Security Awareness Training for the Workforce: Moving Beyond "Check-the-box" Compliance

Julie Haney, National Institute of Standards and Technology
Wayne Lutters, College of Information Studies, University of Maryland
HCIL Symposium, May 27, 2021

Employees continue to fall prey to cyber attacks

Photos used in this presentation are licensed under Creative Commons.

Security awareness training

- Two-fold
  - Bring awareness of issues
  - Provide skills and tools
- Various sectors mandate annual training
- Hope is that compliance will result in sustainable behaviors

BUT does compliance-based training really live up to its promise?

Issues with compliance-based training

- Bad reputation
- Unprepared security awareness professionals
- Unknown effectiveness

Research Efforts

- Interview study of 28 cybersecurity advocates
- Year-long case study of a security awareness team in a U.S. government agency
- In-progress @ NIST: Mixed-methods study (focus groups & survey) of government security awareness programs

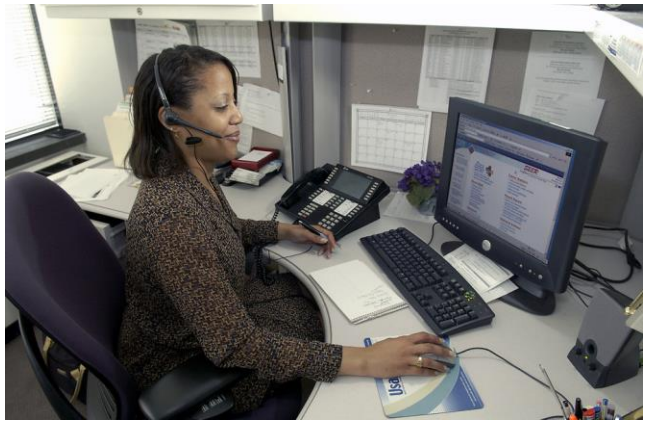
Behavior change, not just compliance

Become an advocate

> If you're a computer scientist, and all you know is the computer science, and you don't have the empathy, you don't have the skills to listen,…you don't have that psychological side, I don't think you can make it work.

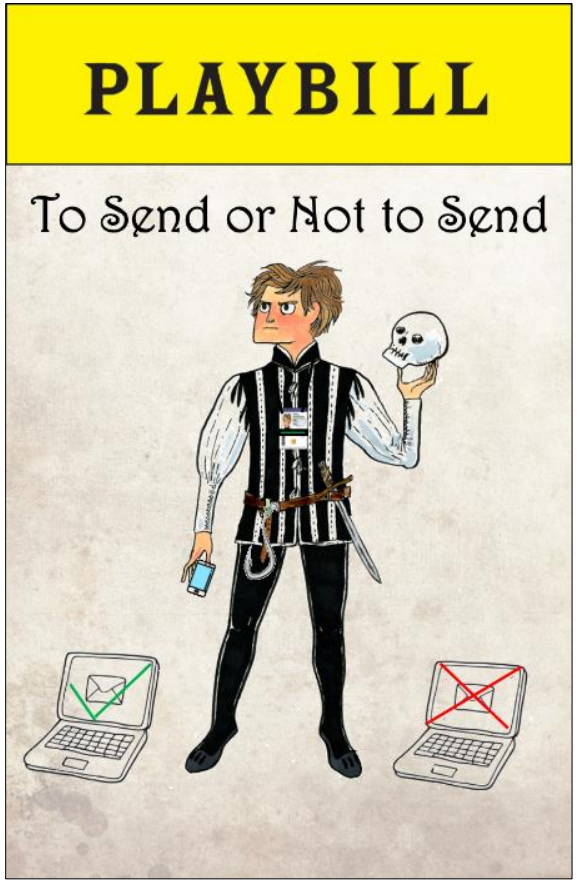
Make security relatable

- Communicate the business value of security
- Show the linkage between security and work duties to prompt sense of personal responsibility
- Provide topical information
- Emphasize the work-home connection



Get employees' attention

> You want to just put a different spin on it because people just see stuff all the time: 'Have a good password. Lock your computer'… Be creative and think outside the box.



Empower

- Provide appropriate tools and guidance to empower employees
- Recommendations should be:
  - Prioritized
  - Practical and achievable
  - Described in easy-to-understand terms

Remember that security is a journey!

Small steps with big impact

Measure the impact

- Completion rates aren't enough
- Examples:
  - Attendance – how many & who
  - Employee feedback
  - User-generated security incidents & reporting
- Holistic approach
- Contextualize and develop targeted solutions

> tie in together the people who take their training to…people who are losing their badges to people who send out information they shouldn't to see what's the correlation here. Are these people just too busy? Are they not paying attention? Is there a training problem?

Be positive

Don’t underestimate the power of positive reinforcement!

Takeaways

- There are baseline benefits of mandated security awareness training
- But compliance doesn't equate to attitude and behavior change
- Organizations should go beyond compliance to engage and empower employees to be responsible cyber citizens in and outside of work

Thank you!

julie.haney@nist.gov

lutters@umd.edu

Haney, J., & Lutters, W. (2020). Security Awareness Training for the Workforce: Moving Beyond "Check-the-Box" Compliance. *Computer*, 53(10), 91-95.

NIST

UNIVERSITY OF MARYLAND 18 56 COLLEGE OF INFORMATION STUDIES