
□	FALSE

Course Summary

Let’s take a moment to review what you have learned in this course.

You learned about our cybersecurity program and cybersecurity threats.

In the first topic, we discussed the risk assessment and answered the following questions:

- What are the threats to our information systems?
- What measures have we put in place to protect us from those threats?
- How do we detect a cybersecurity event?
- How do we respond to a cybersecurity event?
- How do we recover from a cybersecurity event?
- What are our reporting obligations?

Next, you learned about our cybersecurity policies and the importance of protecting the confidentiality, integrity, and availability of company data and nonpublic information. You learned about policies concerning:

- Network and systems security
- Device management
- Data control and access
- Disaster recovery and business continuity

Lastly, we focused on your responsibilities and the best practices that empower you to meet those responsibilities. You learned how to recognize and report cybersecurity threats.

If you wish to review any information, return to the appropriate topic.
If you are ready to take the course assessment, you may access it on the NAL Group LMS training site.

Cybersecurity Awareness Course Acknowledgment of Completion

I acknowledge that I have completed the Cybersecurity Awareness course which describes our cybersecurity program, company policies, and the current employee responsibilities and obligations.

Furthermore, I understand that the cybersecurity policies described in this course might be added to, revised, or deleted at any time. The company provides annual cybersecurity awareness refresher training in order to ensure that I am kept up to date on our program and policies.

____
Employee Signature

____
Employee Name (printed)

____
Date

NAL Group

United States Corporate Offices

74 Carter Drive
Edison, New Jersey 08817
732-739-7200

241 Main Street, 5th Floor
Buffalo, NY 14203
716-854-1994

Canada Corporate Offices

6355 Danville Road
Mississauga, ON L5T 2H7
844-218-1762

Toll free - 866-504-8247

Website - https://nalgroup.com

Email - info@nalgroup.com