Appendix A. Questionnaire Parts

The survey is divided into four parts as shown below.

Appendix A.1. Personal and skill information

This part is optional, so the subject has ability to accept or decline the following questions.

1. **Gender**
   o Male
   o Female
2. **Age**
   o 18-29
   o 30-39
   o 40-49
   o Older than 49
3. **Education Level**
   o High school
   o Undergraduate
   o Postgraduate
   o Others
4. **Major**
   o Engineering
   o Public health
   o Computer science
   o Education
   o Languages
   o Business administration
   o Social science
   o Low
   o others, Specify:
5. **Administrative regions**
   o Riyadh
   o Makkah (Western Province)
   o Madina
   o Qassim
   o Eastern Province
   o Asir
   o Tabuk
   o Hail
   o Northern Board
   o Jazan
   o Najran
   o Baha
   o Jouf
   Note: In the analysis, we defined the ***Southern Province****, which includes following regions: Asir, Jazan, Najran, and Baha, while the* ***Northern Province*** *contains Tabuk, Hail, Northern Board and Jouf*.
6. **How often do you use the Internet and Internet-related services?**
   o Frequently throughout the day
   o Once or twice a day
   o Less frequently once a week or month
7. **What is your Internet/ Digital devices skills level**
   o Beginner, who can go to specific web pages, utilizes social media and a few applications such as Microsoft Word.
   o Intermediate, who has the ability to download applications, manages the settings of devices, and has knowledge about hardware as well as software.
   o Expert, who is a computer specialist, network engineer, or database administrator.
8. **Of the following, which digital devices do you use regularly?** *Tick all that apply*
   o Desktop
   o Laptop
   o Smartphone
   o Tablet
   o Other,
9. **What type of connectivity services do you use in your daily activities?** *Tick all that apply*
   o Public Wi-Fi
   o Private Wi-Fi
   o Cellular
   o Broadband
   o I do not know
10. **For what purposes do you use the Internet?** *Tick all that apply*
    o Education (e.g. information-seeking such as news, articles, etc.,))
    o Professional reasons (e.g. remote access VPNs)
    o Social networks (such as Twitter, Facebook, Snapchat etc.,)
    o Communication (such as using email, video calls)
    o Entertainment (e.g. playing games)
    o Online service (such as Government services, online banking, e-commerce, etc.,)

Appendix A.2. Cybersecurity Activities

The goal of this part is measuring awareness based on assessing the IT knowledge of the participant.

1. **What operating systems do you use on your desktop/laptop?** *Tick all that apply*
   o Windows 10
   o Windows 8
   o Windows 7
   o Old version of Windows
   o MacOS
   o Linux
   o I do not know
2. **What operating systems do you use on your Smartphone/tablet?** *Tick all that apply*
   o Windows
   o Blackberry
   o Android
   o iOS
   o I do not know

3. **Some of the most commonly used security tools and applications for laptops, tablets, mobiles, etc. are given below. Select which of these you have used on your digital devices.** *Tick all that apply*

   o Anti-virus
   o Authentication (e.g. password, PIN)
   o Encryption
   o Software Update
   o Backup
   o Firewall
   o None

4. **How secure do you feel your digital devices (e.g. computers and phones) are?**

   o Very secure
   o Somewhat secure
   o Neutral
   o Somewhat insecure
   o Not sure
   o Not secure at all

5. **Some security practices are described below.** *Please choose your common reaction for each practice*

   I check the legitimacy of a website before accessing it

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

   I create a password that contains my personal information (e.g. last name, date of birth)

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

   I am aware of the danger when clicking on banners, advertisements or pop-up screens that appear when surfing the Internet

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

   I give due attention to privacy settings on my social media account(s) (e.g. Facebook)

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

   Social media services protect my personal information.

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

   I read the terms and conditions carefully before using any website.

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

   I change the passwords of important accounts (such as online banking) frequently.

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

   I feel safe when using public Wi-Fi.

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

   I feel my digital device (computer, smartphone) has no value to hackers, they do not target me.

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

   I regularly install software updates.

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

   I am careful about clicking on links in an email or social media post.

   o Always
   o Often
   o Sometimes
   o Seldom
   o Never

6. **What digital devices do you have Internet security on (e.g. anti-virus)**? *Tick all that apply*

   o Desktop
   o Laptop
   o Smartphone
   o Tablet
   o I do not know
   o None of the above

7. **If you use Internet security (e.g. anti-virus), is this kept up to date in terms of threat filters and signatures?**

   o Yes, I manually updated.
   o Yes, I believe it is automatically updated.
   o No, I think it is automatically updated.
   o I do not know.

Appendix A.3. Cybercrime Consciousness

The goal of this part is evaluating the current awareness of the participants regarding cybercrimes by following questions.

