Making the Case for Cybersecurity Awareness Training

Dr. Tim Tillman, CETL, SFO
What is Awareness?

A series of educational training campaigns designed to help end-users combat malicious attacks, false narratives, and to exhibit expected safe behaviors.
Be suspicious.

It’s ok to delete.
Cybersecurity Awareness Basics

- Physical Security
- Social Engineering
- Phishing Identification
- Phishing Campaigns
- Incident Response
- Malware Identification
- Safe Browsing
- Legal Compliance
- Reporting and Alerting
- Real World Scenarios

- Removable Media
- Social Media Guidance
- Mobile Device Guidance
- Password Best Practices
- IoT Concerns
- Data Protection / Sharing
- Shredding
- Hardware Handling
- Suspicious Activities
- Lost/Stolen Devices
Why do we need it?
In terms of cybersecurity, humans are often the weakest link.
SONICWALL: ‘THE YEAR OF RANSOMWARE’ CONTINUES WITH UNPRECEDENTED LATE-SUMMER SURGE

- 148% surge in global ransomware attacks (495 million) year to date, making 2021 the worst year SonicWall has ever recorded
- Record-breaking total of 714 million ransomware attacks predicted by close of 2021
- Company recorded 1,748 ransomware attempts per customer through Q3
2021 Cybersecurity K12 Report

- 8 MILLION SCHOOL K12 DEVICES REPORTED COMPROMISED
- PHISHING ATTACKS DOUBLED FROM 2020 TO 2021
- KNOWN RANSOMWARE PAYMENTS OF $200M+ FROM K12 SCHOOLS
- ESTIMATED 50% OF LOSSES ATTRIBUTED TO PHISHING ATTACK
- #1 SOURCE IS CREDENTIAL COMPROMISE
- ADMINISTRATION OFFICIALS #1 TARGETS
How do we start?
Implementation Types

• Home-grown

• Free Resources
  • Cofense, Amazon, ESET, Inspired Learning

• Third-Party
  • Hook Security, KnowBe4, InfoSec Institute, Cynerd, Cymonix, Sophos, Rapid7, Kapersky, PhishLabs, SANS Institute, Cofense, TerraNova, ProofPoint
Implementation Best Practices

• Campaigns
• Not a compliance activity
• Not professional develop
• Repetition
• Enforce via Board Policy
• Require participation
• Garner leadership support
• Augment with newsletters, emails, posters, stress balls
• Mid-year reminders/refresh
• Shared Responsibility
• Culture of Advocacy, not Security
• Contiguous Improvement
Does it work?
Effectiveness and Metrics

• Research shows that consistent, engaging, and repetitive educational campaigns have a positive impact on user behavior.
• Establish performance baselines for engagement, phishing, and social engineering.
• Track metrics before, during, after and Y2Y
• Share results to encourage more engagement
Questions?