

Name: _____

2) 23100-1 CYBER SECURITY**2-1 Social Engineering Worksheet - Cyber Security****Page 1****Question 12 - True/False****Points: 1**

Social engineering relies on manipulating human behavior instead of hacking technology directly.

A) True

B) False

Question 11 - Multiple Choice**Points: 1**

Which security practice helps protect accounts even if a password is stolen?

A) Using short passwords

B) Multi-factor authentication (MFA)

C) Saving passwords in a notes app

D) Reusing the same password everywhere

Question 13 - True/False**Points: 1**

Social engineering messages often create urgency or pressure to make someone act quickly.

A) True

B) False

Question 6 - Multiple Choice**Points: 1**

Following an employee into a locked area without permission is best described as:

A) Shoulder surfing

B) Piggybacking/Tailgating

C) Scareware

D) Info written down

Question 5 - Multiple Choice**Points: 1**

Searching through the trash for confidential documents is called:

A) Dumpster diving

B) Pretexting

C) Tailgating

D) Baiting

Question 15 - True/False

Points: 1

Piggybacking is when someone slips into a secure area behind you without permission.

A) True

B) False

Question 10 - Multiple Choice

Points: 1

What is the BEST first step if you receive a suspicious message asking for a password?

A) Pause and verify using a trusted method

B) Forward it to friends to warn them

C) Click the link to confirm your identity

D) Reply quickly so your account doesn't get locked

Question 9 - Multiple Choice

Points: 1

Malware that encrypts files and demands payment is called:

A) Scareware

B) Ransomware

C) Baiting

D) Pretexting

Question 14 - True/False

Points: 1

It is safe to share verification codes if the person claims to be from IT.

A) True

B) False

Question 7 - Multiple Choice

Points: 1

An attacker pretends to be the school IT technician and asks for your login code. This is:

A) Baiting

B) Pretexting

C) Dumpster diving

D) Ransomware

Question 17 - True/False

Points: 1

Unexpected attachments can be a warning sign of a social engineering attempt.

A) True

B) False

Question 3 - Multiple Choice

Points: 1

Offering a free gift card link to get someone to click is an example of:

- A) Shoulder surfing
- B) Dumpster diving
- C) Baiting
- D) Ransomware

Question 2 - Multiple Choice

Points: 1

Which of the following is a common red flag of social engineering messages?

- A) Clear sender address and correct spelling
- B) A message that includes your full legal name and employee ID
- C) A message demanding action "immediately"
- D) A message that encourages you to ask IT for help

Question 1 - Multiple Choice

Points: 1

What is social engineering?

- A) Physically stealing a computer from a building
- B) Hacking into a server by breaking encryption
- C) Writing malware code to infect a device
- D) Manipulating people into giving up information or access

Question 16 - True/False

Points: 1

Ransomware is a tool used to speed up your computer by deleting old files.

- A) True
- B) False

Question 8 - Multiple Choice

Points: 1

A pop-up claims your device is infected and tells you to call a number right away. This is:

- A) Scareware
- B) Dumpster diving
- C) Shoulder surfing
- D) Piggybacking

Question 4 - Multiple Choice

Points: 1

Someone watches you type your password at a computer lab. This is:

- A) Shoulder surfing
- B) Piggybacking
- C) Pretexting
- D) Scareware

Name: _____

2) 23100-1 CYBER SECURITY

2-2 Malicious Code Worksheet

Page 1

Question 5 - Multiple Choice

Points: 1

Spyware may collect:

- A) Software updates
- B) Passwords, PINs, and credit card numbers
- C) Weather information
- D) Printer settings

Question 4 - Multiple Choice

Points: 1

Which of the following is an example of spyware?

- A) Browser
- B) Firewall
- C) Keylogger
- D) Antivirus

Question 17 - True/False

Points: 1

Spam email is always illegal.

- A) True
- B) False

Question 1 - Multiple Choice

Points: 1

What is ransomware?

- A) A web browser extension
- B) A program that blocks access to files or devices until a ransom is paid
- C) A type of antivirus software
- D) A program that improves computer speed

Question 20 - True/False

Points: 1

Opening programs from unknown sources is a safe practice.

A) True

B) False

Question 10 - Multiple Choice

Points: 1

Which topic is often found in spam emails?

