Expert vs. Non-Expert Security Practices

Mike Reiter

Lawrence M. Slifkin Distinguished Professor
Department of Computer Science


Expert Interview

- Interviews with 40 experts
  - In-person semi-structured interviews of 40 security experts at the 2013 BlackHat, DefCon, and USENIX Security conferences
  - Expert = attendee who reported having at least 5 years of experience working in or studying computer security
  - Question: “What are the top 3 pieces of advice you would give to a non-tech-savvy user to protect their security online?”
Survey of 231 experts via Mechanical Turk

- Expert = survey participant who reported having at least 5 years of experience working in or studying computer security
- Question: “What are the 3 most important things you do to protect your security online?”
- Asked about 14 pieces of advice mentioned frequently in the interviews
  - E.g., “Do you use two-factor authentication (e.g., 2-step verification) for at least one of your online accounts?”

Survey of 231 experts via Mechanical Turk (cont.)

- Asked to rate the “goodness” of 20 pieces of advice mentioned frequently in the interviews
  - Asked to consider both how effective the advice was at keeping the user secure and how realistic it was that users could follow it
Non-Expert Survey

- Survey of 294 non-experts via Mechanical Turk
  - Called for participation in a Google study about Internet use
  - Survey content was largely the same as in the expert survey
User Authentication

- I remember passwords
- I write down passwords
- I use a password manager
- I use the same password

Do you use two-factor authentication?

Web Browsing

- Do you look at the URL bar?
- Do you check if HTTPS?
- Do you visit websites you have not heard of?

Percentage of Participants
Email Habits

Summary

- The three things that experts do that many non-experts do not
  - Install updates
  - Use a password manager
  - Use two-factor authentication