

Users Are Not Stupid: Eight Cybersecurity Pitfalls Overturned

Julie Haney

Computer Scientist & Usable Cybersecurity Program Lead
National Institute of Standards and Technology
julie.haney@nist.gov



Disclaimer

Throughout the presentation, certain commercial companies or products may be identified to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor does it imply that the companies or products identified are necessarily the best available for the purpose.



The Human Element of Security

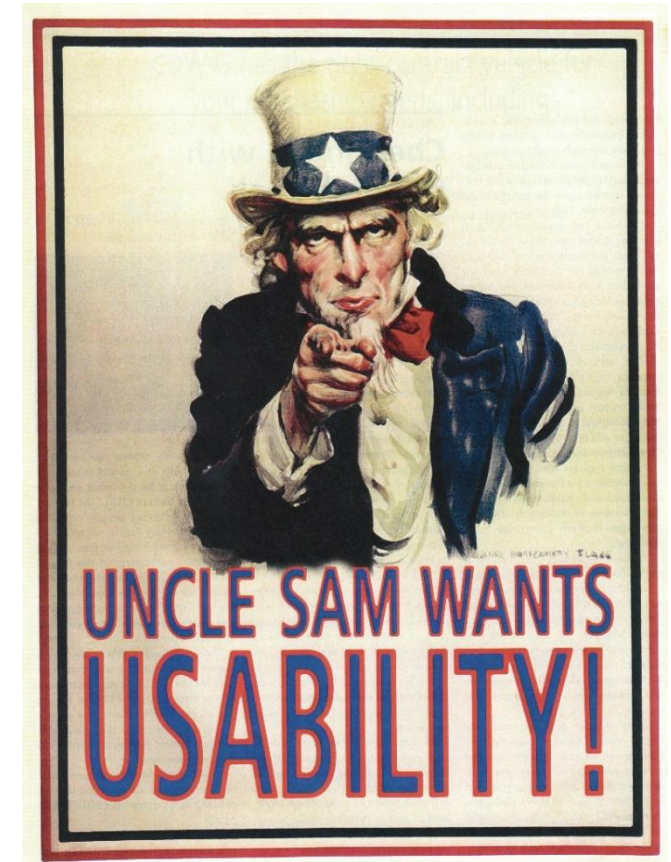


Usability



the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency & satisfaction in a specified context of use

[ISO 9241-11:2018](#)



Usable Security



Security must be usable by persons ranging from nontechnical users to experts and system administrators. Furthermore, systems must be usable while maintaining security. In the absence of usable security, there is ultimately no effective security.



A Roadmap for Cybersecurity Research, U.S. Department of Homeland Security, 2009

Why the Human Element is Often Overlooked



Cybersecurity is a technology-centric field



Many security professionals have little to no training on the human element



Taking a human-centric approach may be viewed as resource-intensive



Security professionals may have misconceptions about the human element

Eight Pitfalls




Pitfall #1: Not identifying all the users in security

- Often only think of “end users” and then lump them all together
- May fail to recognize other people impacted by security solutions and decisions




Pitfall #1: Example



Your resource for keeping your small business secure.

Get cybersecurity basics, guidance, solutions, and training to protect your information and manage your cybersecurity risks.



Credit: Wendy Szwerc

Pitfall #2: Assuming users are stupid or hopeless

- Viewing users as the “weakest link” and the root of all problems
- Us vs. them mentality
- Comes across as arrogant, antagonistic
- Removes user agency



Pitfall #2: Example



Security Fatigue

[Security Fatigue](#)

Pitfall #3: Not tailoring communications

- “Curse of knowledge”
- Not accounting for:
 - Knowledge/skill level
 - Constraints and preferences
- Not addressing relevance to people’s job duties and lives



You can produce as many policies and processes as you like. If you cannot communicate them to people in a language they understand, in a language that means they’re going to be receptive to your message, then they’re worthless.



