**CST-407 Activity 1 Guide**

Contents

[Activity 1: Introduction to Security 2](#_Toc58829166)

[Part 1: Can you Catch a Phish? 2](#_Toc58829167)

[Part 2: Defining Cybersecurity Terms 2](#_Toc58829168)

[Part 3: Cyber Attack Methods 3](#_Toc58829169)

[Part 4: Google Hacking 5](#_Toc58829170)

# Activity 1: Introduction to Security

This activity has multiple parts/assignments. All assignments must be completed prior to documentation submission.

## Part 1: Can you Catch a Phish?

**Overview**

Phishing is the practice of sending a fraudulent email in hopes of stealing data or money. The email is the “bait.” You are the fish. Don’t take the bait. In this activity, students will examine several examples of suspicious looking emails and distinguish the frauds from the legitimate, yet questionable-looking emails.

**Execution**

Execute this activity according to the following guidelines:

1. Locate three examples of faked emails in online forums or blogs.
2. Provide a screenshot of each and paste them into a Microsoft Word document.
3. For each of the examples, indicate what features of the message should give the recipient a “red flag” or indication that the message is a fake.
4. Make sure to properly reference and cite all examples and supporting evidence.
5. Make sure to utilize appropriate industry terminology.

**Documentation**

All documentation will be submitted at the end of the activity to the digital classroom. Ensure documentation of the following:

1. A Word document containing an analysis of each example.

## Part 2: Defining Cybersecurity Terms

**Overview**

In this activity, students will examine terminology used in cybersecurity issues and distinguish the differences between these terms.

**Execution**

Execute this activity according to the following guidelines:

1. Review the associated resources located within the Topic Resources, paying close attention for the terminology mentioned in Table 1 below.
2. Research the terms “Information Security" and "What are Threats vs Vulnerabilities and Attacks?”
3. In a Word document complete, Table 1. For each word in column 1, write a definition and provide a specific example of what it is or does.
4. Make sure to properly reference and cite all examples and supporting evidence.

**Table 1. Key Terms in Cyber Security**

|  |  |
| --- | --- |
| **Terms** | **Definition and Example** |
| **Three Types of Security Threats**  Vulnerability  Threat  Attack |  |
| **Four Types of Attacks**  I  I  M  F |  |
| **Three Pillars of Security**  C  I  A |  |
| **Six Types of Countermeasures**  1.  2.  3.  4.  5.  6. |  |
| **Three Aspects of Hacker Success**  M  O  M |  |

**Documentation**

All documentation will be submitted at the end of the activity to the digital classroom. Ensure documentation of the following:

1. A Word document containing a completed Table 1.

## Part 3: Cyber Attack Methods

**Overview**

In this activity, students will examine hacking techniques and general categories of hacks, as well as case studies related to some of the largest data breaches in history.

**Execution**

Execute this activity according to the following guidelines:

1. Review the associated resources located within the Topic Resources.
2. In a Word document, write a complete answer to the following questions. A complete answer is a fully developed paragraph, including a topic sentence, supporting examples or details, and a conclusion.
3. Make sure to properly reference and cite all examples and supporting evidence.
4. Make sure to utilize appropriate industry terminology.

**Ransomware**

1. What types of software does the person in "Anatomy of Attack: Cybersecurity Update" use to perform their attack? Research the names and techniques shown and explain what they are.
2. What is the primary vulnerability in the company that the hacker relies on to succeed? Give an example of a real-world company that experienced this type of attack.
3. What extent of damage was done to the victim? Give an example of a real-world company that experienced similar damages due to this type of attack.
4. What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would they employ?

**SQL Injection**

1. What types of application programs are vulnerable to a SQL injection attack?
2. What type of damage could be done to the victim with this attack? Give an example of a real-world company that experienced this type of attack.
3. What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would they employ?

**Credit Card Skimmers**

1. What types of systems are vulnerable to this attack?
2. What type of damage could be done to the victim with this attack? Give an example of a real-world company that experienced this type of attack.
3. What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would they employ?

**Man in the Middle**

1. What types of systems are vulnerable to a MITM attack?
2. What type of damage could be done to the victim with this attack? Give an example of a real-world company that experienced this type of attack.
3. What type of cybersecurity expert would likely be properly trained to prevent this type of attack, and what type of interventions would they employ?

**Ethical Dilemmas**

1. In addition, write a 250-word description on what keeps white hat hackers on the right side. A white hat hacker is one who uses computer security skills in service of "good." From a Christian worldview, discuss how people should apply their skills for the common good. Also provide examples by researching the ethical dilemmas behind creating and using white hat hackers. Provide support for your answers by including actual cybersecurity events that have taken place in which white-hat hackers were used to mitigate the criminal attempts of cyber criminals who may have been trying to steal, manipulate, or destroy pertinent information.

**Documentation**

All documentation will be submitted at the end of the activity to the digital classroom. Ensure documentation of the following:

1. Word document containing an analysis of the proposed topics.

## Part 4: Google Hacking

**Overview**

Google Hacking, also called Dorking, is the process of finding sensitive data online with the help of Google’s advanced options in their search engine. Surprisingly, one can find free software, credit card numbers, social security numbers, passwords, and database backups with the help of the most powerful hacking tool online—Google Search.

In this activity, students will examine the extent to which Google indexes sensitive data and recommendations for removal of this data.

**Execution**

Execute this assignment according to the following guidelines:

1. Review the associated resources located in the Topic Resources.
2. Research the phrase “Google Dorking or Hacking” to familiarize yourself with techniques that allow Google to be used as a hacking tool.
3. Research the phrase “Go to Jail for Google Hacking” to see what consequences may or may not be related to utilizing a Google Dork result.
4. Capture a screenshot example of a directory listing of MP3, MP4 or PDF files that were likely hosted unintentionally on a webserver. In the photo caption, explain why you believe this directory probably was not intended to be shared.
5. Capture a screenshot example of a SQL backup file from a site. In the caption, highlight the most vulnerable data contained in the backup file.
6. Explain the process that Google provides users to remove pages from the search results.
7. What advice does Google provide for permanent removal of search results?
8. The **Computer Fraud and Abuse Act (CFAA)** is a U.S. Law that directly addresses the issue of unauthorized access to a computer system. How does the CFAA relate to information obtained by a Google Dork search?
9. Make sure to properly reference and cite all examples and supporting evidence.
10. Make sure to utilize appropriate industry terminology.

**Submission**

Submit the following to the digital classroom:

**Part 1**

1. A Word document containing an analysis of each example.

**Part 2**

1. A Word document containing a completed Table 1.

**Part 3**

1. A Word document containing an analysis of the proposed topics.

**Part 4**

1. A Word document containing an analysis of the proposed topics.