**Pre Survey Questions**

1. **Please indicate your gender:**

* Male
* Female
* Other
* Prefer not to say

1. **What is your age group?**

* Under 18
* 18– 24
* 25 – 29
* 30 – 34
* 35 – 44
* 45+
* Prefer not to say

1. **What is your highest level of education?**

* High School
* Some College, no degree
* Associate degree
* Bachelor’s degree
* Post-graduate degree
* Prefer not to say

1. **Have you completed security training in the past?**

* Yes, I have.
* No, I have not.
* Prefer not to say

1. **If you *have* completed security training previously, where was this training completed?**

* Workplace-related training
* School-related training
* Other
* N/A

**Part 1 Instructions**

You will be presented with a set of hypothetical scenarios. Each scenario should be considered independent from and unrelated to any other scenarios that are presented in this section. Please read through each scenario as if it applies to you. Answer the question for each scenario according to how you would react if you were present in the scenario.

**Part 1 Scenarios**

**Scenario 1**

You are attending a business convention and meet someone who tells you that they work for the same company at one of the branch locations. You spend more time talking with this individual over the course of the convention and you ask if this individual’s branch has upgraded their online system yet. The individual replies that they haven’t yet, but they can’t wait to see the new features. They are curious if it’s much different from the current system. You have your laptop on and open so you offer to show them some of the new features. They get up and stand behind you so that they can see your screen. You open up your company’s system and the login screen appears.

Would you continue to type in your username and password?

Yes

No

**Scenario 2**

You have a movie streaming account and regularly use this service to watch movies and tv shows. You receive an email with the subject line “Update account information” from support@emailer.com. The email states the following:

*Hello valued customer,*

*Your payment method for your account needs to be updated in order to continue using our services. We currently are unable to  authorize your last payment due to an issue with your credit card on file. Please click the link below to verify that your payment information is correct or to update with a new payment method. If you have any questions or concerns please contact customer service.*

You can’t remember what card you used to pay for this streaming service. The email contains the streaming service’s logo and all spelling and grammar is correct.

Would you click on the link to update/verify your payment information?

Yes

No

**Scenario 3**

You work for a company with a large office building where all visitors must sign the visitor log and be escorted by an employee while in the building. All entrances to the building require an employee badge that is also a keycard. You regularly use the employee entrance in the back rather than enter through the front door. One day as you are coming back from lunch you walk toward the employee entrance and scan your badge to get in. As you are opening the door you notice an individual walking up to the door holding several boxes and bags that are from a local office supply store. This individual is struggling with the number of items and is also trying to reach into their pocket to retrieve something.

Would you hold the door open for this individual?

Yes

No

**Scenario 4**

You have been working on your computer for several hours with various applications and web browsers open. As you switch between various windows and applications that you have open a large popup appears on your screen with a smaller popup in front of it. The large popup has the title “WINDOWS VIRUS WARNING!” and underneath a list of alerts that you see contain words like trojan and spyware. It also says that it has detected 23 viruses that pose a threat to your system. The smaller popup on top of this says “Your computer has been locked. Windows has detected a virus attack on your computer. Contact Windows Security Help Line.”The large and small popup both contain a 1-800 number for the help line. You can close out of the smaller popup but you can’t click or interact with anything else on your computer screen.

Would you call the 1-800 number listed?

Yes

No

**Scenario 5**

You are doing research at a local university and one day as you are walking toward the research building you notice a USB drive on the sidewalk outside the building. The USB is the same type that you use in the lab for transferring data. You pick it up and notice a label on it that reads “2018-2021 data results”. There is nothing to indicate the owner of the USB drive. You decide to not leave the USB drive outside so you bring it into the research building with you.

Would you plug this USB drive into a computer to view it’s content?

Yes

No

**Education**

Cybersecurity is a topic that is becoming increasingly common today with the advancement of technology and the prevalent use of smartphones and computers. Cybersecurity deals with the measures and means to protect these devices or systems from attack by those who want to cause damage or gain access to sensitive information.

A cybersecurity attack is not just limited to finding vulnerabilities in a software program or network. Cybersecurity attacks can occur by finding and leveraging vulnerabilities on the human side of security by means of social engineering tactics.

What is social engineering?

Social engineering is a technique used to access information and systems by taking advantage of human weaknesses and behavior. Someone who utilizes social engineering in their attacks relies on knowledge of human behavior in order to access or obtain the information they want. Human vulnerabilities can sometimes be easier to exploit than a vulnerability in your software or network. Anyone can be susceptible to social engineering and should be aware of such techniques.

What are some examples of social engineering and how do you protect yourself against them?

Shoulder Surfing is the act of gaining valuable information such as passwords and login credentials by observing the entering of private information. Often it can be done by simply looking over someone’s shoulder at their computer screen or keyboard to see information that is being entered. Shoulder surfing may be more common in crowded areas where the observer is not as noticeable. The individual shoulder surfing doesn’t need to be directly behind your shoulder, but may observe from a distance or utilize binoculars.

Here are some things to keep in mind to protect yourself against shoulder surfing.

* Don’t type, write, or say out loud your personal information or login credentials when other people are able to see or hear this information.
* When you need to enter confidential information with others around try to place your back to a wall so no one can observe over your shoulder.
* Use a privacy screen on your devices to reduce visibility of your screen to others.

Phishing is the sending of digital communications that appear to be from a valid and trustworthy source to entice individuals to reveal personal information. Many phishing attempts occur by way of email and can appear to truly be from a trusted organization. The goal of the phishing attempt is to get the receiver to trust the message and then act accordingly by giving their information such as passwords or credit card numbers. Many times the recipient is compelled to click on links or attachments by the message creating a sense of urgency, fear, or curiosity.

