Principles of Information Security 7th edition Whitman Solutions Manual

SKU: 9780357506431-SOLUTIONS

Instructor Manual

Whitman and Mattord, Principles of Information Security 7e, ISBN 978-0-357-50643-1; Module 1: Introduction to Information Security

Table of Contents

Purpose and Perspective of the Module 2
Cengage Supplements 2
Module Objectives 2
Complete List of Module Activities and Assessments 2
Key Terms 3
What's New in This Module 5
Module Outline 5
Discussion Questions 18
Suggested Usage for Lab Activities 19
Additional Activities and Assignments 21
Additional Resources 21
Cengage Video Resources 21
Internet Resources 21
Appendix 22
Grading Rubrics 22

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Purpose and Perspective of the Module

The first module of the course in information security provides learners the foundational knowledge to become well versed in the protection systems of any size need within an organization today. The module begins with fundamental knowledge of what information security is and the how computer security evolved into what we know now as information security today. Additionally, learners will gain knowledge on the how information security can be viewed either as an art or a science and why that is the case.

Cengage Supplements

The following product-level supplements are available in the Instructor Resource Center and provide additional information that may help you in preparing your course:

- PowerPoint slides
- Test banks, available in Word, as LMS-ready files, and on the Cognero platform
- MindTap Educator Guide
- Solution and Answer Guide
- This instructor's manual

Module Objectives

The following objectives are addressed in this module:

1.1 Define information security.

1.2 Discuss the history of computer security and explain how it evolved into information security.

1.3 Define key terms and critical concepts of information security.

1.4 Describe the information security roles of professionals within an organization.

Complete List of Module Activities and Assessments

For additional guidance refer to the MindTap Educator Guide.

Module Objective	PPT slide	Activity/Assessment	Duration
	2	Icebreaker: Interview Simulation	10 minutes
1.1–1.2	19–20	Knowledge Check Activity 1	2 minutes
1.3	34–35	Knowledge Check Activity 2	2 minutes
1.4	39–40	Knowledge Check Activity 3	2 minutes
1.1–1.4	MindTap	Module 01 Review Questions	30–40 minutes

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

1.1 – 1.4	MindTap	Module 01 Case Exercises	30 minutes
1.1 – 1.4	MindTap	Module 01 Exercises	10–30 minutes per question; 1+ hour per module
1.1 – 1.4	MindTap	Module 01 Security for Life	1+ hour
1.1 – 1.4	MindTap	Module 01 Quiz	10–15 minutes

[return to top]

Key Terms

In order of use:

computer security: In the early days of computers, this term specified the protection of the physical location and assets associated with computer technology from outside threats, but it later came to represent all actions taken to protect computer systems from losses.

security: A state of being secure and free from danger or harm as well as the actions taken to make someone or something secure.

information security: Protection of the confidentiality, integrity, and availability of information assets, whether in storage, processing, or transmission, via the application of policy, education, training and awareness, and technology.

network security: A subset of communications security; the protection of voice and data networking components, connections, and content.

C.I.A. triad: The industry standard for computer security since the development of the mainframe; the standard is based on three characteristics that describe the attributes of information that are important to protect: confidentiality, integrity, and availability.

confidentiality: An attribute of information that describes how data is protected from disclosure or exposure to unauthorized individuals or systems.

personally identifiable information (PII): Information about a person's history, background, and attributes that can be used to commit identity theft that typically includes a person's name, address, Social Security number, family information, employment history, and financial information.

integrity: An attribute of information that describes how data is whole, complete, and uncorrupted.

availability: An attribute of information that describes how data is accessible and correctly formatted for use without interference or obstruction.

accuracy: An attribute of information that describes how data is free of errors and has the value that the user expects.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

authenticity: An attribute of information that describes how data is genuine or original rather than reproduced or fabricated.

utility: An attribute of information that describes how data has value or usefulness for an end purpose.

possession: An attribute of information that describes how the data's ownership or control is legitimate or authorized.

McCumber Cube: A graphical representation of the architectural approach used in computer and information security that is commonly shown as a cube composed of 3×3×3 cells, similar to a Rubik's Cube.

information system: The entire set of software, hardware, data, people, procedures, and networks that enable the use of information resources in the organization.

physical security: The protection of material items, objects, or areas from unauthorized access and misuse.

bottom-up approach: A method of establishing security policies and/or practices that begins as a grassroots effort in which systems administrators attempt to improve the security of their systems.

top-up approach: A methodology of establishing security policies and/or practices that is initiated by upper management.

chief information officer (CIO): An executive-level position that oversees the organization's computing technology and strives to create efficiency in the processing and access of the organization's information.

chief information security officer (CISO): The title typically assigned to the top information security manager in an organization.

data owners: Individuals who control and are therefore ultimately responsible for the security and use of a particular set of information.

data custodians: Individuals who are responsible for the storage, maintenance, and protection of information.

data stewards: See *data custodians.*

data trustees: Individuals who are assigned the task of managing a particular set of information and coordinating its protection, storage, and use.

data users: Internal and external stakeholders (customers, suppliers, and employees) who interact with information in support of their organization's planning and operations.

community of interest: A group of individuals who are united by similar interests or values within an organization and who share a common goal of helping the organization to meet its objectives.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

[return to top]

What's New in This Module

The following elements are improvements in this module from the previous edition:

- This Module was Chapter 1 in the 6th edition.
- The content that covered Systems Development was moved to Module 11: Implementation.
- The Module was given a general update and given more current examples.

[return to top]

Module Outline

Introduction to Information Security (1.1, 1.2, PPT Slides 4–17)

I. Recognize that organizations, regardless of their size or purpose, have information they must protect and store internally and externally.

II. Analyze the importance and reasoning an organization must be responsible for the information they collect, store, and use.

III. Review the concept of computer security and when the need for it initially arose.

IV. Discuss how badges, keys, and facial recognition of authorized personnel are required to access military locations deemed sensitive.

V. Describe the primary threats to security: physical theft of equipment, product espionage, and sabotage.

VI. Examine information security practices in the World War II era and compare with modern day needs.

The 1960s

I. Explain the purpose of the Department of Defense's Advanced Research Procurement Agency (ARPA) and their need to create redundant networked communications systems so that the military can exchange information.

II. Identify Dr. Larry Roberts as the creator of the ARPANET project and now the modern-day Internet.

The 1970s and '80s

I. Critique the use of ARPANET and how it became more widely used and consequentially misused.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

II. Recognize that Robert M. Metcalfe expressed concerns about ARPANET and how it could be easily hacked into due to password structure vulnerabilities, lack of safety protocols, and widely distributed phone numbers for system access.

III. Conclude that a lack of controls in place provided users limited safeguards to protect themselves from unauthorized remote users.

IV. Discuss how dial-up connections lacked safety protocols when connecting to ARPANET.

V. Recall that authorizations into the system and a lack of user identification were significant security risks for ARPANET during this time.

VI. Evaluate the movement of stronger security protocols thanks to the implementation of conclusions from the Rand Report R-609.

VII. Relate how the need of physical security protocols grew to include computer security protocols as part of a holistic information security plan.

MULTICS

I. Define the purpose of the Multiplexed Information and Computing Service (MULTICS) and its importance to information security.

II. Relate that the restructuring of the MULTICS project created the UNIX operating system in 1969.

III. Contrast the facts that the MULTICS system had multiple security levels planned, whereas the new UNIX system did not have them included.

IV. Examine the decentralization of data processing and why it is important to modern-day information security protocols.

V. Distinguish that in the late 1970s microprocessors transformed computing capabilities but also established new security threats.

VI. Recall the Defense Advanced Research Projects Agency (DARPA) created the Computer Emergency Response Team (CERT) in 1988.

VII. Conclude that not until the mid-1980s computer security was a non-issue for federal information systems.

The 1990s

I. Understand that as more computers and their networks became more common, the need to connect networks rose in tandem during this time. Hence, the Internet was born out of the need to have a global network of networks.

II. Analyze the consequences of how exponential growth of the Internet early on resulted in security being a low priority over other core components.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

III. Identify that the networked computers were the most common style of computing during this time. However, a result of this was the lessened ability to secure a physical computer and stored data is more exposed to security threats internally and externally.

IV. Recognize that toward the turn of the new millennium, numerous large corporations demonstrated the need and integration of security into their internal systems. Antivirus products grew in popularity and information security grown into its own discipline because of these proactive initiatives.

2000 to Present

I. Recall the fact that millions of unsecured computer networks and billions of computing devices are communicating with each other.

II. Recognize and apply the fact that cyberattacks are increasing and have caused governments and corporations to resign themselves to stronger information security protocols.

III. Examine the exponential rise in mobile computing and how these devices bring their own set of vulnerabilities with respect to information security.

IV. Apply the fact that one's ability to secure the information stored in their device is influenced by security protocols on the others they are connected to.

V. Establish that wireless networks and their associated risks often have minimal security protocols in place and can be a catalyst for anonymous attacks.

What Is Security? (1.3, PPT Slides 18 and 21–26)

I. Define the term security and why it is important to have multiple layers of it to protect people, operations, infrastructure, functions, communications, and information.

II. Emphasize the role of the Committee on National Security Systems (CNSS) and its role in defining information security. This includes the protection of critical elements such as systems and hardware that stores, transmits, and use information.

III. Recognize the importance of the C.I.A. Triad but which is no longer an adequate model to apply to modern information security needs.

Key Information Security Concepts

I. Comprehend and define the following security terms and concepts:

- **Access**: A subject or object's ability to use, manipulate, modify, or affect another subject or object. Authorized users have legal access to a system, whereas hackers must gain illegal access to a system. Access controls regulate this ability.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

- **Asset**: The organizational resource that is being protected. An asset can be logical, such as a Web site, software information, or data, or an asset can be physical, such as a person, computer system, hardware, or other tangible object. Assets, particularly information assets, are the focus of what security efforts are attempting to protect.
- **Attack**: An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it. Attacks can be active or passive, intentional or unintentional, and direct or indirect. Someone who casually reads sensitive information not intended for his or her use is committing a passive attack. A hacker attempting to break into an information system is an intentional attack. A lightning strike that causes a building fire is an unintentional attack. A direct attack is perpetrated by a hacker using a PC to break into a system. An indirect attack is a hacker compromising a system and using it to attack other systems—for example, as part of a botnet (slang for robot network). This group of compromised computers, running software of the attacker's choosing, can operate autonomously or under the attacker's direct control to attack systems and steal user information or conduct distributed denial-of-service attacks. Direct attacks originate from the threat itself. Indirect attacks originate from a compromised system or resource that is malfunctioning or working under the control of a threat.
- **Control, safeguard, or countermeasure:** Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization. The various levels and types of controls are discussed more fully in the following modules.
- **Exploit:** A technique used to compromise a system. This term can be a verb or a noun. Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain, or an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or created by the attacker. Exploits make use of existing software tools or custom-made software components.
- **Exposure:** A condition or state of being exposed; in information security, exposure exists when a vulnerability is known to an attacker.
- **Loss:** A single instance of an information asset suffering damage or destruction, unintended or unauthorized modification or disclosure, or denial of use. When an organization's information is stolen, it has suffered a loss. Protection profile or security posture is the entire set of controls and safeguards—including policy, education, training and awareness, and technology—that the organization implements to protect the asset. The terms are sometimes used interchangeably

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

with the term security program although a security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.