[“It’s Scary...It’s Confusing...It’s Dull”: How cybersecurity advocates overcome negative perceptions of security](#)

Pitfall #3: Example



Overturning Pitfalls #1, #2, and #3

1 Empathize, intend to empower

- Realize we're all human
- Try to understand root causes
- Build relationships

3 Be a translator

- Use appropriate language
- Provide digestible guidance
- Communicate the “why”
- Enlist help

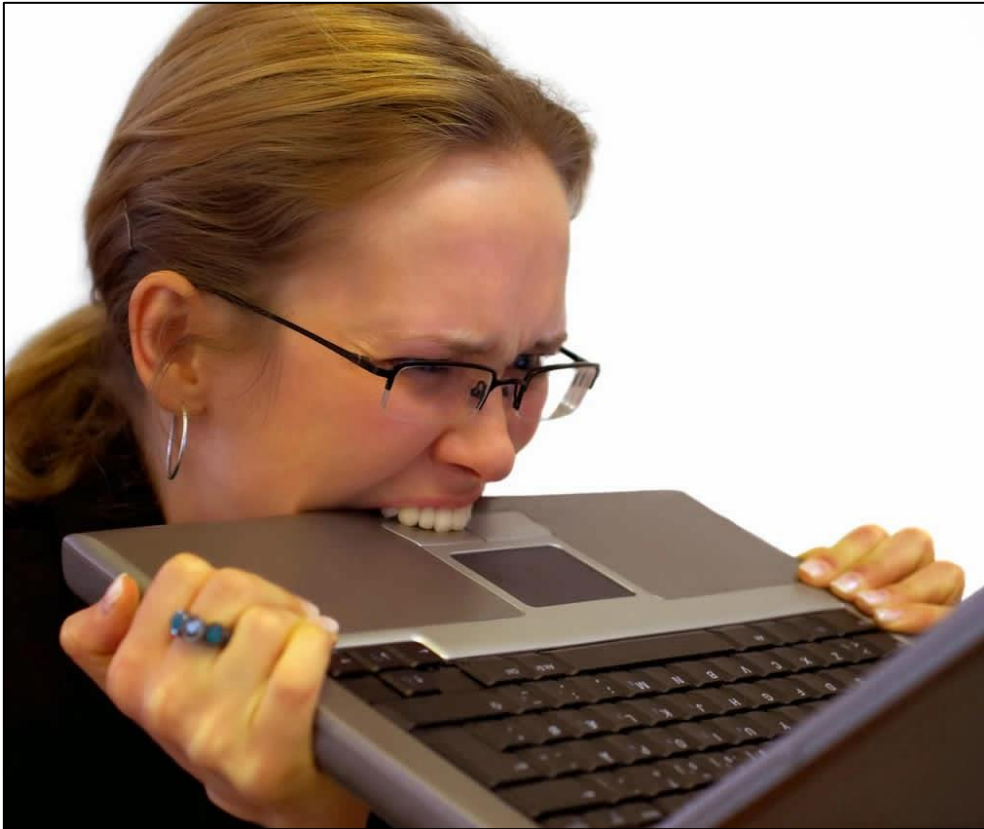
2 Be context aware

- Who are your users?
- What's the environment?
- Where are the interaction points and impacts?