Here are some things to keep in mind to protect yourself against phishing.

* Don’t click on links asking you to verify, enter, or update your information.
* If you need to update or verify your information log in to the application or site directly rather than clicking on a link.
* Don’t open messages or attachments that look suspicious or are unexpected.
* Look for grammar and spelling mistakes in messages as this usually indicates that it’s not a valid message..

Piggybacking or tailgating is when someone gains access to a secure location by means of following or being allowed in by an authorized person. These individuals may try to act like an employee, delivery person, or maintenance person to gain trust to enter without needing the correct credentials. Sometimes they observe how others access the building or even the times that they do so they can mimic the actions of others.

Here are some things to keep in mind to protect yourself against piggybacking/tailgating.

* Don’t let others enter secure locations with you even if they appear or act as if they are allowed to.
* If you see someone that you aren’t familiar with walking around in a secure location don’t assume that they are allowed to be there.
* Don’t hold doors open for others when the door requires a type of key or passcode to enter.
* Be aware of people trying to enter a secure area immediately after you especially if the door wasn’t closed fully behind you.

Scareware is a computer program meant to deceive someone into downloading or buying software that is potentially dangerous. Usually there is a factor of fear involved to urge the user to fall for the scareware. Scareware may come in the form of a warning about your computer or device that needs to be taken care of and presents an antivirus tool or program promising to take care of the issue when it will actually create an issue.

Here are some things to keep in mind to protect yourself against scareware.

* Don’t purchase or click on tools that appear after receiving a warning message on your computer.
* Don’t click on links or call numbers presented in a pop-up message. Contact the company directly if there is an issue with your device.
* Use only trusted antivirus and malware software products.

Baiting occurs by luring someone with an enticing online or physical item that is potentially dangerous. This technique relies on the greed and curiosity of people. Many times an item or promise of a program or tool appears to have a reward that can’t be passed up. A physical computer item may be passed out or left in a conspicuous place for you to take and plug into your device that contains a harmful program.

Here are some things to keep in mind to protect yourself against baiting.

* If something appears too good to be true it probably is so don’t trust it.
* Don’t plug items into your devices that you find or receive from unknown sources.
* Don’t download or click on links that promise an amazing or once in a lifetime offer.

**Part 2 Instructions**

Having read about social engineering you will now be presented with a new set of hypothetical scenarios. Each scenario should be considered independent from and unrelated to any other scenarios that were presented in the first section or that will be presented in this section. Please read through each scenario as if it applies to you. Answer the question for each scenario according to how you would react if you were present in the scenario.

**Part 2 Scenarios**

**Scenario 1**

You work remotely for a company and are responsible for managing the companies financial transactions. You work mainly from home, but you find it easier to get more work done by going elsewhere. You usually go to a nearby coffee shop with your laptop and sit in the booth in the back corner. Today the shop is busier than usual with almost every table full so you find a seat at a table in the center of the shop. You have some transactions that you need to review by the end of the business day. You will need to access the company’s bank statements online through the bank’s website where your company has the account to verify if the transactions are valid. You navigate to the bank’s website and the login screen appears requesting your username and password.

Would you continue with entering your username and password to login?

Yes

No

**Scenario 2**

You don’t have a laptop or desktop computer so you access websites and applications on your cell phone. You have a social media account that you access frequently. One day you receive an email with the following message regarding your social media account:

*Hello,*

*A new device has been used to access your account at 1:13pm today.*

*Operating System: Mac OS X 10.5*

*Browser: Safari*

*Location: Amsterdam, NH, NL*

*If you did this, you may ignore this message.*

*If you did not access your account with this device please secure your account by following the link listed below.*

*Sincerely,*

*Customer Security Team*

You have only used your phone to access your account and you don’t have a Mac OS device nor have you been in the location listed.

Would you click on the link to access your account in order to secure it?

Yes

No

**Scenario 3**

There are many employees at your office and you only know a handful of them by name. You see many in passing and could identify them but not their name or which department they work in. You always use the employee entrance that requires a keycard to get in as it’s more efficient than checking in with the receptionist. One day while walking to the door an individual rushes up behind you as you scan your keycard. You recognize their face as you have seen them sitting outside at the employee picnic table on several occasions eating lunch. You have never spoken to this individual but only observed them in passing. They look stressed and in a hurry. They say “Hey, can you please hold the door? My kid had an accident this morning and it put me out of sorts and I forgot my keycard. I’m late for a meeting that I can’t miss.”

Would you let this individual enter the building with you?

Yes

No

**Scenario 4**

You have an issue with your printer and are searching the internet on your laptop for a solution to get it working. You really need to print off some documents so you have been clicking on any site that may give you a solution. You find a promising yet unfamiliar site and you click on the link. Once you click on the link and get redirected to the site a pop up banner appears at the top of your browser with the following message: “A harmful spyware program has been detected on your computer. Click here to remove harmful programs using the free trial of CleanSpyware removal tool.” Currently your computer doesn’t have any antivirus or security software installed to take care of risks.

Would you click to remove the detected spyware using the CleanSpyware removal tool offered?

Yes

No

**Scenario 5**

You are a huge fan of a popular tv series that you were able to view on a streaming service. Unfortunately the series was removed from the streaming service before you could finish the last few episodes. The last episode that you were able to watch left off on a huge cliffhanger and you desperately want to find out what happens next. There currently isn’t any streaming service that you know of that has this series available. You have been browsing the internet on your cell phone to find where you can watch the last few remaining episodes. You find a site that says that you can watch all full episodes of the series that you were looking for. It has a download link for each of the seasons. You see that it has a link for the last season that you want to watch.

Would you click on the link to watch the episodes that you missed?

Yes

No