- **Risk:** The probability of an unwanted occurrence, such as an adverse event or loss. Organizations must minimize risk to match their risk appetite—the quantity and nature of risk they are willing to accept.
- **Subjects and objects of attack:** A computer can be either the subject of an attack—an agent entity used to conduct the attack—or the object of an attack: the target entity. See Figure 1-8. A computer can also be both the subject and object of an attack. For example, it can be compromised by an attack (object) and then used to attack other systems (subject).
- **Threat:** Any event or circumstance that has the potential to adversely affect operations and assets. The term threat source is commonly used interchangeably with the more generic term threat. The two terms are technically distinct, but to simplify discussion, the text will continue to use the term threat to describe threat sources.
- **Threat agent:** The specific instance or a component of a threat. For example, the threat source of "trespass or espionage" is a category of potential danger to information assets, while "external professional hacker" (like Kevin Mitnick, who was convicted of hacking into phone systems) is a specific threat agent. A lightning strike, hailstorm, or tornado is a threat agent that is part of the threat source known as "acts of God/acts of nature."
- **Threat event:** An occurrence of an event caused by a threat agent. An example of a threat event might be damage caused by a storm. This term is commonly used interchangeably with the term attack.
- **Threat source:** A category of objects, people, or other entities that represents the origin of danger to an asset—in other words, a category of threat agents. Threat sources are always present and can be purposeful or undirected. For example, threat agent "hackers," as part of the threat source "acts of trespass or espionage," purposely threaten unprotected information systems, while threat agent "severe storms," as part of the threat source "acts of God/acts of nature," incidentally threaten buildings and their contents.
- **Vulnerability:** A potential weakness in an asset or its defensive control system(s). Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door. Some well-known vulnerabilities have been examined, documented, and published; others remain latent (or undiscovered).

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Critical Characteristics of Information

I. Recognize that when a characteristic of information changes, the value of that information may increase but more so decreases.

II. Comprehend and define the following security terms and concepts: confidentiality, personally identifiable information (PII), integrity, availability, accuracy, authenticity, utility, and possession.

Confidentiality

I. Define the purpose of confidentiality and the measures that must be in place to protect information.

- Information classification
- Securely storing documents
- Applying general security policies and protocols
- Educating information custodians and end users

II. Analyze common reasons confidentiality breaches occur.

III. Review the concept of personally identifiable information (PII) and its application to confidentiality.

Integrity

I. Examine the concept of integrity and its application to information security principles.

II. Justify that file corruption is not strictly the result of hackers or other external forces but can include internal forces such as noise, low-voltage circuits, and retransmissions.

Availability

I. Define the concept of availability and how it allows users to access information without restriction in their required formats.

Accuracy

I. Understand that accuracy of data transmitted in information is important as it must be free of mistakes or errors, and it aligns with end user's expectations.

Authenticity

I. Identify the fact that information is authentic when it is given to a user in the same state that it was created, placed, stored, or transferred.

II. Evaluate the example of e-mail spoofing and how messages sent look authentic on the surface but are, in fact, not.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Utility

I. Examine the usefulness of information and how it can be applied for an end purpose.

Possession

I. Recall this attribute as one where the ownership or control of information has legitimacy or authorization.

II. Assess the scenario where a breach of possession does not always equate to a breach of confidentiality.

CNSS Security Model

I. Discuss the concept of the McCumber Cube and its application into computer and information security protocols.

- Quantify via Figure 1-9 (page 14) within the text that there are a total of 27 areas (3 x 3 x 3) that must be properly addressed during a security process.
- Understand the fact that as policy, education, and technology increase, so too the needs for confidentiality, integrity, availability, storage, processing, and transmission.

II. Conclude that a common exclusion in this model is the need for guidelines and policies that provide direction for implementation technologies and the practices of doing so.

Components of an Information System (1.3, PPT Slide 27)

I. Gain an understanding that to have a full understanding of the importance of an information system, one must have an awareness of what all is included within it.

II. Review the six most common elements of an information system.

- Software
- Hardware
- Data
- People
- Procedures
- Networks

Software

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

I. Compare and contrast the different types of software that are used to digitally operate an information system. These include applications or programs, operating systems, and assorted command utilities.
II. Justify the core reason that software is used is to carry information through an organization.

Hardware

I. Classify that this part of an information system is the physical technologies that house and execute software, stores and transports data, and provides an interface for entry and removal of information within it.
II. Acquire an understanding of the concept of physical security and its importance to an information system.

Data

I. Recall that data that is stored, processed, and/or transmitted must be protected as it is the most valuable asset an organization possesses.
II. Gain awareness that the protection of physical information is just as important as the protection of electronic information.

People

I. Establish that people are often the weakest link of an information system since they provide direction, design, develop, and ultimately use and game them to operate in the business world.

Procedures

I. Recall that procedures are written instructions that are created to accomplish a specific task or action. Note that they may or may not use the technology of an information system.
II. Recognize that they provide the foundation for technical controls and security systems that must be designed so they can be implemented.

Networks

I. Acknowledge the fact that modern information processing systems are highly complex and rely on numerous internal and external connections.
II. Conclude that networks are the highway in which information systems pass data and users complete their tasks on a daily basis.
III. Justify that proper network controls in an organization are vital to managing information flows and the security of data transmitted internally and externally.

Quick Quiz 1

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

1. True or False: Network security addresses the issues needed to protect items, objects, or areas.

   Answer: False

2. Which type of security addresses the protection of all communications media, technology, and content?

   a. information

   b. network

   c. physical

   d. communication

   Answer: d

3. Which type of security encompasses the protection of voice and data networking components, connections, and content?

   a. information

   b. network

   c. physical

   d. communications

   Answer: b

4. What term is used to describe the quality or state of ownership or control of information?

   a. confidentiality

   b. possession

   c. authenticity

   d. integrity

   Answer: b

5. True or False: If information has a state of being genuine or original and is not a fabrication, it has the characteristic of authenticity.

   Answer: True

Security and the Organization (1.4, PPT Slides 28–33, 36–38, and 41)

I. Analyze components that make up security as a program and the professionals who are tasked with maintaining it within an organization.

Balancing Information Security and Access

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

I. Recall that everyone does not have carte blanche access to all data that is transmitted, processed, or stored within or outside an organization.

II. Comprehend that security is never an absolute as it is a process and not a goal.

III. Interpret that security is a delicate balance between protection and availability.

Approaches to Information Security Implementation

I. Compare and contrast the two most commonly used approaches to information security implementation: bottom-up and top-down.

- Bottom-up approaches implement security policies and/or policies from the ground up where system administrators are responsible for improving the security of the system.
- A top-down approach is quite the opposite where upper management determines security policies for an organization. This is usually the Chief Information Officer (CIO) or the Vice President of Information Technology (VP-IT).

II. Conclude that often a bottom-up approach rarely works, and a top-down approach has the most effectiveness in an organization.

Security Professionals

I. Compare and contrast the different positions that are part of an implementation for an information security program.

- The Chief Information Officer (CIO) is the senior technology officer of an organization and provides guidance to the owner or CEO strategic planning that affects information management in an organization.
- The Chief Security Officer (CISO) assesses, manages, and implements information security in an organization.

Senior Management

I. Examine that the Chief Information Officer (CIO) is the senior technology officer although other titles such as vice president of information, VP of information technology, and VP of systems may also be used. The CIO is primarily responsible for advising the chief executive officer, president, or company owner on the strategic planning that affects the management of information in the organization.

II. Contrast with the CIO that the Chief Information Security Officer (CISO) is the individual primarily responsible for the assessment, management, and implementation of securing the information in the organization. The CISO may also be referred to as the manager for security, the security administrator, or a similar title.

Information Security Project Team

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

I. Review the core team members of an information security project team and their specific role:

- **Champion:** A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.
- **Team leader:** A project manager, who may be a departmental line manager or staff unit manager and who understands project management, personnel management, and information security technical requirements.
- **Security policy developers:** Individuals who understand the organizational culture, policies, and requirements for developing and implementing successful policies.
- **Risk assessment specialists:** Individuals who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used.
- **Security professionals:** Dedicated, trained, and well-educated specialists in all aspects of information security from both a technical and nontechnical standpoint.
- **Systems administrators:** Individuals whose primary responsibility is administering the systems that house the information used by the organization.
- **End users:** Those whom the new system will most directly impact. Ideally, a selection of users from various departments, levels, and degrees of technical knowledge assist the team in focusing on the application of realistic controls applied in ways that do not disrupt the essential business activities they seek to safeguard.

Data Responsibilities

I. Compare and contrast persons who own and safeguard data within an organization.

- **Data Owners:** Those responsible for the security and use of a particular set of information. Data owners usually determine the level of data classification associated with the data, as well as changes to that classification required by organizational change.
- **Data Custodians:** Those responsible for the storage, maintenance, and protection of the information. The duties of a data custodian often include overseeing data storage and backups, implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the data owner.
- **Data Trustees**: Individuals appointed by data owners who oversee the management of an information set and its use. Though these are often executives, they appoint someone else to handle these responsibilities.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

- **Data Users:** End users who work with the information to perform their daily jobs supporting the mission of the organization. Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

II. Recall that data stewards are also known as data custodians.

Communities of Interest

I. Establish an understanding that each organization develops and maintains its own unique culture and values.
II. Recall that a community of interest is a group of individuals who are united by similar interests or values within an organization and who share a common goal of helping the organization to meet its objectives.
III. Disseminate the fact there can be many different communities of interest in an organization which aid in information security practices.

Information Security Management and Professionals

I. Apply knowledge that these professionals are aligned with an information security's community of interest.

II. Review the fact that their goal is to protect an organization's information and stored information from internal and external attacks.

Information Technology Management and Professionals

I. Recognize that these individuals are often a team of IT managers and skilled professionals in a number of areas: systems design, programming, and networks at a minimum.

II. Establish an understanding their goals do not always align with the information security community based on an organization's structure. Conflict may result if there are inconsistencies between them.

Organization Management and Professionals

I. Analyze that this group of persons in an organization are often other managers and professionals who are consumers of information being secure.

Information Security: Is It an Art or a Science? (PPT Slides 42–43)

I. Gain an understanding that the implementation of information security has often been described as a combination of art and science due to the complex nature of information systems.
II. Discuss the concept of a "security artisan" and explain how it is based on the way individuals see technologists as computers became more commonplace in the workplace.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Security as Art

I. Recognize that there are no hard and fast rules regulating the installation of various security mechanisms, nor are there many universally accepted complete solutions.
II. Conclude that there is no one user's manual that can solve all security issues that a system may encounter. As an organization becomes more complex, so do the controls and technology needed to keep it together.

Security as a Science

I. Establish an understanding that technologies that are developed are enacted by highly trained computer scientists and engineers who are required to operate at rigorous levels of performance.
II. Conclude that specific scientific conditions often cause virtually all actions that occur in a computer system. Nearly everything that negatively occurs in a system is a result of an interaction between software and hardware.
III. Justify that with enough time and resources, developers could eliminate faults that occur.

Security as a Social Science

I. Understand a combination of both components of art and science make security a social science.
II. Identify a social science as the examination of people's behavior and their interactions with (information) systems.
III. Conclude that end users who need the information security personnel protect are often the weakest links in the security chain.

Quick Quiz 2

1. When projects are initiated at the highest levels of an organization and then pushed to all levels, they are said to follow which approach?
   b. executive-led
   c. trickle down
   d. top-down
   e. bottom-up

   Answer: c
2. _____ ensures that only users with the rights, privileges, and need to access information are able to do so.
   a. confidentiality
   b. enhanced credentials
   c. software engineers

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

d. awareness

Answer: a

3. True or False: The person responsible for the storage, maintenance, and protection of the information is the data custodian.