4 Mix it up

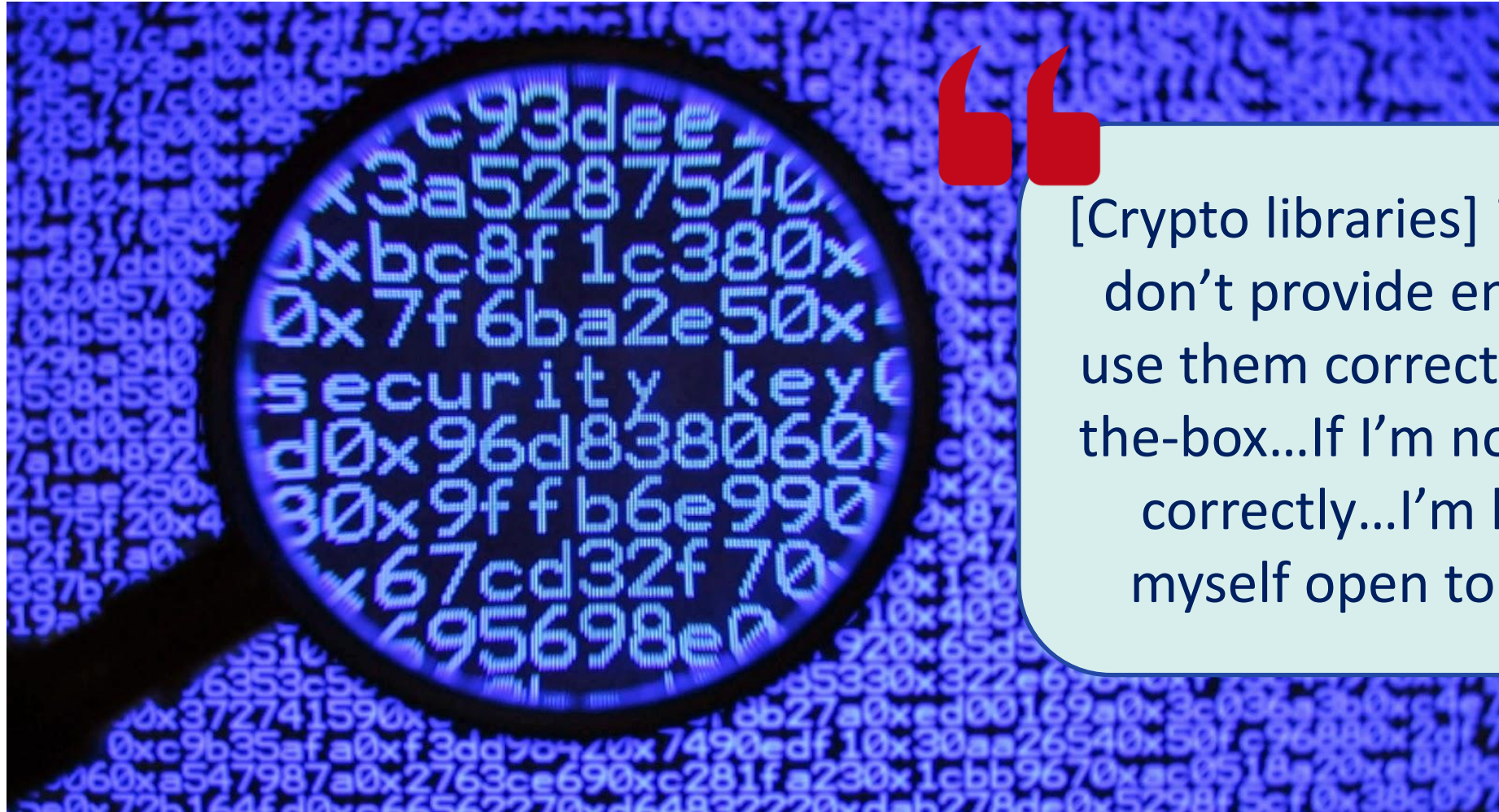
- Use a variety of formats to disseminate information
- Accommodate different preferences and constraints

Pitfall #4: Putting too much burden on users



- Pushing users beyond their limits
 - Time
 - Effort
 - Cognitive load
- Can result in errors, frustration, anxiety

Pitfall #4: Example

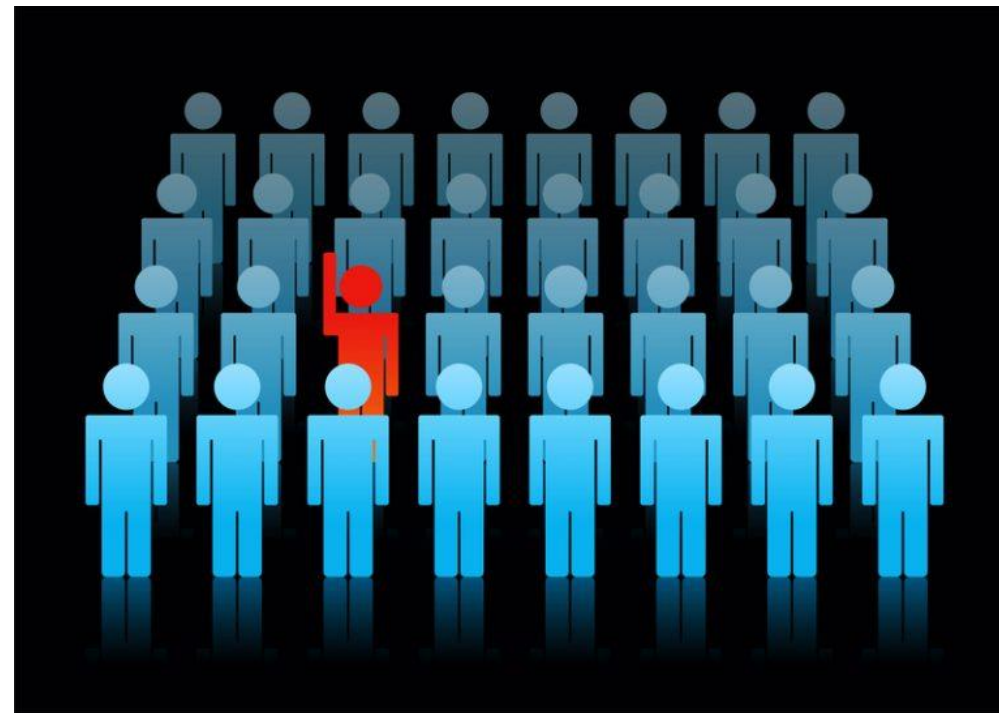


[Crypto libraries] in general don't provide enough to use them correctly out-of-the-box...If I'm not using it correctly...I'm leaving myself open to attack.

