Why People are Susceptible to Phishing

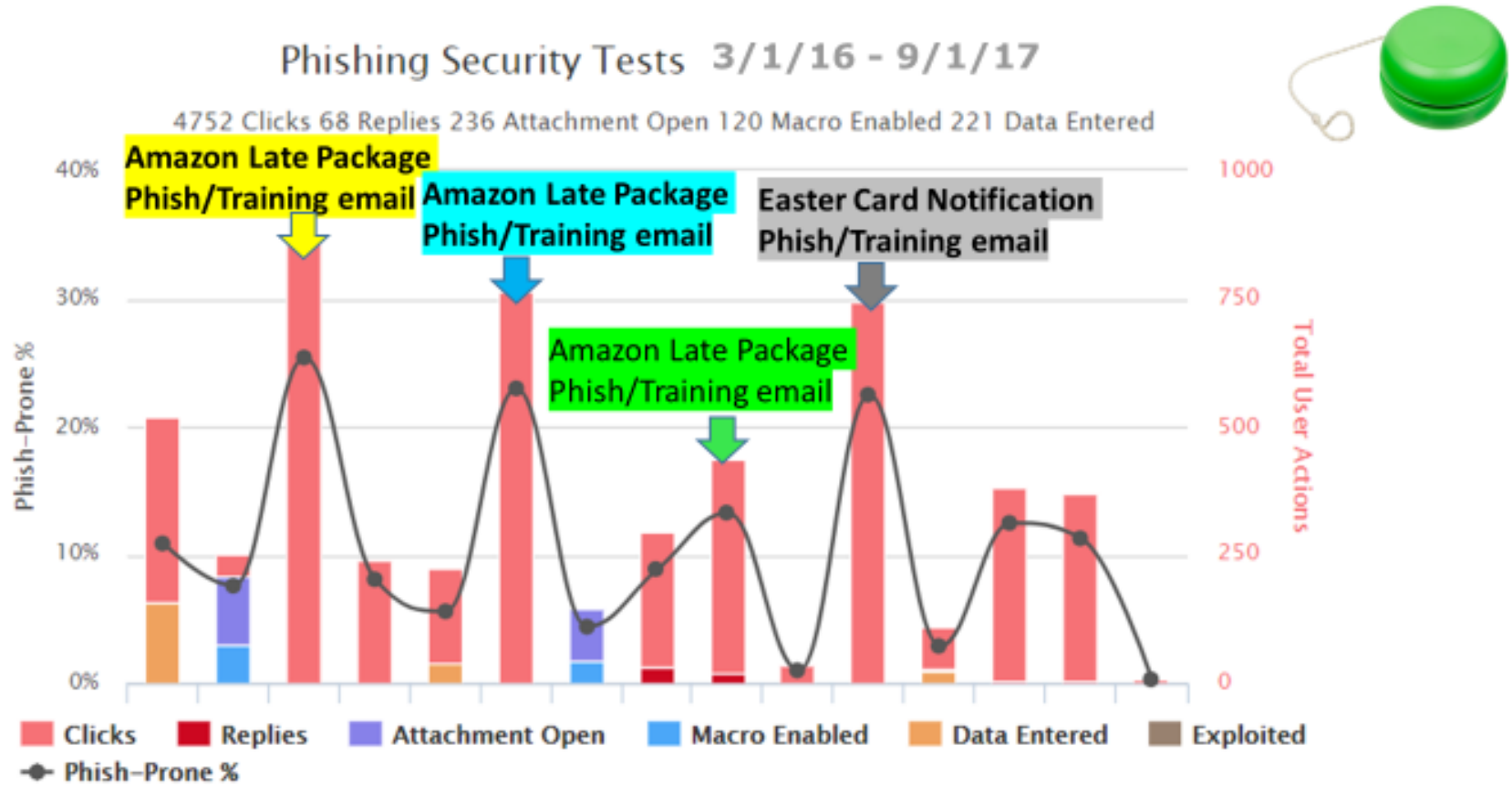
James Robinson, Ph.D.
Center for Cybersecurity & Data Intelligence

University of Dayton

Why are people susceptible to phishing?