   Answer: True

4. Which critical characteristic of information discussed is one that focuses on the fact when information stored, transferred, created, or placed is in the same state as it was received?

   a. utility

   b. possession

   c. accuracy

   d. authenticity

   Answer: d

5. Which of the following examines the behavior of individuals as they interact with systems, whether societal systems or information systems?

   a. community science

   b. social science

   c. societal science

   d. interaction management

   Answer: b

[return to top]

Discussion Questions

You can assign these questions several ways: in a discussion forum in your LMS, as whole-class discussions in person, or as a partner or group activity in class.

These questions are separate from the review questions and exercises in the textbook. For answers to the textbook questions, see the associated solutions for this module.

Additional class discussion options:

1. What are the defining differences between computer security and information security? (1.2, PPT Slides 5, 7–9, and 13) Duration 15 minutes.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

2. When reviewing the critical characteristics of information, which one is the most important? Why is that the case and should all receive equal attention? (1.3, PPT Slides 18 and 25–26) Duration 15 minutes.
3. Do information security professionals have superiority over one another outside of their ranking in an organization? Why or why not? (1.4, PPT Slides 29–33) Duration 15 minutes.

[return to top]

Suggested Usage for Lab Activities

A series of hands-on labs has been developed to complement the text material for this course and are available for download at the Instructor Center. The labs do not depend on specific chapter content, so instructors can insert them where they best suit the syllabus. The following is a list of lab titles, objectives, and approximate durations to assist with lesson planning.

Lab Title	Objective	Duration
Ethical Considerations in IT and Detecting Phishing Attacks	Upon completion of this activity, you will: • have a better understanding of the ethical expectations of IT professionals; and • be able to identify several types of social engineering attacks that use phishing techniques.	Ethical Considerations lab in 15 to 20 minutes. Phishing E-Mail lab in 60 to 75 minutes.
Web Browser Security	Upon completion of this activity, the student will be able to: • Review and configure the security and privacy settings in the most popular web browsers.	1 to 1.5 hours
Malware Defense	Upon completion of this activity, the student will be able to: • Understand the basic setup and use of an open-source AV product. • Install and use Clam AV on a Windows system. • Using a USB storage device create a portable AV scanner. • Understand what a YARA file is and how it is used.	1 to 1.5 hours

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Windows Password Management	Upon completion of this activity, the student will be able to: • Review and configure password management policies in a Windows client computer.	30 minutes to 1 hour
Backup and Recovery and File Integrity Monitoring	Upon completion of this activity, you will be able to: • Describe backup and recovery processes and will be aware of basic backup activities using Windows 10 or another desktop operating system (OS). • Perform file integrity monitoring using file hash values.	15–20 minutes
OS Processes and Services	Upon completion of this activity, the student will be able to: • Review available and enabled OS services. • Review available and enabled OS processes. • Review current system resource utilization.	60–90 minutes
Log Management & Security	Upon completion of this activity, the student will be able to: • Access and review the various logs present in a Windows 10 computer.	30 minutes to 1 hour
Footprinting, Scanning, and Enumeration	Upon completion of this activity, the student will be able to: • Identify network addresses associated with an organization. • Identify the systems associated with the network addresses.	40–60 minutes
AlienVault OSSIM	Upon completion of this activity, the student will be much more knowledgeable about the AlienVault OSSIM software and how to install, configure, and operate it. You will use the software more extensively in a subsequent lab.	2–3 hours

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Image Analysis Using Autopsy	Upon completion of this activity, the student will be able to perform basic drive image analysis using the Autopsy software package.	45–70 minutes

[return to top]

Additional Activities and Assignments

Please see associated solutions for the Closing Scenario at the end of the textbook module.

Additional project options include the following:

1. Using the Internet, find a recent feature article about a CISO or other IT professional with CISO job functions. Write a short summary of that individual and how he or she came to hold that position. The publications ComputerWorld and Information Week often have these kinds of features. Have students list the hardware assets found in a computing lab and then list the attributes of those assets. They should provide as many facts about each asset as possible.
2. Using a library with current periodicals, find a recent news article about a topic related to information security. Write a one- to two-page review of the article and how it is related to the principles of information security introduced in the textbook.

[return to top]

Additional Resources

Cengage Video Resources

- MindTap Video: What is Information Security

Internet Resources

- Internet Society—Histories of the Internet
- CNSS National Information Assurance Glossary
- Microsoft Security Development Lifecycle
- The Role of a Chief Security Officer

[return to top]

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Appendix

Grading Rubrics

Providing students with rubrics helps them understand expectations and components of assignments. Rubrics help students become more aware of their learning process and progress, and they improve students' work through timely and detailed feedback.

Customize these rubrics as you wish. The grading rubric suggests a 4-point scale and the discussion rubric indicates 30 points.

Grading Rubric These grading criteria can be applied to open-ended Review Questions, Real-World Exercises, Case Studies, and Security for Life activities			
3 Exceeds Expectations	2 Meets Expectations	1 Needs Improvement	0 Inadequate
• Student demonstrates accurate understanding of the concept. • Student applies the concept appropriately. • Student uses sound critical analysis to develop an insightful and comprehensive response to the prompt.	• Student demonstrates accurate understanding of the concept. • Student applies the concept appropriately. • Student develops a complete response to the prompt.	• Student's response demonstrates a gap in understanding of the concept. • Student applies the concept incorrectly. • Student's response is poorly developed or incomplete.	• Student's response is missing or incomplete. • Student's response demonstrates a critical gap in understanding. • Student is unable to apply the concept.

[return to top]

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible website, in whole or in part.

Hands-On Lab: Ethical Considerations in IT and Detecting Phishing Attacks

To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 978-0-357-50643-1; Ethical Considerations in IT and Detecting Phishing Attacks

Table of Contents

Objective 2
Estimated Completion Time 2
Materials Required 2
Introduction 2
Ethical Considerations in the Use of Information Security Tools 3
Are You a White Hat? 3
The White Hat Agreement 4
(ISC)^2 Code of Ethics 5
Self-Reflection and Response 7
Instructor's Response 7
Detecting and Responding to Phishing Attacks 8
Legitimate Messages Don't Request Sensitive Information 8
Legitimate Messages Usually Call You by Your Name 9
Legitimate Messages Come from Authentic Domains 10
Legitimate Messages Come from People Who Know How to Spell and Write 11
Legitimate Messages Don't Force You to a Web Site 12
Legitimate Messages Don't Include Unsolicited Attachments 13
Legitimate Messages Have Links that Match Legitimate URLs 13
Legitimate Messages Don't Create an Artificial Sense of Urgency 14
Legitimate Messages Display Reliable Names 15
Legitimate Messages Don't Solicit Money 16
How You Should Respond to Phishing E-Mails 18
Test Your Knowledge 19
Instructor's Response: 26

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Objective

Upon completion of this activity, you will:

- have a better understanding of the ethical expectations of IT professionals; and
- be able to identify several types of social engineering attacks that use phishing techniques.

Estimated Completion Time

If you are prepared, you should be able to complete:

- The Ethical Considerations lab in 15 to 20 minutes.
- The Phishing E-Mail lab in 60 to 75 minutes.

Materials Required

Completion of this lab does not require any software to be installed and configured on your computer.

Introduction

This module does not include a "hands-on" project to develop specific skills. Instead, it discusses two topics that will be useful for the projects you perform in the later modules. You will first learn about the ethical dimension of using information security tools and techniques that many consider to be from the "dark side."

Social engineering is a term to describe malicious actions that exploit human psychology to gain access to sensitive information or money. Attackers manipulate people through dishonest social interactions and exploit the human tendency to trust to gather valuable information.

Phishing is a popular form of social engineering attack in which an attacker provides what appears to be a legitimate communication (usually e-mail), but it contains hidden or embedded code that redirects the reply to a third-party site to extract personal or confidential information.

The best defense against e-mail phishing attacks is user awareness. Many organizations now filter employee e-mail using commercial products, but even the best of these products will not stop every phishing e-mail. Having an alert workforce and a trained service support staff are also required.

In the second part of this lab, you will begin by reading about the indicators that an e-mail is actually a phishing attack. Next, you will assume the role of a help-desk analyst who is responding to alerts from users that have received suspicious e-mails.

[return to top]

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Ethical Considerations in the Use of Information Security Tools

Using some of the "tools of the trade" in information security might lead students (and their instructors) to use software and techniques that are designed to break the rules and allow bad acts to occur. Because each academic community sets certain standards, you need to be aware of how they might apply in your specific circumstances.

Conformance to standards and exhibiting ethical behavior is required to ensure the unhindered pursuit of knowledge and the free exchange of ideas. Academic integrity means that you respect the right of other individuals to express their views and opinions, and that you, as a student or faculty member, do not engage in plagiarism, cheating, illegal access, misuse or destruction of college property, or the falsification of college records or academic work.

As a member of the academic community, and as a future InfoSec or IT professional, you are expected to adhere to standards of ethical behavior. You are expected to read and follow your institution's code of conduct, which usually is found in your student handbook. You need to be aware that if you violate these standards, you will be subject to penalties outlined in your institution's student conduct and academic integrity procedures. These penalties likely range from grade penalties to permanent expulsion.

Your instructor may require you to read the white hat agreement and code of ethics that follow. Your instructor might also ask you to sign a form acknowledging that you agree to abide by these ethical standards while you are a student. Your agreement would indicate that you understand the ethical behavior expected of you as part of an academic community, and that you understand the consequences of violating those standards. For those of you in InfoSec or cybersecurity programs, the standard is even higher, given that you will be a guardian of an organization's data in the future.

Are You a White Hat?

As part of this course, you may be exposed to systems, tools, and techniques related to information security. With proper use, these components allow a security administrator or technician to better understand vulnerabilities and the security precautions used to defend an organization's information assets. Misuse of these components, either intentionally or accidentally, can result in breaches of security, damage to data, or other undesirable results.

Because the labs in this book will sometimes be carried out in a public network that is used by people for real work, you must agree to the following before you can participate. If you are unwilling to sign this agreement, your instructor may not allow you to participate in the projects.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Hands-On Lab: To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 978-0-357-50643-1; Ethical Considerations in IT and Detecting Phishing Attacks

The White Hat Agreement

If you have questions about any of the following guidelines, please contact your instructor. This document may be changed from time to time by your instructor, who will notify you of such changes and may ask you to reaffirm your understanding and agreement.

1. Just because you *can* do something doesn't mean you *should*.
2. As you engage in projects, you will be granted access to tools and training that have the potential to do harm even when they are used to determine or investigate the security of an information system. Use these tools with care and consideration of their impact, and only in the ways specified by your instructor.
3. If any question arises in your mind about whether you can or should perform an activity or use a tool in a particular way, stop and ask your instructor for clarification. In information security, it is most definitely NOT easier to ask for forgiveness than for permission.
4. You are only allowed to use the tools and exercises if you are currently registered for a grade in the course. An instructor always has the right to ask students for appropriate identification if necessary.
5. Any instance of suspected misconduct, any illegal or unauthorized use of tools or exercises, or any action construed as being outside the guidelines of the course syllabus and instruction will be investigated by the instructor and may result in severe academic and/or legal penalties. Being a student does not exempt you from consequences if you commit a crime.
6. All students are expected to follow the $(ISC)^2$ code of ethics, which is available at *www.isc2.org/ethics* and included later in this document.
7. By acknowledging this agreement, you confirm that you *will:*
    - Only perform the actions specified by the course instructor for using security tools on assigned systems.
    - Report any findings to the course instructor or in specified reporting formats without disclosing them to anyone else.
    - Maintain the confidentiality of any private information learned through course exercises.
    - Manage assigned course accounts and resources with the understanding that their contents may be viewed by others.
    - Hold harmless the course instructor and your academic institution for any consequences or actions if you use course content outside the physical or virtual confines of the specified laboratory or classroom.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

- Abide by the computing policies of your academic institution and by all laws governing the use of computer resources on campus.