"We make it a big deal in the company": Security mindsets in organizations that develop cryptographic products

Pitfall #5: Making users into insider threats due to poor usability

- Unusable security may backfire
- Stringent security measures may be viewed as counterproductive
- To cope, users may engage in workarounds or make risky decisions



Pitfall #5: Example



Change Temporary Password

This is your first login. Please change the temporary password to a more personalized password in order to continue. Clicking the 'Change' button will log you out of the platform.

Old Password:

New Password: i

Confirm Password:

strong

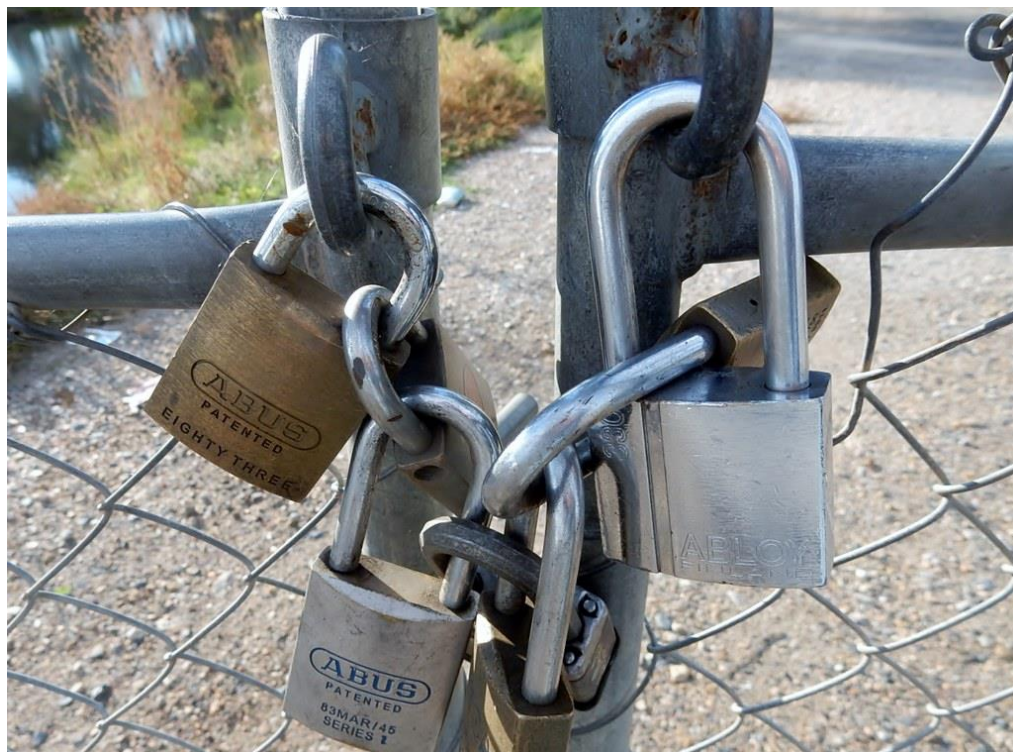
Change

Password must

- Be at least 6 characters in length
- Must not reuse previous 6 passwords
- Must contain at least one lowercase character
- Must contain at least one number
- Must not repeat the Login ID
- Must not reverse the Login ID
- Must not contain more than three repetitive characters
- Must not contain number as the last character

