**Please rate how familiar you are with the following websites (1=Not at All Familiar, 5=Very Familiar)?**

|  |  |  |  |
| --- | --- | --- | --- |
| adcash.com | 1 |  | 5 |
| 3.0 | | | |
| adf.ly | 1 |  | 5 |
| 3.0 | | | |
| adobe.com | 1 |  | 5 |
| 3.0 | | | |
| airbnb.com | 1 |  | 5 |
| 3.0 | | | |
| aliexpress.com | 1 |  | 5 |
| 3.0 | | | |
| amazon.com | 1 |  | 5 |
| 3.0 | | | |
| battle.net | 1 |  | 5 |
| 3.0 | | | |
| dropbox.com | 1 |  | 5 |
| 3.0 | | | |
| ebay.com | 1 |  | 5 |
| 3.0 | | | |
| expedia.com | 1 |  | 5 |
| 3.0 | | | |
| flipkart.com | 1 |  | 5 |
| 3.0 | | | |
| giphy.com | 1 |  | 5 |
| 3.0 | | | |
| github.com | 1 |  | 5 |
| 3.0 | | | |
| godaddy.com | 1 |  | 5 |
| 3.0 | | | |
| netflix.com | 1 |  | 5 |
| 3.0 | | | |
| paypal.com | 1 |  | 5 |
| 3.0 | | | |
| salesforce.com | 1 |  | 5 |
| 3.0 | | | |
| stackoverflow.com | 1 |  | 5 |
| 3.0 | | | |
| steampowered.com | 1 |  | 5 |
| 3.0 | | | |
| tripadvisor.com | 1 |  | 5 |
| 3.0 | | | |
| twitch.tv | 1 |  | 5 |
| 3.0 | | | |
| twitter.com | 1 |  | 5 |
| 3.0 | | | |
| ups.com | 1 |  | 5 |
| 3.0 | | | |
| wordpress.com | 1 |  | 5 |
| 3.0 | | | |
| yahoo.com | 1 |  | 5 |
| 3.0 | | | |
| yelp.com | 1 |  | 5 |
| 3.0 | | | |

**What is your gender?**

Male  
Female  
Other (please specify):



Prefer not to say



Top of Form

Bottom of Form

Top of Form

1. **What is phishing?**

Pretending to be someone or a company to steal users’ information  
Making a fake website that looks legitimate to steal user information  
Sending spam emails, Defrauding someone online  
Other methods for stealing information  
Hacking someone’s computer  
Tracking your internet habits to send advertisements   
I Do not Know



Bottom of Form

Top of Form

1. **What is the purpose of an X.509 certificate?**

The certificate provides encryption  
The certificate protects information  
The certificate shows the website is registered and valid  
The certificate actively is secure and safe against malicious stuff, including hackers  
The website is trustworthy and has proper privacy protection and is accountable for information use  
I Do not Know



Bottom of Form

Top of Form

1. **SQL injection is a technique to:**

Inject a malicious virus to the database SQL engine  
Inject a security patch to the database SQL engine in response to the discovery of new threats  
Inject a statement that checks the database integrity through a website  
Inject root user privileges to a regular user without using the graphical user interface (GUI) of the database  
Inject a malicious statement to the database through a website  
I Do not Know



Bottom of Form

Top of Form

1. **The difference between a passive and reactive Intrusion Detection System is?**

Passive IDS is software based and reactive is hardware based  
Passive IDS provides only alerts and reactive IDS can retaliate by sending malicious code to the attacker  
There are no real differences, they are just brand names  
Passive IDS is included in a Firewall while reactive IDS is a standalone network component  
Reactive IDS can reprogram the Firewall and passive IDS does not  
I Do not Know



Bottom of Form

Top of Form

1. **Without any other changes in the default settings of a web server, what can be the motivation to close port 80?**

Block incoming XMLhttp Request  
Block File Transfer Protocol daemon  
Block Hypertext Transfer Protocol daemon  
Block incoming and outgoing requests from SMB/CIFS clients  
Block Hypertext Transfer Protocol Secure daemon  
I Do not Know



