Top Human Risks

Lance Spitzner

securingthehuman.sans.org
lspitzner@sans.org
@securethehuman
Security Awareness Maturity Model

- Non-existent
- Compliance Focused
- Promoting Awareness & Behavior Change
- Long-Term Sustainment & Culture Change
- Metrics Framework
Keep it Short

Focus only on the topics that have the greatest ROI

- People can only remember so much (cognitive overload)
- You have limited time & resources
- Fewer topics easier to reinforce
- Avoid ‘training fatigue’
- Costs
Top Topics / Risks

- Phishing
- Poor password security
- Patching / updating
- Mobile devices
- Sharing too much on social media
- Not realizing you are a target
- Accidental data loss / exposure
Phishing
Dear Customer,

Unfortunately we unable to deliver your package this morning. We will be making two more attempts in the next 48 hours. If we are unable to deliver your package we will then have to return to sender. Please verify that your delivery address is correct by clicking on the link below, or updating the attached document.

Order# 44187

Shipping Tracking Information

Shipping Provider: UPS
Tracking #: IZ9Y424V039787851X
Tracking Information: http://www.ups.com/tracking/1Z9Y424V039787851X
Ship Date: 18/10/2012

Thank you,
United Parcel Service
Key Points

• People have feelings
• Announce program ahead of time, then start slow and simple
• Do not embarrass people (no Viagra e-mails)
• Do not release names of those who fail.
• Focus on real world risks, do not ‘trick’ people
• Monthly
• Once program matures, 5% / new hires.
Passwords
Typical Password Training

• A classic security awareness topic is passwords
  – Minimum 12 characters
  – 1 symbol
  – 1 number
  – 1 capital letter
  – Change every 90 days
• Costs associated with this
What are We Missing?

• Do not get infected
• Do not share your passwords
• Do not login using untrusted systems
• Personal questions for password reset
• Passphrases – Where is my Coffee?
• Different passwords for different accounts (encourage password managers)
• Use dual factor authentication when possible
Patching / Updating
Problem?

• People often think that updates are all about new functionality (new emojis) – they do not realize updates are also about security
• Updating can be hard / confusing
• Automate whenever possible
Mobile Devices
Biggest Threat?

It’s not malware, it’s losing your device.

– Put a pin / passcode on that device
– Do the butt check whenever leaving a taxi, plane, restaurant, room
– Point of contact sticker on device
Social Media
Over Sharing

But it’s not what you think

– Organizations typically train on - “Do not share company information”

– Problem is people share too much about themselves, making it easier for targeted attacks

– It’s the bits and pieces that people post which is then pieced together
You Are a Target
Engagement

• People do not feel like they are a target, as a result they do not care
• People feel security team / technology will protect them – “But I have Anti-virus installed”
• Feel like their actions don’t make a difference
• Engage people at an emotional level, explain WHY they should care.
Accidental
Accidents

Far too often forget about accidental.

– Auto-complete in email
– Forgetting documents in the taxi or your laptop at airport security
– Uploading data to the ‘test’ server
2016 Security Awareness Report

• Survey of security awareness officers
  – Questions developed by community
  – 369 took the survey
• Results analyzed by five community experts
  – Bob Rudis (Verizon DBIR)
  – Dr. Lance Hayden (People Centric Security)
  – Angela Sasse (Prof, University College of London)
• Release in two weeks - (webcast 29 Mar)
Upcoming Events

- Monthly Webcasts
- Security Awareness Summits
  - San Francisco: 04/05 Aug
  - London: 11 Nov
- SANS MGT433 Courses

[securingthehuman.sans.org/events]