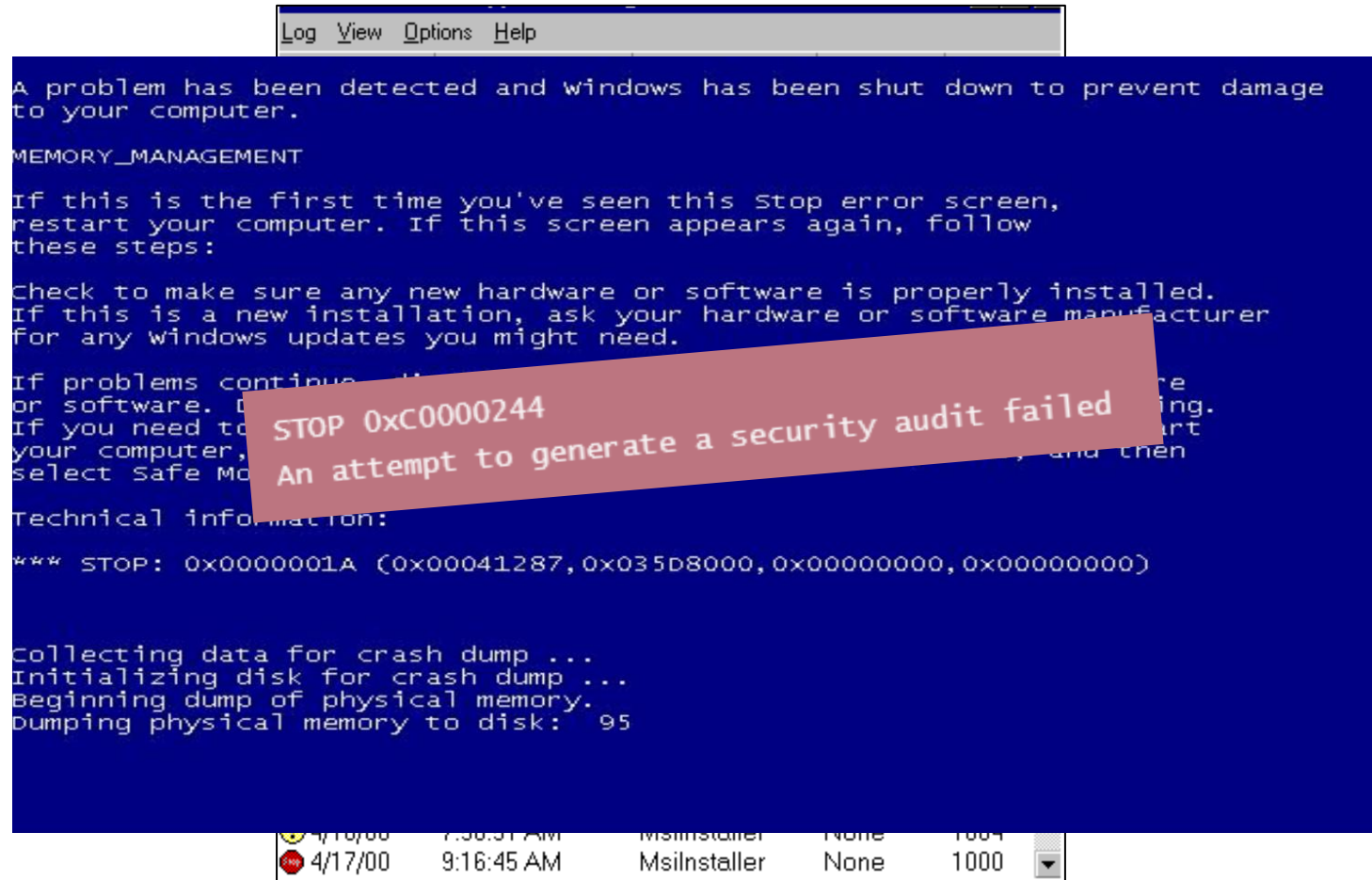


Pitfall #6: Assuming the most secure solution is best



- “One-size-fits-all” approach
- High level of security may not be practical or necessary for everyone/all organizations
- May cause unforeseen impacts on users

Pitfall #6: Example



Overturning Pitfalls #4, #5, and #6

1 Conduct basic usability testing

- Pilot proposed solutions
- Observe errors, misinterpretations
- Ask for feedback

3 Offload burden when possible

- Don't expect the impossible or difficult
- Offload difficult tasks to computers or those better equipped

2 Make it actionable

- Provide tools and achievable guidance
- Break down into manageable, prioritized chunks

4 Take a risk-based approach

- Avoid “one-size-fits-all” solutions
- Tailor to the environment and its security needs

Pitfall #7: Using punitive measures to get users to comply

- Punishing users for security mistakes or lapses
- Negative messaging
- May be counterproductive, turn people off from security



Pitfall #7: Example



Pitfall #8: Not considering user feedback and user-centric measures of effectiveness



- Not seeking out user-centric security indicators/data
- Not incorporating user feedback
- Results in a blind spot about user impacts, behaviors, and attitudes



Pitfall #8: Example



Overturning Pitfalls #7 and #8

1 Don't rely on fear alone

- Fear doesn't always prompt action
- Honestly communicate the risk
- Build self-efficacy to take action