- **Assumption**: End users are susceptible to phishing because they lack the information they need & experience identifying phishing attack messages
- **Solution**: Rule-Based Training
  - Writing errors
  - Urgency
  - Generic greetings
  - Dodgy email address
  - Requests for private or personal information
  - Threats
  - URL's or modified URL's,
  - Unusual domain name
  - Low quality graphics/images
- **Outcome**: Reduced rates of victimization (especially short term)
- **Let's look at the data…**

Phishing Employees – Every 2 Weeks over 7 Months



University of Dayton

This is not what we would expect

- There are three reasons people remain susceptible
  1. Conditioned to click links
  2. Multitasking produces inattentional blindness
  3. People rely on heuristics
- Let’s look at these three reasons more closely

Conditioned Behavior

- People click on links – many can't help themselves
  - They can't stop because they've been conditioned to click URL's
  - Behaviorists would say the target behavior (clicking links) is reinforced when they receive the information they desire
    - The strength of the target behavior is determined by how quickly the reinforcement follows the click, and
    - The number of clicks it takes to get the reinforcement – bad search results & bad links further strengthen the target behavior

✓ How much thought do rats give to pressing a lever that drops food into their cage?

✓ Would rule-based training help a rat?

✓ How much do you think before clicking a link?

University of Dayton

Inattentional Blindness

University of Dayton

ELM & Information Processing

- The Elaboration Likelihood Model suggests that people process information in two very different ways
  - **Central Processing** occurs when people carefully scrutinizes information
    - People process information centrally based on topic salience
    - When people think information is important, they process it carefully
  - **Peripheral Processing** occurs when information is not believed to be important
    - Instead of mindful consideration of the information they rely on heuristics to evaluate the information
    - I bet the surgeon general is a pretty good doctor, so if she says don't smoke, I probably shouldn't smoke
- As you might expect, when people are multitasking, they often process information peripherally or with little effort/thought

A Study to Make this Idea Clear

- Langer asked people making copies if she could make her copies first
  1. One third were asked “Excuse me, I have 5 pages. May I use the Xerox machine?” (Request Only individuals let her make copies first 60% of the time)
  2. One third were asked “Excuse me, I have 5 pages. May I use the Xerox machine, because I’m in a rush?” (Request + Real Information people let her make copies 94% of the time)
  3. The final third were asked “Excuse me, I have 5 pages. May I use the Xerox machine, because I have to make copies?” (Request + Placebo information people let her make copies 93% of the time)
- Moral: The reason for making a small request is not very important

Langer Study – Part Two

- Langer asked people making copies if she could make her copies first
  1. One third were asked “Excuse me, I have 20 pages. May I use the Xerox machine?” (Request Only individuals let her make copies first 24% of the time)
  2. One third were asked “Excuse me, I have 20 pages. May I use the Xerox machine, because I’m in a rush?” (Request + Real Information people let her make copies 24% of the time)
  3. The final third were asked “Excuse me, I have 20 pages. May I use the Xerox machine, because I have to make copies?” (Request + Placebo information people let her make copies 24% of the time)
- Moral: The rationale for the request matters if a request is large but not if the request is small

Langer Study Relevance to Phishing Susceptibility

- In the context of phishing, when the attack message contains a request that is small, information is processed less carefully
- The word BECAUSE in the request functions as a heuristic – a reason for the request is coming
  - Because people are cognitive misers, it is easier for them to comply with a small request than it is to scrutinize it
  - So we see that one key to reducing victimization is motivating people to process email requests carefully – regardless of the request size
- We see Rule-Based Training is not help if people are processing info. peripherally. They are not being mindful so they miss/ignore the cues

The Research on Phishing & Mindfulness

- Jensen et al (2017) found rates of victimization decrease when mindfulness training into the traditional Rule-Based training
  - Adding mindfulness training to message cue recognition training reduced rates of victimization from 13.4% to 7.5%
  - Mindfulness training reduces victimization because it reduces
    - Mindless or conditioned clicking of links
    - People miss message cues because they are inattentionally blind
    - Mindless responses to request that result from relying on heuristics and not the careful processing of email requests

Comparing Mindfulness & Rule Based Training

Mindfulness Training

1. **Stop!**
   - Don't do anything by reflex or habit
2. **Think . . .**
   - Does email ask for private/proprietary info?
   - Is the request unexpected or rushed?
   - Does the request make sense?
   - Why would the sender need me to do this?
   - Can I solve this problem with a phone call instead of a reply to an email
3. **Check.**
   - Does the email address look legitimate?
   - Is there contact information in the email?
   - Does the contact information match the contact information available online?