8. By acknowledging this agreement, you confirm that you *will not:*
   - Attempt to gain access to a system, attempt to increase privileges on any system, or access any data without proper authorization.
   - Disclose any information that you discover as a direct or indirect result of this course exercise.
   - Take actions that will modify or deny access to any system, data, or service except those to which administrative control has been delegated to you.
   - Attempt to perform any actions or use utilities presented in the laboratory outside the confines and structure of the projects or classroom.
   - Use any security vulnerabilities beyond the target accounts in the course or beyond the duration of the course exercise.
   - Pursue any legal action against the course instructor or the university for any consequences or actions if you use what you learn in the course outside the physical or virtual confines of the laboratory or classroom.
9. You will abide by the following code of ethics:

   Safety of the commonwealth, duty to our principles, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

(ISC)² Code of Ethics

Protect society, the common good, necessary public trust and confidence, and the infrastructure.

- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

Act honorably, honestly, justly, responsibly, and legally.

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.
- Treat all constituents fairly. In resolving conflicts, consider public safety and duties to principles, individuals, and the profession in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Provide diligent and competent service.

- Preserve the value of systems, applications, and information.
- Respect the trust and privileges granted to you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

Advance and protect the profession.

- Sponsor for professional advancement those best qualified. All other things being equal, prefer those who are certified and who adhere to these canons.
- Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

The ISC^2 code of ethics is available from **www.isc2.org/ethics**.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Self-Reflection and Response

In the space below, write a brief statement indicating your intention to abide by the ethics codes spelled out in this lab.

Instructor's Response

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Detecting and Responding to Phishing Attacks

The following questions indicate some of the telltale signs of phishing attacks. In general, you should ask yourself these questions for each e-mail you receive:

- Does the message ask for sensitive information, such as account numbers, passwords, or even your birthday?
- Does the message use your correct name and refer to other details accurately?
- Does the address look authentic?
- Are there misspelled words and improper grammar?
- Does the message force you to a web site?
- Does the message have an attachment you are not expecting?
- Do links in the message fail to match the visible URL?
- Does the message request that you send money?

Each of these questions is explained with examples in the following sections.

Legitimate Messages Don't Request Sensitive Information

If you receive an unsolicited e-mail that appears to be from an official institution and the message includes a functional link or attachment, it's a scam. Most companies do not send e-mail asking for passwords, credit card information, credit scores, or tax numbers, nor do they send log-in links. If a company needs information, you will usually be asked to visit its web site or mobile app, but you should not need a special e-mail link—after all, you do business with the company already.

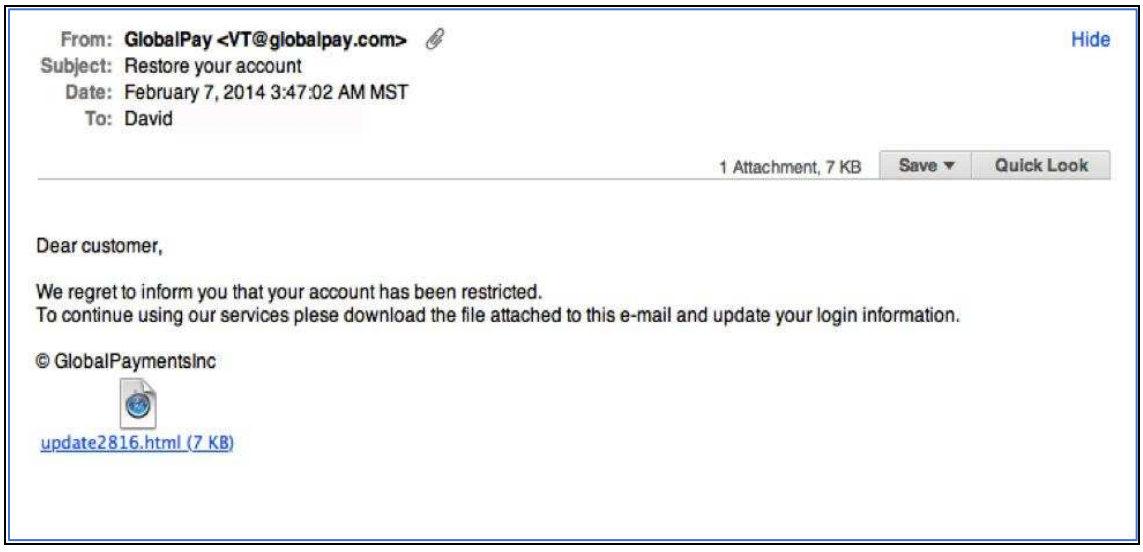


Figure L01-1 Global Pay Phishing E-Mail

In Figure L01-1, notice the unsolicited web link attachment. Also, look at the generic salutation at the beginning ("Dear customer"). Such greetings are discussed next.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Legitimate Messages Usually Call You by Your Name

Phishing e-mails typically use generic salutations such as “Dear valued member,” “Dear account holder,” or “Dear customer.” If a company you deal with actually required information about your account, the e-mail would refer to you by name and would probably direct you to contact the company via phone, a phone app, or the official company web site.

However, some hackers simply avoid a salutation altogether. This is especially common with advertisements. In the phishing e-mail shown in Figure L01-2, everything is nearly perfect. So, how would you spot it as suspicious?

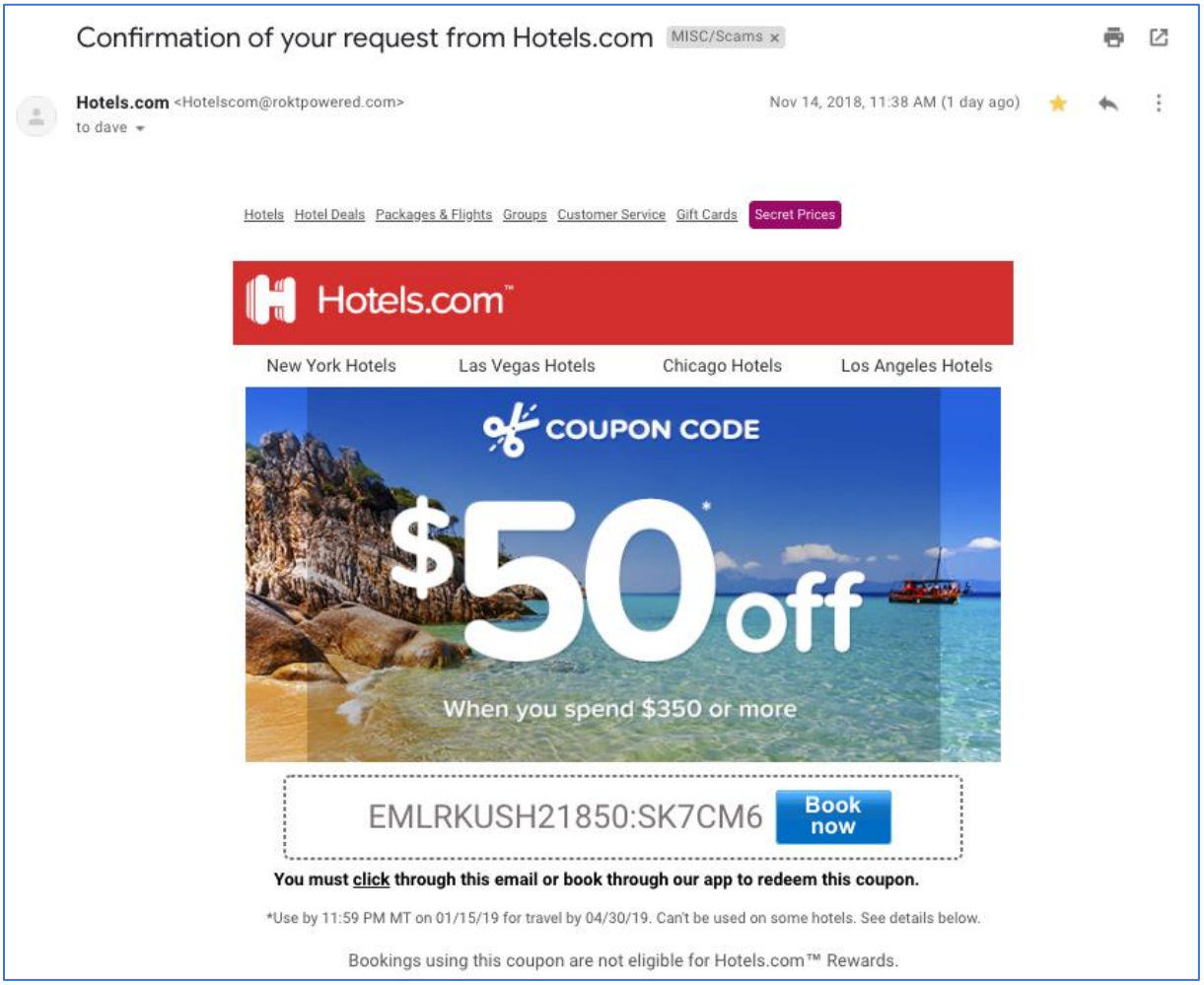


Figure L01-2 Hotels.com Phishing E-Mail

The example in Figure L01-2 is very convincing, but the fact that the message has the recipient’s name spelled correctly does not make it legitimate. The clue that the message is not legitimate is indicated by the e-mail domain, as you will learn next.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Legitimate Messages Come from Authentic Domains

Don't just check the name of the person who sent you the e-mail. Check the e-mail address by hovering your mouse over the contents of the From line. Make sure there have been no alterations, such as additional numbers or letters. For example, be suspicious if the e-mail address appears to be ***michelle@paypal.com*** but is ***michelle@paypal23.com*** when you hover the mouse over the From line. This isn't a foolproof method of demonstrating fraud, however. Some companies make use of varied domains to send e-mails, and some smaller companies use third-party e-mail providers.

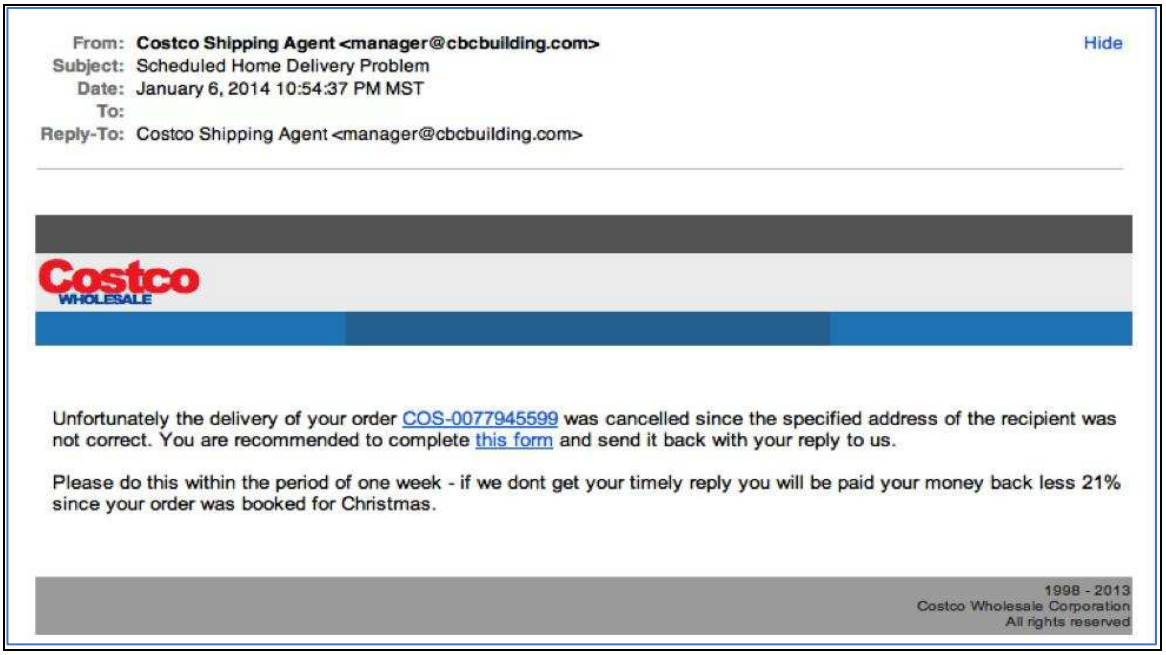


Figure L01-3 Costco Phishing E-Mail

In the example shown in Figure L01-3, the Costco logo is just a bit off. To see the actual logo, you can go to **https://costco.com**. Do you see the difference?