1. **How do you keep yourself updated about cybercrime?** *Tick all that apply* . (Online sources)
   o TV, news, radio
   o Internet, website, email bulletins, blogs, etc.
   o Government websites
   o Internet service provider
   o Rely on automatic updates
   o I do not feel that I keep myself updated
   o Others, specify
2. **How do you keep yourself updated about cybercrime?** *Tick all that apply* . (Offline sources)
   o Newspapers, magazines, Posters
   o Professional activities: conferences, meetings, briefings, etc.
   o Internet service provider ISPs
   o Government or professional reports
   o I do not feel that I keep myself updated
   o Other, please specify
3. **What is your opinion of each of the following statements?** *Select the appropriate response for each*

   I think one should avoid disclosing personal information online
   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   I feel that the risk of becoming a victim of cybercrime has increased in the past year.
   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   I am concerned that my online personal information is not secure enough
   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   I feel that I am well protected against cybercrime.
   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   I am willing to accept increased Internet surveillance from the government if it can enhance Internet security.
   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   I believe that the laws in effect are effective in managing the cybercrime problem.
   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   I feel informed about the threat of cybercrime.
   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree
4. **There are several activities that constitute cybercrimes. How often have you experienced or been victim of the following situations?** *Select the appropriate response for each.*

   Received phishing emails (e.g. asking for money, personal information or bank account details).
   o Always
   o Sometimes
   o Never
   o Do not know

   Identity theft (somebody stealing your personal data and impersonating you, e.g. tweeting under your name).
   o Always
   o Sometimes
   o Never
   o Do not know

   Malware (e.g. virus) infection of a device.
   o Always
   o Sometimes
   o Never
   o Do not know

   Being unable to access online services (e.g. banking services) because of cyber attacks.
   o Always
   o Sometimes
   o Never
   o Do not know

   Accidentally encountering material that promotes hatred or religious extremism.
   o Always
   o Sometimes
   o Never
   o Do not know

   Online extortion (a demand for money to avert or stop extortion, or to avert scandal).
   o Always
   o Sometimes
   o Never
   o Do not know

5. **Some of the most common cybercrimes are presented below. What is your opinion of each of the following statements?** *Select the appropriate response for each.*

   I am concerned about identity theft (somebody stealing your personal data and impersonating you, e.g. tweeting under your name).

   o Always
   o Sometimes
   o Never
   o Do not know

   I am not concerned about accidentally encountering child pornography online.

   o Always
   o Sometimes
   o Never
   o Do not know

   I am concerned about receiving phishing emails (e.g. asking for money, personal information or bank account details.

   o Always
   o Sometimes
   o Never
   o Do not know

   I am concerned about not being able to access online services (e.g. banking services) because of cyber attacks.

   o Always
   o Sometimes
   o Never
   o Do not know

   I am concerned about accidentally encountering material that promotes hatred or religious extremism.

   o Always
   o Sometimes
   o Never
   o Do not know

   Online extortion (a demand for money to avert or stop extortion, or to avert scandal).

   o Always
   o Sometimes
   o Never
   o Do not know

   Other, Specify

6. **What do you feel about the threat of cybercrimes in the future?**

   o They will become a more serious issue in the future

   o The threat will vanish eventually

   o No significant change

   o I do not know

7. **Considering each of the following parties, please rate the extent to which you believe they are responsible for raising awareness of cybercrime.**

   - The government

   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   -The media

   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   - Those offering online/Internet-based services (e.g. banks, online retailers, telecommunication companies, etc.)

   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   - User themself

   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   - Education system

   o Strongly Agree
   o Agree
   o Neutral
   o Disagree
   o Strongly Disagree

   o Others, specify:

8. **What do you think the role of the government should be in combating cybercrimes?** *Tick all that apply*

   o Have stricter laws and punishments for cybercrimes.

   o Make people aware of cybercrime

   o Monitor organizations misusing consumer information

   o Work towards providing a global cybersecurity framework

   o No role

   o I do not know

Appendix A.4. Case Reports

This part examined whether the participants had been a victim of a cyber-attack or not based on following questions.

1. **Have you been a victim of cybercrime? (E.g. lost data or email account, device infected with virus or spyware, stole your picture/s or digital device/s).**

   o Yes
   o No

2. **A. If Yes, When you had been a victim of cybercrime, did you report it?**

   o Yes
   o No

3. **A1. If Yes, To whom did you report or contact?** *Tick all that apply*
   o Saudi CERT
   o Police
   o Committee for the Promotion of Virtue and the Prevention of Vice
   o Saudi eGovernment Portal
   o No one
   o Others
4. **A2. If No, What was/were the reason/s?** *Tick all that apply*
   o I did not know how to describe or write reports about cybercrime
   o I did not know how to write reports about cybercrime
   o I did not know what the impact on me will be
   o I think that there is no value to reporting
   o I fixed the problem by myself
   o It was my fault to trust an unauthorized person
   o Not sure
   o I did not know what the crime was
   o I did not trust the third party
   o I feel it is waste of time
   o Others
5. **B. If No, If you become a victim of cybercrime would you like to report it?**
   o Yes, I would
   o No, I would not
6. **B1. If Yes, To whom would you report or contact?** *Tick all that apply*
   o Committee for the Promotion of Virtue and the Prevention of Vice
   o Saudi eGovernment Portal
   o Saudi CERT
   o Police
   o Committee for the Promotion of Virtue and the Prevention of Vice
   o Dont know but will ask friends for advice
   o Others
7. **B2. If No, What is/are the reason/s?** *Tick all that apply*
   o I do not know what the crime was
   o I do not know who to write report about cybercrime
   o I do not know what the impact on me will be
   o I do not know how to describe or write reports about cybercrime
   o I feel it is a waste of time
   o I think that there is no value to reporting
   o I do not trust the third party
   o I fixed the problem by myself
   o Not sure
   o Other