Awareness Programs are Designed to Fail:
Behind every stupid user is a stupider security professional

Ira Winkler, CISSP
ira@securementem.com
+1-443-603-0200
ABCs of Awareness

• Awareness = Information
  – Statistically 20% of impact

• Culture = Consequence
  – 80% of impact

You don’t care about what people know; You only care about what they do
Why Do You Drive Safely?

• Isn’t it easy to drive dangerously?
• Isn’t it less convenient to drive safely?
• How frequently do you take mandatory training?
• Why do you drive safely?
• Why wear seatbelts?
NSA Badge Story
Behind Every Stupid User...

• …is a stupider security professional
  – Usually
• They ass/u/me knowledge
• If there is not a specific procedure or guideline in place that you can point to a user violating, it is your fault
• If you cannot show that the user was properly informed of the procedure or guideline, it is your fault

*There is no common sense without common knowledge*
Most Awareness Programs Are Just Gimmicks

- *Focus on pushing out information*
- They choose entertaining videos
- They come up with giveaways
- Tests of finite knowledge
- They treat security like a “Should”
- They are afraid to define required behaviors/actions with penalties, JUST LIKE ANY OTHER POLICY
Awareness Programs Should All Over People
Sommelier vs. Grandma
In Other Words

Awareness =

Culture =
ALL EMPLOYEES MUST:
1. Tape Webcam
2. Tape Microphones
3. Install Password Manager
4. Enable 2FA on their accounts
5. Use a Hardware Token

Do NOT use Hooli products.

Do NOT post pictures or videos of the office on Social Media.
Who Are You Creating?
Focus on Creating Culture

• Procedures and guidelines
  – How do people just do their jobs correctly, with embedded security

• Peer pressure

• Enforcement
The Book, The Myth, The Legend
For More Information

ira@securementem.com
+1-443-603-0200
@irawinkler
www.securementem.com
www.linkedin.com/in/irawinkler
Facebook.com/irawinkler