3 Gather user-centric data

- Identify “symptoms” via user-level security incidents, help desk calls
- Get to root cause by going straight to the source
- Encourage feedback

2 Be positive

- Recognize good security behaviors
- Be collaborative and instructive rather than punitive

4 Use data to drive improvements

- Incorporate what you found to improve user's security interactions
- Communicate what was done

Takeaways



Apply What You've Learned Today



- Next week you should:
 - Think about where you/your colleagues may be falling victim to the pitfalls
 - Start identifying *all* your users and ways in which they may be negatively impacted by security
- In the first three months following this presentation you should:
 - Begin gathering user-centric data to uncover both symptoms and root causes of security issues
 - Devise and execute a repeatable process for obtaining user feedback and piloting new security solutions

Parting Thoughts



You can't do it alone!

Do your part to consider the human element and empower others to be informed, capable, and active partners in security.

Thank You!

julie.haney@nist.gov

<https://csrc.nist.gov/usable-cybersecurity>



References & Resources

- Bada, M., Sasse, A. M., & Nurse, J. R. (2019). [Cyber security awareness campaigns: Why do they fail to change behaviour?](#) *arXiv preprint arXiv:1901.02672*.
- Choong, Y. & Theofanos, M. F. (2015). [What 4,500+ people can tell you – Employees' Attitudes toward Organizational Password Policy Do Matter](#). In *Proceedings of the 3rd International Conference on Human Aspects of Information Security, Privacy, and Trust* (2015)
- Dawson, J., & Thomson, R. (2018). [The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance](#). *Frontiers in Psychology*, 9.
- Green, M., & Smith, M. (2016). [Developers are not the enemy!: The need for usable security APIs](#). *IEEE Security & Privacy*, 14(5), 40-46.
- Hadnagy, C., & Fincher, M. (2015). *Phishing Dark Waters: The offensive and defensive sides of malicious emails*. John Wiley & Sons.
- Haney, J., Lutters, W., & Jacobs, J. (Jul./Aug. 2021) [Cybersecurity Advocates: Force Multipliers in Security Behavior Change](#). *IEEE Security & Privacy*, 19(4).
- Haney, J. M. & Lutters, W. G. (2021). [Cybersecurity Advocates: Discovering the Characteristics and Skills for an Emergent Role](#). *Journal of Information and Computer Security*, 29(3), 485-499.
- Haney, J.M. & Lutters, W. G. (Oct. 2020). [Security Awareness Training for the Workforce: Moving Beyond “Check-the-box” Compliance](#). *IEEE Computer*, 53(10)
- Haney, J. M. & Lutters, W. G. (2018). [“It’s Scary...It’s Confusing...It’s Dull”: How Cybersecurity Advocates Overcome Negative Perceptions of Security](#). In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS 2018)* (pp. 411-425).
- Haney, J. M., Theofanos, M., Acar, Y., & Prettyman, S. S. (2018). [“We make it a big deal in the company”: Security Mindsets in Organizations that Develop Cryptographic Products](#). In *14th Symposium on Usable Privacy and Security (SOUPS 2018)* (pp. 357-373).

References & Resources

- International Organization for Standardization (2018). ISO 9241-11:2018 Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts. <https://www.iso.org/standard/63500.html>
- Pfleeger, S. L., & Caputo, D. D. (2012). [Leveraging behavioral science to mitigate cyber security risk](#). *Computers & Security*, 31(4), 597-611.
- Post, G. V., & Kagan, A. (2007). [Evaluating information security tradeoffs: Restricting access can interfere with user tasks](#). *Computers & Security*, 26(3), 229-237.
- Renaud, K., & Dupuis, M. (2019, September). [Cyber security fear appeals: Unexpectedly complicated](#). In *Proceedings of the New Security Paradigms Workshop* (pp. 42-56).
- Spitzner, L. (Oct. 10, 2016). [What makes a good security awareness officer?](#) Educause Review.
- Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). [Security fatigue](#). *IT Professional*, 18(5), 26-32.
- Steves, M. P., Greene, K. K., & Theofanos, M. F. (2020). [Categorizing Human Phishing Difficulty: A Phish Scale](#). *Journal of Cybersecurity*, 6(1), tyaa009.
- Wash, R. (2010, July). [Folk models of home computer security](#). In *Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS 2010)* (p. 11).
- West, R., Mayhorn, C., Hardee, J., & Mendel, J. (2008). [The Weakest Link: A Psychological Perspective on Why](#). In M. Gupta (Ed.), *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*.