Rule-Based Training

1. Never click on a link or open an attachment in an e-mail from an unknown sender.
2. Access a website by typing the web address yourself.
3. Do not reply to e-mails asking for private information.
4. Real organizations such as banks or employers will never ask for private information in an e-mail.
5. Be suspicious of an email or a website that asks for private information.
6. Look for cues such as HTTPS in the address bar or a lock icon in your browser to identify a fake website.
7. Look for threats & a sense of urgency
8. Check for writing errors

One Final Reason Training Fails

- **The Cyber-Health Belief Model (CHBM)**
- The CHBM identifies six message characteristics that should be included in any effort to promote cybersecurity awareness & behavior
- Motivating end users to be security conscious by explaining
  - Their **susceptibility of** being victimized in cybersecurity attack
  - The consequences or **severity** of being victimized
  - The **benefits** & costs or **barriers** of security consciousness (2 sided messages)
- In addition, end users need to be provided **cues to action** or reminders to be security conscious
- Most importantly end users need to have a sense of **self-efficacy**
  - End users must believe they can protect themselves against an attack

Susceptibility & Severity Messages

- **Susceptibility Messages**
  - Phishing's #1 cause of data breaches
  - 30% of phishing messages are opened
  - Hackers attack every 39 seconds
  - ~30% phishing emails evade network security
  - 57 million victims (Uber breach)
  - Hackers attack someone 2k times a day
  - 150 million victims (Under Armor breach)
  - 500 million phishing attacks in 2022
  - In 2022, 300,497 phishing victims
  - 36% of all breaches involved phishing
  - 3.4 Billion phishing emails sent every day
- **Severity Messages**
  - Financial loss occurs in ~25% attacks
  - In at will employment states (Ohio)
    - Victims can be fired for breaches
    - 1 in 4 reportedly do get fired
  - Consequences of victimization
    - Increased levels of stress (71%)
    - Negative mental health impact (63%)
    - Adverse effects on physical health (39%)
  - Credit Card Fraud/Phishing
    - 25% of victims experience financial loss
    - Average loss ~$500 if fraud goes unreported for 2 days

Susceptibility + Severity Messages = Fear Appeals

- Using susceptibility & severity is to motivating end users with fear
- Fear appeals contain two components
  - **A threat** (e.g., susceptibility & severity information)
  - **A solution** (or strategy for avoiding the threat)
- The documentary *Scared Straight* (1978) reported juvenile delinquents changed their evil ways after exposure to prisoners at Rahway State Prison
  - Research suggests fear appeals/scared straight programs produce higher rates of criminality & recidivism than the juvenile criminal justice system
  - Research also suggests why fear appeals work and when fear appeals will not motivate change

When Do Fear Appeals Work?

- People respond to threats/fear appeals in two ways
  - **Danger Response** means the individual changes their behavior to avoid the risk identified in the fear appeal
  - **Fear Response** means the individual counterargues against the evidence and denigrates the source of the threat
- People respond with a Danger Response when they believe the solution to the threat will be effective (response efficacy) & when they feel efficacious (believe they can successfully enact the solution)
- When people do not have a sense of self-efficacy, they do not change their behavior
- Training must focus on increasing end user feelings of self-efficacy

The Implications of Fear Appeals & Training

- If the training does not increase feelings of self-efficacy, people will not change their attitude or their behavior
  - Worse yet, they will counterargue against the solution/training and strengthen their anti-training attitude
- If the training does not make end users feel that the solution will be effective, they will not voluntarily engage in the solution or advocated security behavior either
  - Attitude and behavior change is more than the provision of information and efficacy (self and response) is critical to training success

Conclusions

- If we do not raise mindfulness and feelings of self-efficacy, our training is going to be less effective.
- If we rely on rules based training, we must be sure that the rules actually discriminate between email and phishing attacks
  - Go home and look at your email – say the next three days.
  - Now compare the content of your email to the rules.

What percentage of your email messages contain

- Writing errors
- Urgency
- Generic greetings
- Dodgy email address
- Requests for private or personal information
- Threats
- URL’s or modified URL’s,

- We may need better rules, too