Bottom of Form

Top of Form

1. **How many computer programming languages do you know (Not including HTML)?**

10+  
5-10  
1-5  
1  
None



Bottom of Form

Top of Form

1. **How many years of working experience do you have in network operation and security area?**

10+ years  
5-10 years  
1-5 years  
A few months (less than a year)  
None



Bottom of Form

Top of Form

1. **On average, how many times do you have to deal with computer security related problems?**

Many times every day  
Once every day  
Once every week  
Once every month  
Once every year or less



Bottom of Form

Top of Form

1. **What information and network security tools do you use regularly? (Please mark all those that apply)**

Firewall  
Anti-virus  
Intrusion Detection System (IDS)  
Secure Shell (SSH)  
Pretty Good Privacy (PGP)  
Access control (AC)



Bottom of Form

Top of Form

1. **Have you ever (select all that apply)**

Designed a website  
Registered a domain name  
Used SSH  
Configured a firewall  
Created a database  
Installed a computer program  
Written a computer program  
None of the above



Bottom of Form

Top of Form

1. **Which of the following indicators do you use to decide if it is safe to enter your username and password on a particular website? Please mark all that apply.**

https  
lock icon on the page  
certificate  
website privacy statements  
type of website  
professional-looking website



other



Bottom of Form

Top of Form

Bottom of Form

Top of Form

1. **Others can access my smartphone or tablet without needing a PIN or passcode.**

Strongly disagree  
Disagree  
Neither agree nor disagree  
Agree  
Strongly agree



Bottom of Form

1. Top of Form
2. **Whenever I step away from my computer, I lock the screen.**

Strongly disagree  
Disagree  
Neither agree nor disagree  
Agree  
Strongly agree



Bottom of Form

Top of Form

1. **Rather than logging out of websites, I usually just navigate elsewhere or close the window when I’m done.**

Strongly disagree  
Disagree  
Neither agree nor disagree  
Agree  
Strongly agree



Bottom of Form

1. **Some IUPIC questions.**

Strongly disagree  
Disagree  
Neither agree nor disagree  
Agree  
Strongly agree

1. **Please answer the following questions about phishing.**
   * 1. Voluntary: To what extent do you have a choice in being exposed to this risk? (1=Voluntary; 5=Involuntary)

Completely voluntary  
Voluntary  
Neither voluntary nor involuntary  
 Involuntary  
 Completely involuntary

* + 1. Immediacy: Is the risk from the phishing immediate or does it occur at a later time? (1=Immediate; 5=Delayed)

Immediate   
Somewhat immediate  
Neither   
 Somewhat Delayed  
 Delayed

* + 1. Knowledge to the exposed: How much would a person like you reasonably know about the implications of phishing?

No knowledge   
Very little knowledge  
May or may not know about the risk   
 Knowledgeable   
 Very knowledgeable

* + 1. Knowledge to the expert: How much would an expert know about the implications of phishing?

No knowledge   
Very little knowledge  
May or may not know about the risk   
 Knowledgeable   
 Very knowledgeable

* + 1. To what extent can you control (or mitigate) the risk from being phished? (1=Uncon trollable; 5=Controllable)

Can prevent all harm  
Can prevent some harm

May or may not know be able to prevent harm   
 Can somewhat reduce harm  
 No control over resulting harm

* + 1. Newness: Is phishing a new risk resulting from new technologies or is it a new  version of an old risk? (1=Old; 5=New)

Entirely an old risk   
Mostly an old risk  
Neither new or old   
Somewhat new  
Completely new

* + 1. Common-Dread: Is phishing commonplace or rarely encountered? (1=Common; 5=Rare)

Common   
Infrequently encountered  
Neither common nor rare  
Frequently encountered  
Rare

* + 1. Chronic-catastrophic: Does phishing affect only the person who is phished or does it affect  many people? (1= Individual; 5=(Many People) Global)