A) Get-rich-quick schemes

B) School schedules

C) Weather forecasts

D) Science experiments

Question 14 - True/False

Points: 1

Spyware spreads to other computers like a worm.

A) True

B) False

Question 19 - True/False

Points: 1

Malware may cause a computer to freeze or crash.

A) True

B) False

Question 12 - Multiple Choice

Points: 1

Malware may cause a user to:

A) Improve browser performance

B) Increase internet speed

C) Lose access to the Internet or their computer

D) Gain free software

Question 18 - True/False

Points: 1

Malware can degrade computer performance.

A) True

B) False

Question 13 - Multiple Choice

Points: 1

Why should system files be updated regularly?

A) To increase spam emails

B) To remove documents

C) To change the computer's color scheme

D) To install security patches

Question 11 - Multiple Choice

Points: 1

Malware may damage files by:

A) Deleting or corrupting important data

B) Organizing folders

C) Compressing files

D) Backing up documents

Question 8 - Multiple Choice

Points: 1

What does PUP stand for?

A) Program Update Patch

B) Potentially Unwanted Program

C) Protected User Program

D) Private Utility Package

Question 7 - Multiple Choice

Points: 1

Adware is commonly installed with:

- A) Shareware or freeware applications
- B) Computer hardware
- C) Printers
- D) Antivirus software

Question 6 - Multiple Choice

Points: 1

What is adware?

- A) A file-sharing program
- B) A type of operating system
- C) Software that removes ads
- D) Software that displays advertisements through toolbars, pop-ups, or banners

Question 15 - True/False

Points: 1

Adware is only found on paid software applications.

- A) True
- B) False

Question 2 - Multiple Choice

Points: 1

Which is a method used by ransomware?

- A) Removing advertisements
- B) Updating software
- C) Backing up files
- D) Encrypting files

Question 3 - Multiple Choice

Points: 1

What is spyware?

- A) Software that creates backups
- B) Software that protects personal information
- C) Software that blocks spam emails
- D) Software that gathers data and sends it to a third party without the user's knowledge

Question 16 - True/False

Points: 1

Potentially Unwanted Programs (PUPs) are always malicious.

- A) True
- B) False

Question 9 - Multiple Choice

Points: 1

What is spam?

- A) A type of virus
- B) Unsolicited commercial email
- C) A computer operating system
- D) Antivirus software

Name: _____

2) 23100-1 CYBER SECURITY

2-3 Phishing Worksheet

Page 1

Question 4 - Multiple Choice

Points: 1

What can happen if you enter information on a phishing website?

- A) Your computer automatically updates
- B) Your internet speed increases
- C) Nothing happens
- D) Your information can be stolen

Question 15 - True/False

Points: 1

The sender's email address should match who they claim to be.

- A) True
- B) False

Question 11 - True/False

Points: 1

Phishing emails often create a sense of urgency.

- A) True
- B) False

Question 12 - True/False

Points: 1

Spam emails are usually sent to many recipients at once.

- A) True
- B) False

Question 6 - Multiple Choice

Points: 1

What should you do with a suspicious phishing email?

- A) Reply with your personal information
- B) Forward it to friends
- C) Click all links to investigate
- D) Remove it and report it

Question 7 - Multiple Choice

Points: 1

What is spear-phishing?

- A) A phishing attack from a video game
- B) A phishing attack targeted at a specific person or organization
- C) A phishing attack sent to everyone
- D) A phishing attack sent through television

Question 9 - Multiple Choice

Points: 1

What is smishing?

- A) Phishing through email only
- B) Phishing through websites only
- C) Phishing through text messages
- D) Phishing through advertisements

Question 8 - Multiple Choice

Points: 1

What is whaling?

- A) Targeting high-value individuals with phishing attacks
- B) Sending phishing texts
- C) Collecting large amounts of spam
- D) Sending phishing phone calls

Question 3 - Multiple Choice

Points: 1

Which of the following is NOT typically part of a phishing attack?

- A) Entering personal information on a bogus site
- B) Installing a legitimate software update
- C) A fake email from a trusted organization
- D) A link to a fake website

Question 14 - True/False

Points: 1

Spam emails always contain a sense of urgency.

- A) True
- B) False

Question 10 - Multiple Choice

Points: 1

What is vishing?

