Submitted by -
Amanda Fellows, Gregory Haynes, Patricia Heiss, Pooja Upadhyay

Interview Protocol- Digital Security on the internet (Draft)

Research Question: How can a technology-based product or service help users understand cybersecurity risks and help them take appropriate measures to secure their personal data.

Screener questions:

(Note: options are for moderators to be aware of termination or continue criteria, do not read options out loud to participants)

1. Are you at least 18 years of age?
    [ ] Yes (continue)
    [ ] No (terminate)

2. Do you use a mobile device to conduct activities on the internet?
    [ ] Yes (continue)
    [ ] No (terminate)

3. Do you use a web browser on a laptop/desktop device?
    [ ] Yes (continue)
    [ ] No (terminate)

4. How often do you use the internet?
    [ ] Once daily (continue)
    [ ] Multiple times daily (continue)
    [ ] Less than once daily (terminate)

5. Which of the following activities do you conduct online?
    [ ] Search and browsing only (terminate)
    [ ] Email only (terminate)
    [ ] Social networking only (terminate)
    [ ] Payments / banking only (terminate)
    [ ] All (continue)

Introduction:

Thank you for agreeing to participant in this study of Digital Security Perceptions. My name is _____, and I am a graduate student at DePaul University. The aim of this study is to determine to what extent do internet users understand cybersecurity; or data security; risks and how to minimize those risks.

The interview will take about 45 minutes and your answers will be kept confidential.
Before we begin, please review and sign the informed consent form. Thank you. Do you have any questions for me?

Interview Questions:

NOTE:
- Follow up questions are mentioned as - bullet points
- Conditions to follow up questions are mentioned as [If yes], [If no]. Moderators should ask all other questions

Warm up

(Build rapport and get participant to think about their actions)

1. Which browser do you use the most? (If needed, give examples: Chrome, Firefox)

    - What features do you like about it?
    - Do you use more than 1 browser?
    - Do you think using more than 1 browser impacts the security of your personal information?

2. Which websites do you perceive as secure, and visit often?

    - Which websites do you perceive as unsecure?
    - Why do you think they are unsecure?

3. Have you received any information or tips about cybersecurity; or data security; through work, school, websites or word-of-mouth?

    - [If yes] Can you describe to me what you learned about cybersecurity; or data security?

General browsing activity

4. Do you think there are any risks associated with browsing on (browser mentioned in Q1)?

    - [If yes] What types of risks?
    - [If yes] Do you use any security measures while browsing to protect your information?

5. While browsing the web, how do you know if a website is secure?

    - How do you think using unsecure websites affects your personal information?

6. What is your experience with fake websites?

    - How would you differentiate between a fake and a genuine website?
    - How do you think fake websites affect the safety of your information?

7. What is your experience with pop-up ads or links on websites and videos?

    - Do you perceive any risk from pop-ups or ads?
    - Do you use ad-blockers or popup- blockers?
    - What do you think ad-blockers or popup-blockers do?

8. While providing your information on websites, do you use autofill forms?

- [If yes] What type of information is saved on your browser for autofill? (If needed, give examples: Credit card info., home address, phone number, full name)
- [If yes] Do you control what type of information is saved by this feature?
- [If yes] Are there any specific websites for which you use this feature, or for general browsing?
- [If no] Have you witnessed your browser providing suggestions while filling forms? What do you think about that?

9. Do you perceive any risk from using autofill in filling forms?

    - [If yes] What types of risk?

10. Do you think your browser protects you from unsecure websites?

    - [If yes] How?

Account related activity

11. Do you use the remember password/ login credentials feature to enter passwords?

    - [If yes] Do you do that on your personal devices, other computers/devices, or both?
    - [If yes] Do you keep track of how many passwords are saved in your device?
    - Do you trust your browser to maintain the safety of passwords?

12. Do you use any password manager software? (If needed, give examples: Last pass or 1Password)

    - How do you think password managers work?
    - Do you otherwise store your passwords as paper notes, electronic notes, in email or elsewhere?

13. Do you use the same password for all accounts, or different passwords?

    - Why? Do you think this has any effect on the safety of your information?
    - How long are your passwords; how many characters?
    - What type of characters do you use in your passwords?

14. Have you shared your passwords with friends or family?

    - [If yes] How did you share it with them?
    - Do you think it could affect the safety of your information? How?

15. Do you use the "stay logged in" feature while logging into your personal accounts such as Gmail or yahoo etc.?

    - [If yes] Do you use that feature on personal devices, other devices /computers, or both?
    - Do you think it could affect the safety of your information? How?
    - Do you specifically log out of your accounts when using non-personal devices?
    - Do you use "incognito" mode / private browsing? [If yes] Why?

Payment related activity

16. What kind of risks, do you think, are associated with online payments?
17. What websites do you conduct payment activities on?

- Do you trust these websites to protect your payment information?

18. Do you use your credit / debit card information to make payments online?

- [If yes] Do you save your payment information online?
- [If yes] What kind of payment information do you save online?
- [If yes] Do you use your card information on specific websites only?

19. Do you use services such as Apple pay/PayPal to store and use payment methods?

- Do you think these services are safer than entering card information online?
- [If no] How do you conduct payments online for shopping, banking etc.?

20. How do you assess the safety of a payment webpage; What do you look for?
21. What kind of additional safety measures do you use while conducting payments?
22. Do you share payment or banking related information online?

- [If yes] How?

23. Do you use online or mobile banking to monitor your card usage?
24. Have you received emails asking for your payment details?

- What do you think about them?

Internet activity on different devices

25. While using your mobile and your laptop/computer, do you think one device is safer over the other for specific activities?

- [If yes] Can you explain more about the activities?

26. Do you connect to wifi networks other than home/school/workplace?

- Do you think connecting to other networks could affect the safety of your personal information?

Wrap up

27. Can you tell me about security risks that one could face while using the internet? (other than what we spoke about)

- Can you describe these risks to me?

28. Do you use any additional security measures to protect your personal information? (other than what we spoke about)

- [If yes] Can you tell me how you think they protect your data?
- [If no] Are you aware of any other security measures that could be taken?

29. If there was a technology product to teach users about cybersecurity; or data security; do you think it would help internet users know more?

- What features should it to have?
- (if needed) What kind of security measures would you want to know about?

Demographics:

1. How old are you?
2. What is your occupation?
3. How often do you use the internet on a typical day?
4. What kind of internet activities do you conduct on a typical day?

Conclusion

This concludes the activity. Thank you again for taking the time to meet with me today. If you have any questions later, please feel free to contact me. I can be reached at _____.
Your input will be helpful for us in understanding user perception of data security.