Waterhouse interview questions
Alex Lambert; Steve Bezek

These questions were borrowed from Simson Garfinkel’s “Johnny 2” study, which is based on Tygar’s original “Why Johnny Can’t Encrypt” study. Garfinkel suggested that future studies reuse the scenario and questions so the community has a metric by which to judge new solutions (like ours).

Goal: Determine how well inexperienced users (with respect to security) can send secure e-mail and understand the security properties of electronic messaging using Waterhouse.

Experiment: a very condensed version of the Johnny2 study.

Prequestions

Thank you for your interest in participating in the testing! Here is the intake questionnaire. The answers will be used to select a set of test participants that has the particular demographic characteristics needed for this research study. All information you give will be kept private, and will only be included in research results in anonymized form.

1. How old are you?

2. What is your highest education level (high school, some college, undergrad degree, some grad school, grad degree)?

3. What is your profession or main area of expertise (for example arts, science, medicine, business, engineering, computers, administration...)?

4. For how long have you been using electronic mail?

5. Have you ever studied number theory or cryptography?

6. Have you ever used security software, such as secure email in Thunderbird or Microsoft Outlook, or PGP, or any other software that involved data encryption? If yes, what was the name of that software?

7. Do you know the difference between public (asymmetric) key cryptography and private (symmetric) key cryptography? If yes, please explain briefly.

8. How do you read your email? (What program or online service?)

9. How did you hear about this study?
Debriefing

1. Rate the ease of use of Waterhouse, on a scale from 1-7
   1  2  3  4  5  6  7

2. Rate your perception of the overall security provided by Waterhouse, on a scale from 1-7
   1  2  3  4  5  6  7

3. Did you notice the colored security messages?

<show small screenshots with labeled UI text>

4. What did message 1 mean to you? <message 1 will be “sender verified with Facebook”>

5. What did message 2 mean to you? <message 2 will be “protected from eavesdropping”>

6. What did message 3 mean to you? <message 3 will be “sending with extra protection”>

<show small screenshot of message w/o security decorations>

7. If you saw this message, would you believe that the sender’s e-mail address could be forged? Why or why not?

8. If you saw this message, would you believe that others could have eavesdropped on it? Why or why not?

9. Was there anything you thought about doing but then decided not to bother with?

10. Is there anything you think you would have done differently if this had been a real scenario rather than a test?

11. Were there any aspects of the software that you found particularly helpful?

12. Were there any aspects of the software that you found particularly confusing?

13. Are there any other comments you’d like to make at this time?