Also, note the "From" field is from a different business: "cbcbuilding.com" rather than "costco.com"

Also, note that most companies use the *https://* service in their URLs. If the "s" is missing, dig a little deeper.

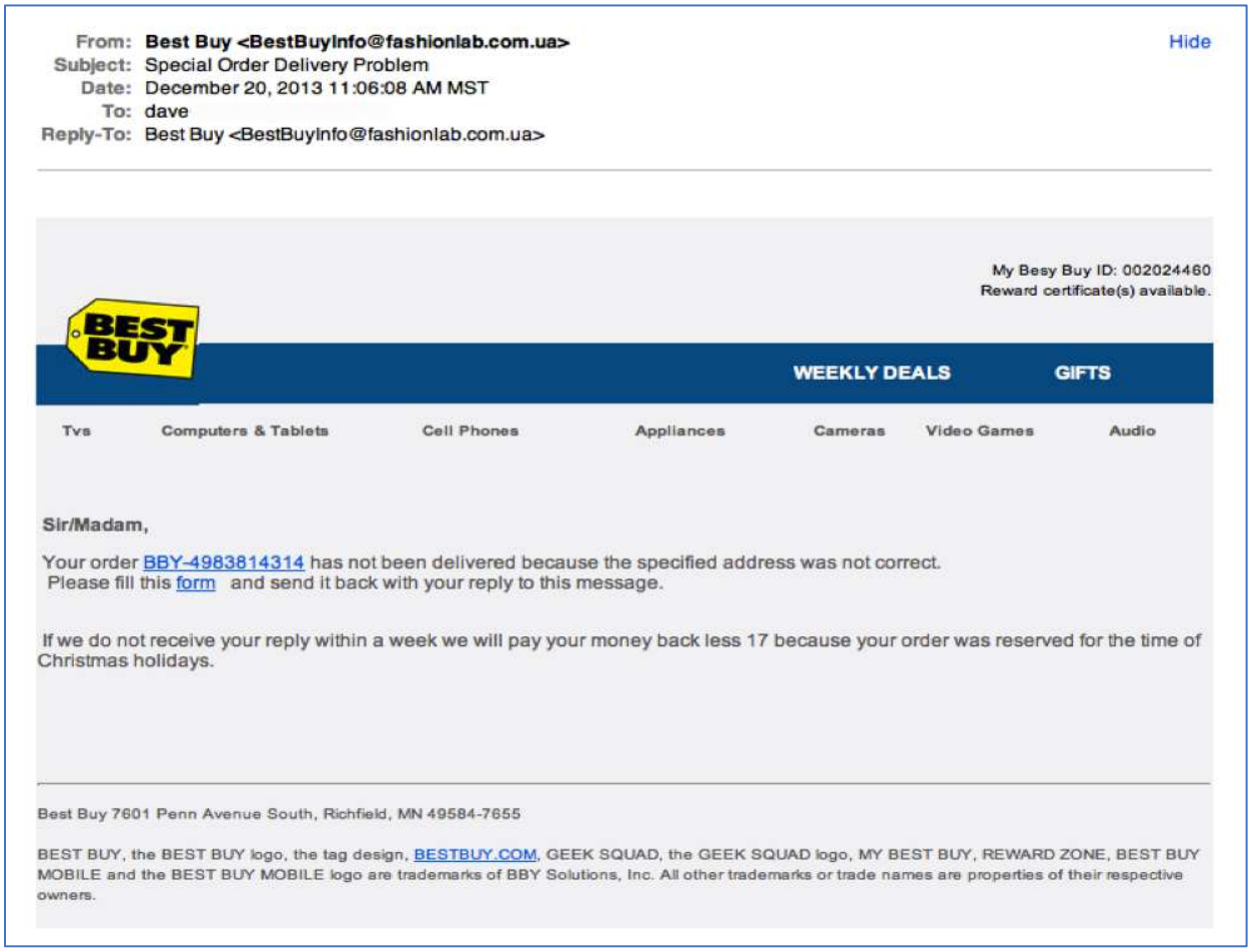
© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Legitimate Messages Come from People Who Know How to Spell and Write

Possibly the easiest way to recognize a suspicious e-mail is through its use of bad grammar and misspelled words. An e-mail from a legitimate organization is usually well written.

Look at this example:



From: **Best Buy <BestBuyInfo@fashionlab.com.ua>** Hide
Subject: Special Order Delivery Problem
Date: December 20, 2013 11:06:08 AM MST
To: dave
Reply-To: Best Buy <BestBuyInfo@fashionlab.com.ua>

My Besy Buy ID: 002024460
Reward certificate(s) available.

BEST BUY

WEEKLY DEALS GIFTS

Tvs Computers & Tablets Cell Phones Appliances Cameras Video Games Audio

Sir/Madam,

Your order BBY-4983814314 has not been delivered because the specified address was not correct.
Please fill this form and send it back with your reply to this message.

If we do not receive your reply within a week we will pay your money back less 17 because your order was reserved for the time of Christmas holidays.

Best Buy 7601 Penn Avenue South, Richfield, MN 49584-7655

BEST BUY, the BEST BUY logo, the tag design, BESTBUY.COM, GEEK SQUAD, the GEEK SQUAD logo, MY BEST BUY, REWARD ZONE, BEST BUY MOBILE and the BEST BUY MOBILE logo are trademarks of BBY Solutions, Inc. All other trademarks or trade names are properties of their respective owners.

Figure L01-4 Best Buy Phishing E-Mail

In addition to the generic salutation in Figure L01-4, the grammar gaffes and extra spaces are a good clue that something is wrong—for example, note the sentence that begins “Please fill this form.” Also, notice the “17” that appears in the middle of the next sentence for no reason.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Legitimate Messages Don't Force You to a Web Site

Phishing e-mails are sometimes coded so that the entire message is a graphic image tagged as a hyperlink. Clicking anywhere in the e-mail will open a fake Web page or download malware, ransomware, or spam to your computer. For this reason, you must be careful and deliberate when performing analysis on suspect e-mails. If you click or activate the attachment, it can infect your system. You will need tools to render the attachment or headers harmless without activating the trap. Right clicking your mouse and using basic tools can be very helpful.

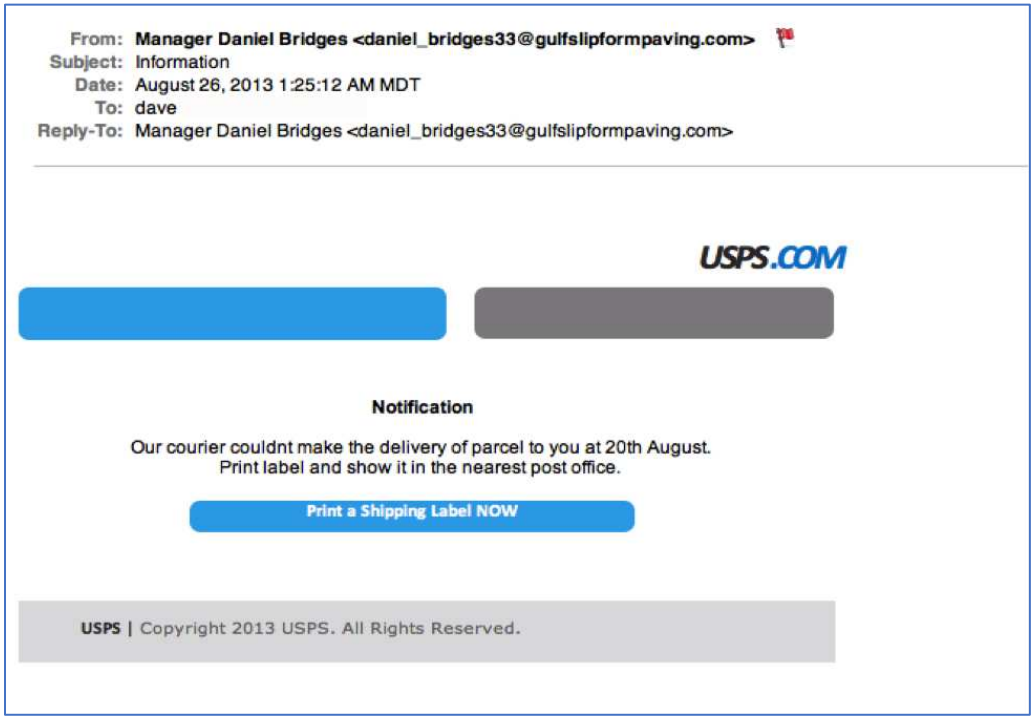


Figure L01-5 USPS Phishing E-Mail

The entire e-mail shown in Figure L01-5 was sent as an image tagged as a single hyperlink. If a recipient clicked anywhere in the e-mail, a malicious attack would be initiated. You can guard against this by hovering your mouse cursor over the message to see if a link address preview appears. You can also see the spelling and grammar errors in the body of the "Notification."

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Legitimate Messages Don't Include Unsolicited Attachments

Unsolicited e-mails that contain any type of attachment should make you suspicious. Typically, authentic institutions do not randomly send you e-mail with attachments, but instead direct you to download documents or files from their secured web site.

Like many of the other tips in this lab, this method isn't foolproof. Companies that already have your e-mail address sometimes send you information, such as a white paper, that may require a download. In that case, be on the lookout for high-risk attachment file types, such as .exe, .scr, and .zip. Even .pdf and .docx files are suspicious. If you think the e-mail might be legitimate but you have doubts, contact the sender directly using information obtained from a source other than the e-mail.

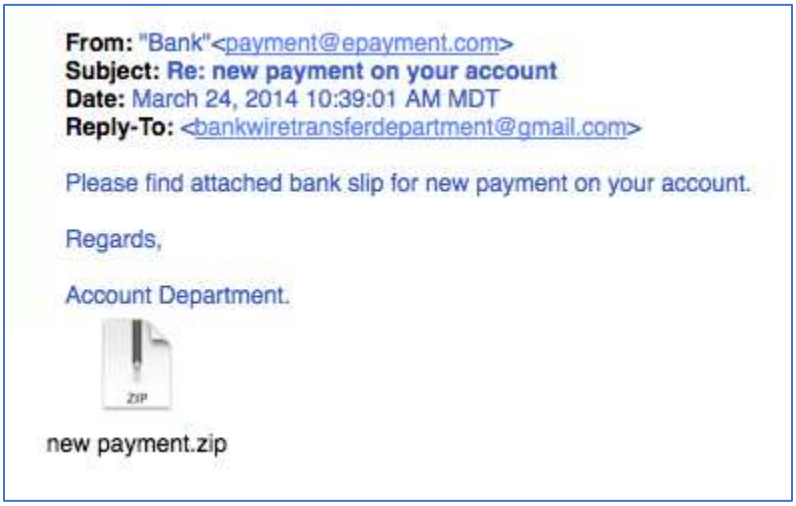


Figure L01-6 ePayment Phishing E-Mail

Before you wonder what's in the .zip file attached in Figure L01-6, remember that curiosity killed the cat.