Individual   
Multiple people  
May be global or individual  
Large numbers of people  
Global

* + 1. Severity: In the worst possible outcome, how severe are the consequences of phishing? (1=Not Severe; 5=Severe)

Not at all severe, trivial  
Not trivial but not severe  
Neither trivial nor severe  
May be severe  
Severe

1. **Please answer the following questions about account takeover.** 
   * 1. Voluntary: To what extent do you have a choice in being exposed to account takeover? (1=Voluntary; 5=Involuntary)

Completely voluntary  
Voluntary  
Neither voluntary nor involuntary  
 Involuntary  
 Completely involuntary

* + 1. Immediacy: Is the risk from the to account takeover immediate or does it occur at a later time? (1=Immediate; 5=Delayed)

Immediate   
Somewhat immediate  
Neither   
 Somewhat Delayed  
 Delayed

* + 1. Knowledge to the exposed: How much would a person like you reasonably know about the implications of account takeover?

No knowledge   
Very little knowledge  
May or may not know about the risk   
 Knowledgeable   
 Very knowledgeable

* + 1. Knowledge to the expert: How much would an expert know about the implications of account takeover?

No knowledge   
Very little knowledge  
May or may not know about the risk   
 Knowledgeable   
 Very knowledgeable

* + 1. To what extent can you control (or mitigate) the risk from being account takeover? (1=Uncon trollable; 5=Controllable)

Can prevent all harm  
Can prevent some harm

May or may not know be able to prevent harm   
 Can somewhat reduce harm  
 No control over resulting harm

* + 1. Newness: Is account takeover a new risk resulting from new technologies or is it a new  version of an old risk? (1=Old; 5=New)

Entirely an old risk   
Mostly an old risk  
Neither new or old   
Somewhat new  
Completely new

* + 1. Common-Dread: Is account takeover commonplace or rarely encountered? (1=Common; 5=Rare)

Common   
Infrequently encountered  
Neither common nor rare  
Frequently encountered  
Rare

* + 1. Chronic-catastrophic: Does account takeover affect only the person who is phished or does it affect  many people? (1= Individual; 5=(Many People) Global)

Individual   
Multiple people  
May be global or individual  
Large numbers of people  
Global

* + 1. Severity: In the worst possible outcome, how severe are the consequences of account takeover ? (1=Not Severe; 5=Severe)

Not at all severe, trivial  
Not trivial but not severe  
Neither trivial nor severe  
May be severe  
Severe

Scenario: You are visiting a website of a discount club. The club offers discounts on consumer products (e.g., electronics, media) to its members. Generally, an annual membership fee is $50. To obtain free membership, you are required to fill out your personal purchase preference information (e.g., favorite product category, brand, design).



1. Online companies would be trustworthy in handling my personal purchase preferences

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)

1. I trust that online companies would keep my best interests in mind when dealing with my personal purchase preference information.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)

1. In general, it would be risky to give my personal purchase preference information to online companies.

1 (Strongly Disagree)

2

3

4

5

6

1. (Strongly Agree)



1. There would be high potential for loss associated with giving my personal purchase preference information to online firms.

1 (Strongly Disagree)

2

3

4

5

6

1. (Strongly Agree)



1. I would feel safe giving my personal purchase preference information to online companies.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)

1. I am willing to give my personal purchase preference information to online companies in exchange for discounts on consumer products.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree

These are general privacy questions, not related to the scenario nor the experiment.

1. It usually bothers me when online companies ask me for personal information.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)



1. When online companies ask me for personal information, I sometimes think twice before providing it.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)



1. It bothers me to give personal information to so many online companies.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)



1. I'm concerned that online companies are collecting too much personal information about me.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)

1. Online companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)



1. When people give personal information to an online company for some reason, the online company should never use the information for any other reason.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)



1. Online companies should never sell the personal information in their computer databases to other companies.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)



1. Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.

1 (Strongly Disagree)

2

3

4

5

6

7 (Strongly Agree)