- A) Phishing through voice messages or phone calls
- B) Phishing through social media posts
- C) Phishing through video advertisements
- D) Phishing through gaming apps

Question 5 - Multiple Choice

Points: 1

Which clue may indicate a phishing email?

- A) An expected email from a teacher
- B) Matching sender name and email address
- C) Misspellings and incorrect grammar
- D) Correct grammar and spelling

Question 2 - Multiple Choice

Points: 1

Phishing is considered:

- A) A type of antivirus software
- B) A gaming technique
- C) A harmless prank
- D) One of the top four biggest threats in the digital world

Question 13 - True/False

Points: 1

It is safe to provide passwords to a website that looks identical to a real site.

- A) True
- B) False

Question 1 - Multiple Choice

Points: 1

What is phishing?

- A) A type of computer hardware
- B) The use of bogus emails and websites to trick people into providing personal information
- C) A secure way to send information
- D) A firewall program

Name: _____

2) 23100-1 CYBER SECURITY

2-4 OSINT Worksheet

Page 1

Question 4 - Multiple Choice

Points: 1

Which of the following is an example of OSINT?

- A) Reading a public social media post
- B) Installing malware
- C) Stealing a password
- D) Breaking into a computer system

Question 1 - Multiple Choice

Points: 1

What does OSINT stand for?

- A) Open Systems Internet Technology
- B) Organizational Security Information Tracking
- C) Open-Source Intelligence Tools
- D) Online Security Internet Tracking

Question 10 - True/False

Points: 1

Social media profiles may contain useful information for OSINT.

- A) True
- B) False

Question 5 - Multiple Choice

Points: 1

What can Google Reverse Image Search help you do?

- A) Find information using a photo
- B) Create new images
- C) Delete photos online
- D) Edit photographs

Question 8 - True/False

Points: 1

LinkedIn can provide information about homes, including descriptions and pictures.

A) True

B) False

Question 3 - Multiple Choice

Points: 1

OSINT information must be:

A) Private

B) Legally accessible to the public

C) Hidden from search engines

D) Stolen directly from a company

Question 2 - Multiple Choice

Points: 1

Why might a cybercriminal use OSINT?

A) To install software updates

B) To gather information about a target

C) To repair computers

D) To create video games

Question 7 - True/False

Points: 1

Google Maps Street View can be used as an OSINT tool.

A) True

B) False

Question 6 - True/False

Points: 1

Reconnaissance means gathering information about a target before an attack.

A) True

B) False

Question 9 - True/False

Points: 1

Amazon wish lists and gift registries can be sources of OSINT information.

A) True

B) False

Name: _____

2) 23100-1 CYBER SECURITY

2-5 Mitigating the Human Risk Worksheet

Page 1

Question 10 - True/False

Points: 1

Hoaxes are intended to educate users about cybersecurity.

A) True

B) False

Question 5 - Multiple Choice

Points: 1

What does "mitigate" mean?

A) Ignore a problem

B) Make less severe or reduce adverse effects

C) Increase risk

D) Create a threat

Question 9 - True/False

Points: 1

User training is part of the mitigation process.

A) True

B) False

Question 2 - Multiple Choice

Points: 1

Installing unauthorized software may result in a:

A) Backup

B) Update

C) Backdoor

D) Firewall

Question 8 - True/False

Points: 1

A policy is a series of steps used to implement a procedure.

A) True

B) False

Question 3 - Multiple Choice

Points: 1

What is Reverse Social Engineering?

A) The user reports suspicious activity to their IT department

B) The attacker creates a situation so the victim makes the initial contact

C) The attacker repairs a problem

D) The victim creates an attack

Question 7 - True/False

Points: 1

A procedure helps implement a policy.

A) True

B) False

Question 6 - Multiple Choice

Points: 1

Human risk can be mitigated by:

A) Removing all software

B) Setting clear expectations for users

C) Ignoring policies for other departments within the company

D) Limiting internet access for everyone

Question 1 - Multiple Choice

Points: 1

Which of the following is an example of not following organizational rules?

- A) Installing unauthorized hardware
- B) Following procedures
- C) Attending security training
- D) Creating strong passwords

Question 4 - Multiple Choice

Points: 1

The purpose of many hoaxes is to:

- A) Educate users on cyber security policies
- B) Improve security
- C) Frighten and mislead recipients into forwarding messages
- D) Fix computer problems