Legitimate Messages Have Links that Match Legitimate URLs

If an e-mail appears to be suspicious, take precautions with any web links in the message. Make a habit to always double-check URLs. If the link in the text isn't identical to the URL displayed when you hover the mouse cursor over the link, that's a sure sign you will be taken to a site you don't want to visit. If a hyperlink's URL doesn't seem correct or doesn't match the context of the e-mail, don't trust it. Instead, use your web browser to find the company's authentic web site. To help ensure security, hover your mouse over an embedded link (without clicking!), confirm that it begins with *https://*, and consider whether the rest of the link looks like what you might expect.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

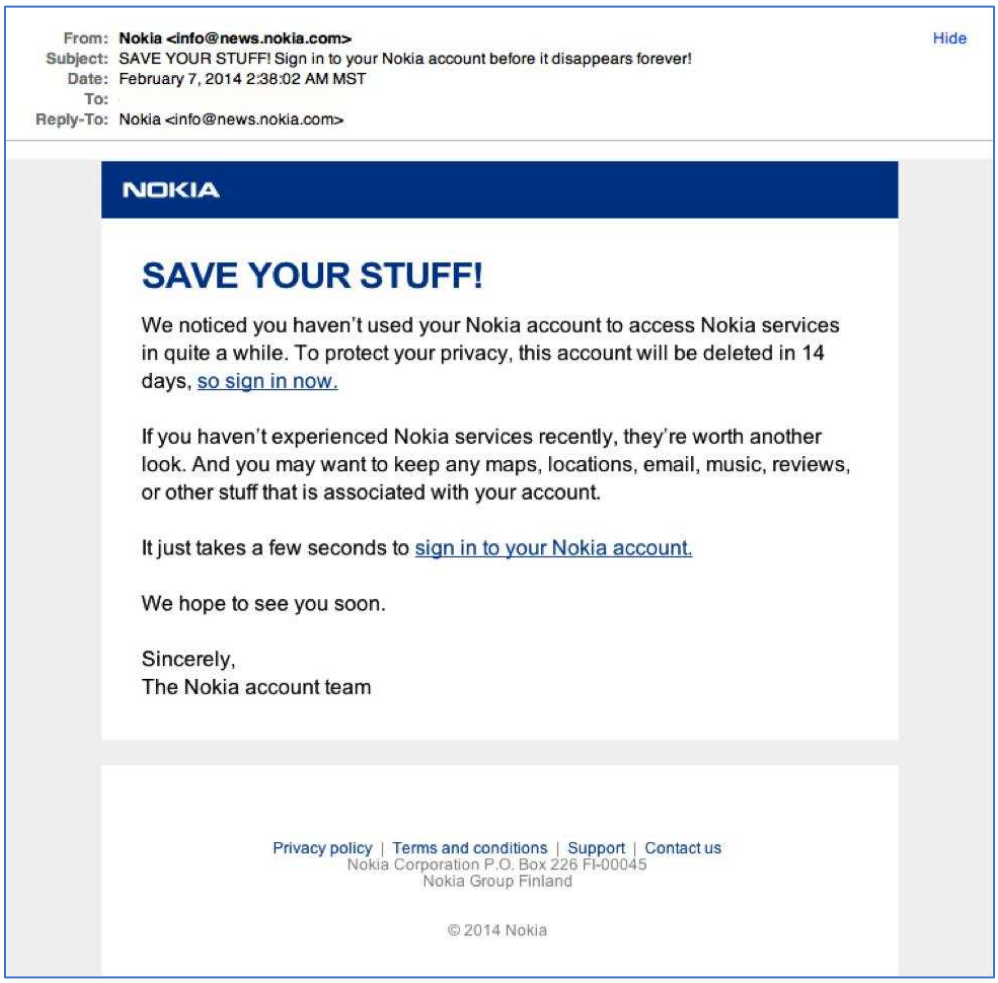


Figure L01-7 Nokia Phishing E-Mail

Although the preceding message looks convincing, Nokia wouldn't actually send a "Save your stuff" e-mail from *info@news.nokia.com*. A mouse flyover of the link would show a domain you should not trust.

Legitimate Messages Don't Create an Artificial Sense of Urgency

Scammers know that most of us procrastinate and then have to get things done in a hurry so many phishing attempts request that we act now before it's too late. Scammers also understand that crises in the workplace are common and must be handled quickly. Unfortunately, hurrying creates a greater chance of making mistakes and bad choices.

When you take time to think about something, you are much more likely to notice things that don't seem quite right. For instance, when you receive an unexpected e-mail from a major company, maybe you'll think twice and realize that the organization has never contacted you via e-mail. Maybe you'll receive what appears to be a frantic e-mail from a co-worker and realize that he simply would have called you in case of an actual emergency.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

A common workplace scam is to pretend that a problem has arisen with a commonly used service or account, such as that with a bank or credit card company an organization uses. Any actual problems with such accounts would cause an immediate inconvenience. Criminals know we're likely to drop everything if our boss e-mails us with a vital request, especially when other senior colleagues are supposedly waiting for us to act.

A typical example looks like Figure L01-8.

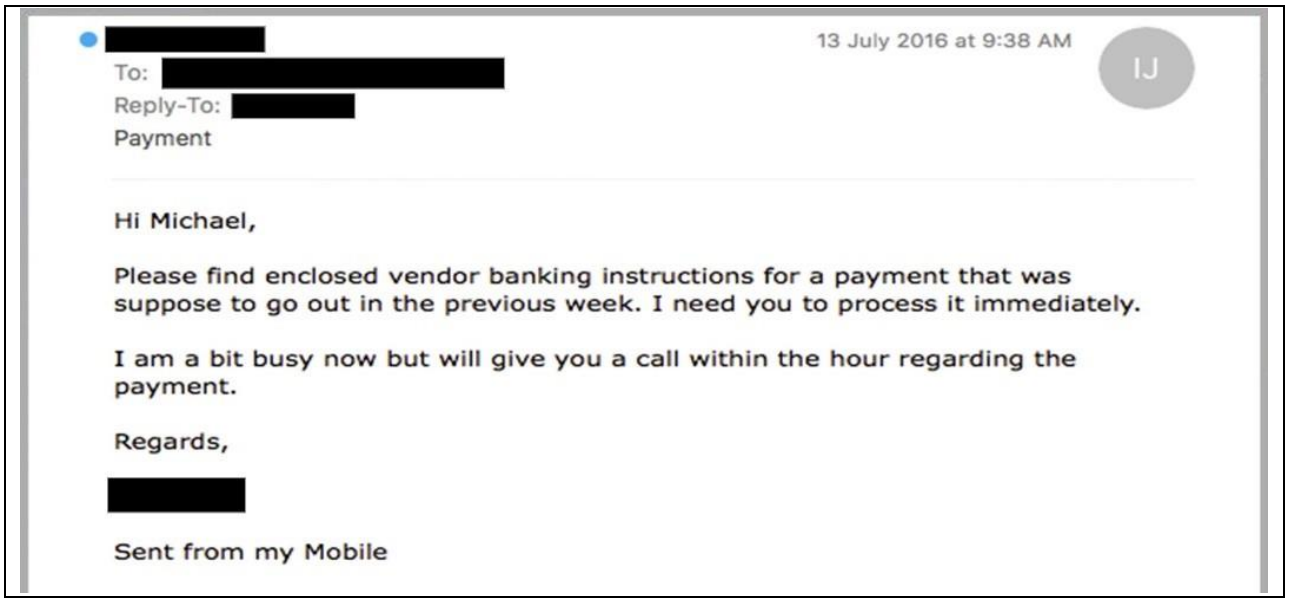


Figure L01-8 Mobile Phishing E-Mail

Legitimate Messages Display Reliable Names

A favorite phishing tactic among cybercriminals is to spoof the display name of an e-mail, just like robocalling telemarketers can spoof your phone's caller ID. For example, if a fraudster wanted to impersonate your bank, the top of the e-mail message might look like Figure L01-9. Check out the domain name (in the example, ***accounts@secure.com***) to see if it matches the display name (My Bank).

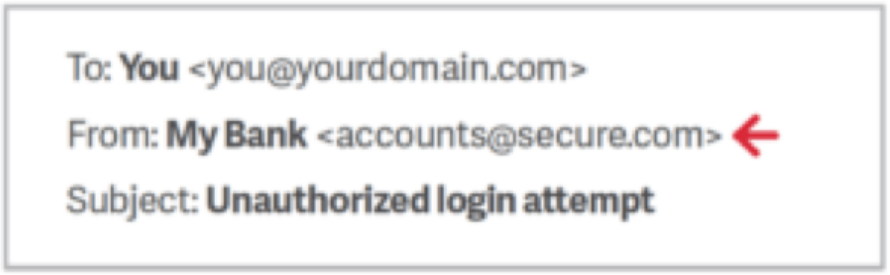


Figure L01-5 Secure.com Phishing E-Mail

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Legitimate Messages Don't Solicit Money

Many successful phishing attacks create a false sense of urgency or appeal to a person's greed. One type of scam that attempts to exploit greed is the advance fee fraud, which uses confidence tricks and is much older than e-mail. This approach typically involves promising the victim a significant share of a valuable prize, a desired business objective, or a sum of money in return for a small, up-front payment. This payment is needed to obtain the larger sum—hence the name "advance fee fraud."

One of the best-known frauds is the Nigerian 4-1-9 scam, which has been around for a long time. Originally conducted via phone, fax, and traditional mail, this scam invites victims to send a small amount of money with the promise of receiving a much larger sum in return. The development of e-mail has made it much easier for scammers to reach new victims. The best-known source of these e-mail scams is Nigeria, although they can originate from anywhere. In Nigeria, the e-mails have become a significant source of income for some, although section 4-1-9 of the Nigerian legal code prohibits them (hence the name).

A typical Nigerian 4-1-9 scam begins with a potential victim opening a letter or e-mail that's purportedly from a famous person or an exiled politician. The person may claim to be from a place that's currently in the news, possibly because of a recent civil disturbance. The message explains that, due to political instability or the death of a relative, a significant amount of money is trapped in some form of escrow account. The message goes on to explain that if the reader could send just a small amount of cash, it will pay the fee needed to access the account. In return for their trust and generosity, the reader is promised a large percentage of the money that's locked away.

If the reader does decide to send money, more requests will follow. According to subsequent e-mails sent by the scammer, unexpected costs are often discovered, such as increased taxes or bribes to officials. The scammers will continue to ask for money as long as the victim sends it. Needless to say, victims will never receive a payout, regardless of how much money they send.

A variant of the 4-1-9 attack involves vendors that supposedly sell products or rent accommodations online. A fraudster first identifies a company from a foreign country that offers to buy a product, rent a property, or contract a service. The fraudster then sends the victim a fake check or international money order for a much greater amount than the item or activity is worth, along with an explanation for why they cannot pay a smaller amount. The fraudster asks the victim to deposit the money in a personal bank account and then transfer the overage back to the fraudster. Later, of course, the victim discovers the swindle and that the original "payment" was fake.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

These types of scams have some common traits:

- The message (usually an e-mail) is unexpected.
- You don't know the sender.
- There is a long, sad story about why the sender needs your help to access money.
- You are asked to help by transferring funds.
- A large payment is offered in exchange for assistance.

The examples of advance fee fraud are many and varied; they include investment proposals, lottery winnings, and online dating scams. The example shown in Figure L01-10 is fairly typical.



[EXTERNAL] Partnership

M

Ms E. A Alhashimy <office1@hiiragi.or.jp>
Tue 2020-09-29 18:29
To: Recipients <office1@hiiragi.or.jp>

Hello,

My name is Reem E. Al-Hashimi, the Emirates Minister of State and Managing Director of the United Arab Emirates (Dubai) World Expo 2020 Committee. I am writing to you to stand as my partner to receive my share of gratification from foreign companies whom I helped during the bidding exercise towards the Dubai World Expo 2020 Committee and also i want to use this funds to assist Coronavirus Symptoms and Causes.

Am a single Arab women and serving as a minister, there is a limit to my personal income and investment level and For this reason, I cannot receive such a huge sum back to my country or my personal account, so an agreement was reached with the foreign companies to direct the gratifications to an open beneficiary account with a financial institution where it will be possible for me to instruct further transfer of the fund to a third party account for investment purpose which is the reason i contacted you to receive the fund as my partner for investment in your country.

The amount is valued at Euro 47,745,533.00 with a financial institution waiting my instruction for further transfer to a destination account as soon as I have your information indicating interest to receive and invest the fund, I will compensate you with 30% of the total amount and you will also get benefit from the investment.

If you can handle the fund in a good investment. reply on this email only: r19772744@gmail.com

Regards,
Ms. Reem

Figure L01-10 UAE World Expo Phishing E-Mail

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

How You Should Respond to Phishing E-Mails

The easiest response to suspected phishing e-mails is to delete them. Most larger organizations have automated filters in place to catch phishing attempts. Most companies also offer staff assistance to deal with such e-mail, and offer an account like **abuse@yourcompany.com** where you can send suspicious messages. Many organizations have a web resource that explains examples of current phishing messages that are making the rounds; this resource helps users stay abreast of emerging threats in social engineering. At Kennesaw State University in Georgia, the resource is called the phishmarket. You can see it at **https://uits.kennesaw.edu/ocs/phish-market/index.php**.

When dealing with suspicious e-mail, the best advice is to be skeptical. Phishers are good at what they do. Many malicious e-mails include convincing brand logos, persuasive language, and a seemingly valid e-mail address. However, if an e-mail message looks even remotely suspicious, do not open it. If the message seems too important to ignore and you cannot easily toss it away, try to follow up using resources you can find that are NOT in the e-mail. Go to the sender's web site or call the colleague who allegedly sent you the attachment or urgent request. If the original message was valid and urgent, the sender will appreciate your follow-up.

You should report fraudulent e-mail and other types of social engineering attacks. If you work for a company, contact the help desk or the information security team. For suspicious e-mails sent to your personal account, your e-mail provider or ISP may be able to help you. After evaluation, the company's technical support team should follow up to ensure that the e-mail was deleted, and no losses occurred. If you fall victim to a phishing attack, get help as soon as possible because lost time can factor into the ability to recover losses. If the attack involved a bank or a credit card company, or if you have an identity protection service (like LifeLock), get them involved as soon as you can.

When dealing with phishing attacks, it does not matter if your organization has the most secure security system in the world. It takes only one untrained employee to be fooled and give away data your organization has worked hard to protect. Make sure that you and your co-workers understand the examples illustrated in this lab so you can detect the telltale signs of a phishing attempt.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Test Your Knowledge

Now let's test your knowledge. Imagine that you are a help-desk analyst reading your organization's abuse e-mail account as co-workers send in suspicious messages. Look at each of the following messages and then determine whether you think they are legitimate or suspicious. Print out the answer page at the end of the lab for recording your answers.

For each suspicious message, explain why you think it fails the "smell test."

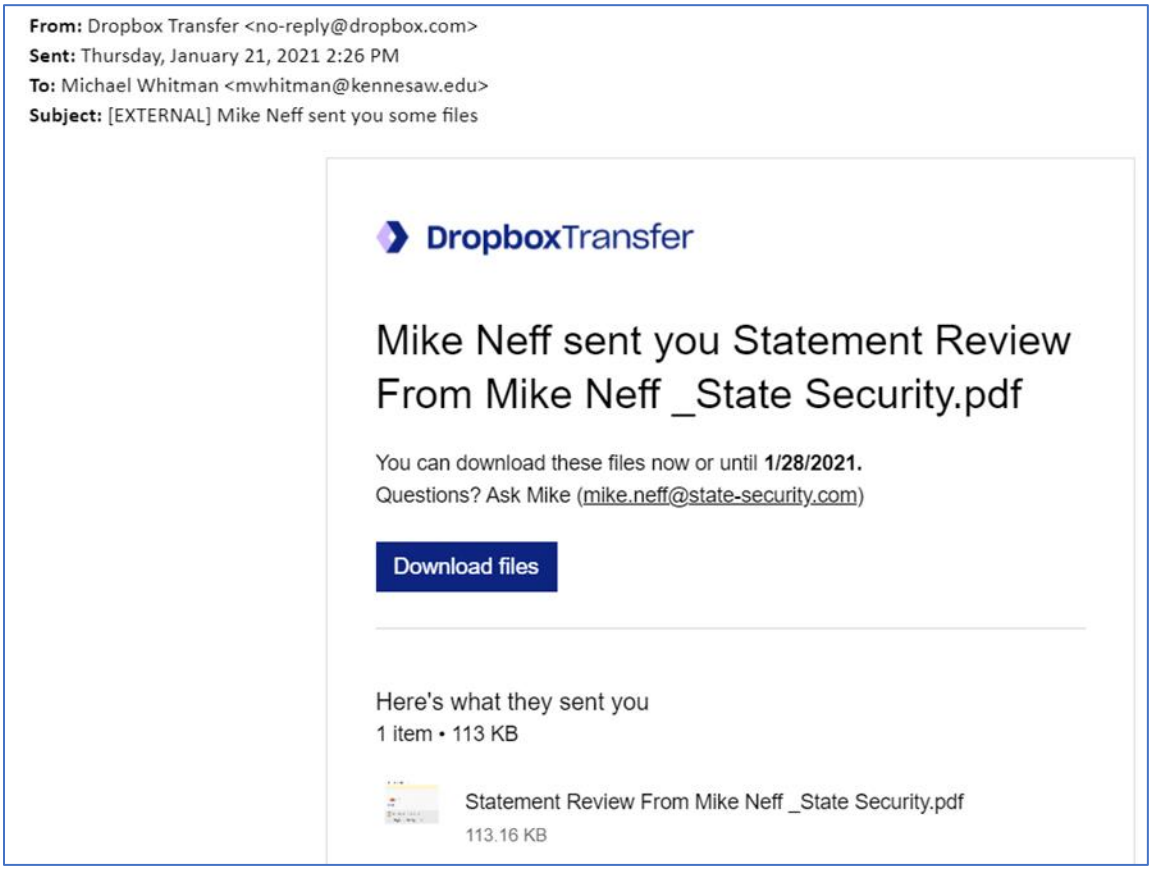
Here is a handy list you can use when evaluating each of the following example e-mails:

- The message asks for sensitive information.
- The message does not contain your correct name; other details are incorrect as well.
- The address does not look authentic.
- There are misspelled words and improper grammar.
- The message forces you to a web page.
- The message has an attachment that is not expected.
- Links in the message seem suspicious.
- The message requests that you send money.

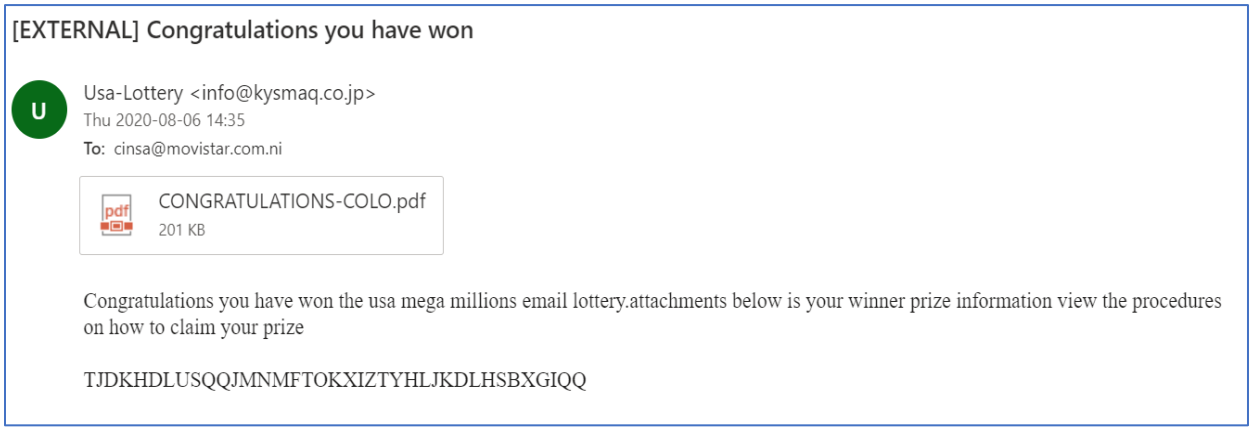
© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Example 1



Example 2



© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Example 3

Bears Moving Co Booking Confirmation 1-29-21 Herbert Mattord 6 pm Inbox ×

Qualin Ransom <qualinransom@gmail.com> Jan 18, 2021, 6:00 PM (3 days ago) Reply

to me

The scheduled Move agreement is as follows. For $225 we will provide 2-hours of service. We will provide 2-men, all moving equipment (i.e., hand-trucks, pads, dollies, etc). There are no hidden fees (I.e., fuel charges). If the job exceeds the allotted time frame, service charges are as following: $100 per hour beyond the 2-hour minimum. Thanks for booking with us, we look forward to servicing you! Please give us a call for any changes or updates.

***Methods of payment: Cash, Check, Cash App, Venmo (no processing fees).

Credit/Debit (3% processing fee).

Please allow a 1-hour window for arrival.

Example 4

Vincenz Cruz <lhtcletisjx@outlook.com>
Sun 2018-09-30 12:18
To: [redacted]

drawde is one of your password:) I am Vincenz. I recorded your webcam which shows your immoral sexual actions & video you played on the porno video because that website was infected with my virus. You happen to be appearing eye-catching in the video footage.

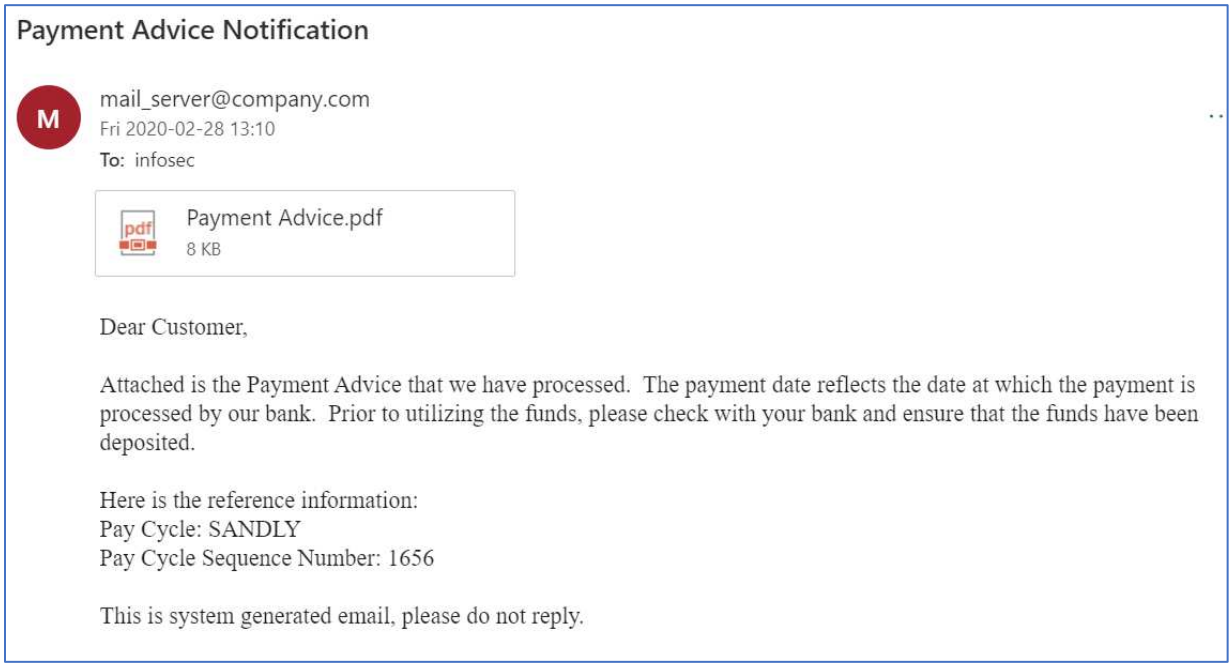
The malware then sent all of your email and FB contacts to me.

I'll email your recording to your friends unless you send me 3000 USD via B I T C O I N S in the next 24 hours to the below address:
B I T C O I N Address: 1Fvfp3183h9YgHD6YaoA1nFUCBUgkjGP3w
Make sure to Copy-Paste address because it is CasE SenSiTiVe.

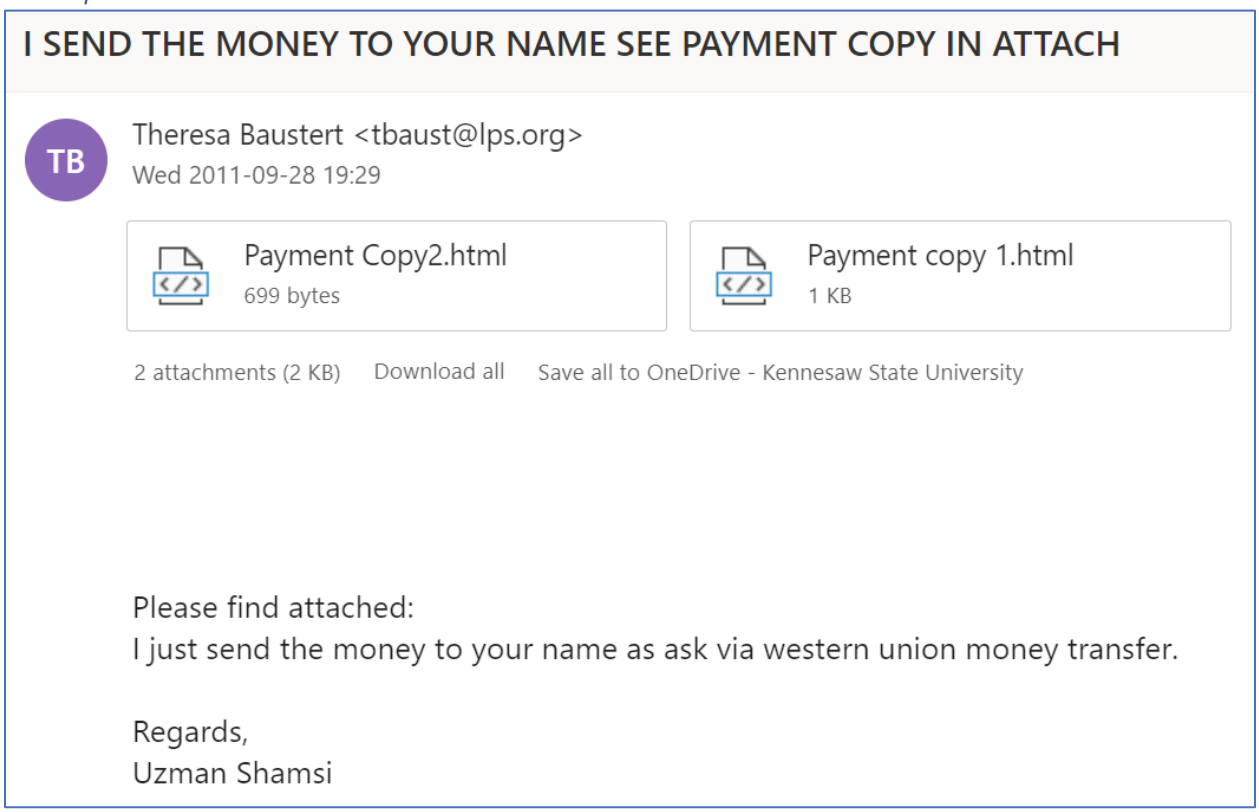
Once money is received by me, I will delete your video and every bit of information I have about you.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Example 5



Example 6



© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Example 7

Please I Need Ur Help!!

VH

Vogelaar, Heleen <Heleen.Vogelaar@uwv.nl>
Sat 2009-06-27 10:16

Dear Friend,
With a very desperate need for assistance.I am Capt. James Micheal. presently in Iraq with the United States Marine Corps;I found your contact particulars in an Address journal.I am seeking your assistance to evacuate the sum of $500,000.00 to you,as far as I can be assured that it
will be safe in your care until I complete my service here.
SOURCE OF MONEY:
some money in various currencies was discovered concealed in barrels with piles of weapons and ammunitions at a location near one of Saddam's old palaces
during a rescue operation,and it was agreed by all party present that the money will be shared amongst us.
The above figure was given to me as my share, There is a secured way of getting the package out to a safer country for you to pick up,and i will discuss this with you when I am sure that you are willing to
assist me, because I do not know for how long we will remain here.
Please you can reach me on my personal e-mail address below for more
information.
Email: capt.james001@sify.com
Thanks
Capt. James Micheal.

Example 8

AP

ACH Payment <Opal@boomansion.net>
Wed 2011-09-21 02:38
To: hmitcheld@kennesaw.edu

FDIC

Your Corporate and Business banking accounts
Federal Deposit
Insurance Corporation
Security Updates for ACN and Wire transfers

Dear client,

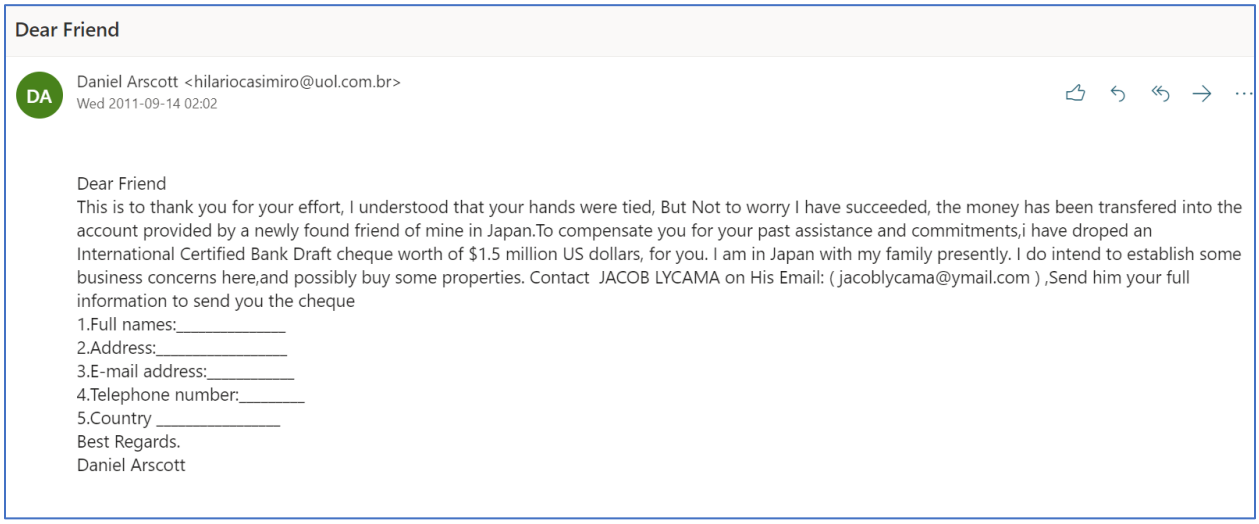
Your account **ACH and Wire transactions** have been **temporarily suspended** for your Security,
due to the expiration of your security version.
To download and **install the newest Updates**, follow this link security http://www.update.fdic.gov

As soon as it is set up, your transaction abilities will be fully restored.
Best regards, *Online security department*, Federal Deposit Insurance Corporation.

FDIC Public Information Center
3501 North Fairfax Drive, Room E-1002.Section 515. Arlington, VA 22226
Fax Number: (703) 562-2296 Email Address: publicinfo@fdic.gov

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Example 9



Dear Friend

DA

Daniel Arscott <hilariocasimiro@uol.com.br>
Wed 2011-09-14 02:02

Dear Friend
This is to thank you for your effort, I understood that your hands were tied, But Not to worry I have succeeded, the money has been transfered into the account provided by a newly found friend of mine in Japan.To compensate you for your past assistance and commitments,i have droped an International Certified Bank Draft cheque worth of $1.5 million US dollars, for you. I am in Japan with my family presently. I do intend to establish some business concerns here,and possibly buy some properties. Contact JACOB LYCAMA on His Email: (jacoblycama@ymail.com) ,Send him your full information to send you the cheque
1.Full names:_____
2.Address:_____
3.E-mail address:_____
4.Telephone number:_____
5.Country _____
Best Regards.
Daniel Arscott

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Example 10

-------- Forwarded Message --------
Subject:AUTO RENEWING EMAIL
Date: Thu, 21 Jan 2021 23:23:27 +0530
From: Norton Official <nortonofficial20@gmail.com>
To:alisaqlain989@gmail.com



AUTO RENEWAL EMAIL

MODE OF PAYMENT : CREDIT CARD
ORDER NUMBER : 85692563
CHARGE : $480.87
HELPLINE NUMBER : +1 (570) 260-6102.

Dear Sir/Madam,

Thank You for renewing your Norton Life Lock security for the upcoming one year.

Norton informs you that the contract electronically signed by you with our company for the maintenance of your computer services has expired, and it is auto renewed today for the upcoming year. The transaction of $399.99 would appear within the next 48 working hours on your account.

We would like to inform you that this month we have served over 1 million customers and you are one of them . We hope you will enjoy the services . Due to COVID-19 we are unable to notify each customer through a confirmation call .

If you have any questions or wish to cancel the subscription and get back your refund,

Please contact us on +1 (570) 260-6102.

Thank You,

Team Norton.

(Finance Team)

NOTE: THIS IS AN AUTO GENERATED EMAIL PLEASE DON'T REPLY TO THIS EMAIL.

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual

Phishing Email Responses

Email	Trustworthy (T) or Suspicious (S)	Reason
Example 1		
Example 2		
Example 3		
Example 4		
Example 5		
Example 6		
Example 7		
Example 8		
Example 9		
Example 10		

Instructor's Response:

© 2022 Cengage. All Rights Reserved. May not be scanned, copied or duplicated, or posted to a publicly accessible Web site, in whole or in part.

Principles of Information Security 7th edition Whitman Solutions Manual