PRIVACY, SECURITY AND USABILITY

Training and Awareness

Training and Awareness

- Phishing-Cybersecurity

Spear phishing

- Targets specific groups of individuals
- Often targeted towards an organization's employees rather than their customers

High volume of phishing attacks

- 76% of businesses reported being a victim of a phishing attack in the last year
- 30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or link
- 95% of all attacks on enterprise networks are the result of successful spear phishing [SANS Institute]
- Nearly 1.5 million new phishing sites are created each month]

Trends Summary

- Phishing was found > 200 different top level domains
- The number of unique phishing reports submitted to APWG during Q3 2017 was 296,208
  - nearly 23,000 more than the previous quarter
- Phishers are using HTTPS protection to fool victims into thinking phishing sites are safe
  - Most-targeted sector: payment providers

Why phishing works

- Phishers take advantage of Internet users' trust in legitimate organizations
- Lack of computer and security knowledge
- People don't use good strategies to protect themselves

Anti-phishing strategies

- Silently eliminate the threat
  - Find and take down phishing web sites
  - Detect and delete phishing emails
- Warn users about the threat
  - Anti-phishing toolbars and web browser features
- Train users not to fall for attacks
- Recover from attacks quickly

User education is challenging

- Users are not motivated to learn about security
- For most users, security is a secondary task
- It is difficult to teach people to make the right online trust decision
  - without increasing their false positive errors

Is user education possible?

- Security education “puts the burden on the wrong shoulder.” [Nielsen, J. 2004]
- “Security user education is a myth.” [Gorling, S. 2006]
- “User education is a complete waste of time…. They are not interested…they just want to do their job.”

  [Martin Overton, a U.K.-based security specialist at IBM, http://news.cnet.com/2100-7350_3-6125213-2.html]

Web site training study (1)

- Teaching Johnny Not to Fall for Phish [Kumaraguru, et Al. 2010]
- Laboratory study of 28 non-expert computer users
- Control group: evaluate 10 sites, 15 minute break to read email or play solitaire, evaluate 10 more sites
- Experimental group: evaluate 10 sites, 15 minutes to read web-based training materials, evaluate 10 more sites

Web site training study

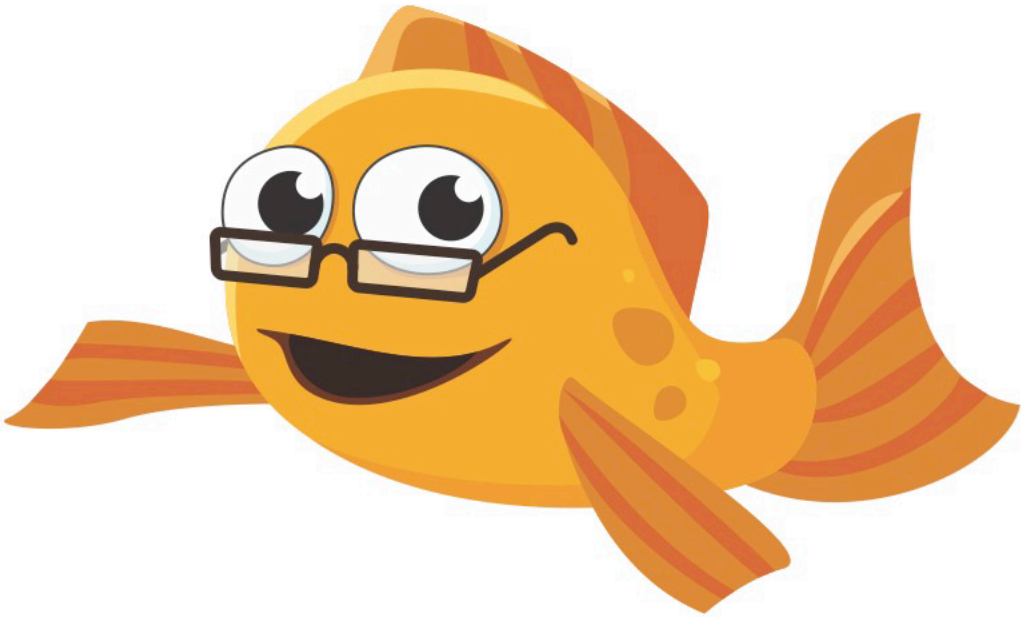
- Experimental group performed significantly better identifying phish after training, but more false positives
- People learn from online training, if only they pay attention!

How to get people trained?

- Problem
  - Existing materials good, but could be better
  - Most people don't proactively look for security training materials
  - "Security notice" emails sent to employees and/or customers tend to be ignored
    - Too much to read
    - People don't consider them relevant
- Solution
  - Find a "teachable moment": PhishGuru
  - Make training fun: Anti-Phishing Phil
  - Use learning science principles

Solution: Develop training software

- PhishGuru
- Anti-Phishing Phil



PhishGuru embedded training

- Send emails that looks like a phishing attack
- If recipient falls for it, intervention warns and highlights what cues to look for in succinct and engaging format
- User studies have demonstrated that this is effective
- Delivering same training via direct email is not effective!

From research to reality

- Iterated on PhishGuru designs
- PhishGuru user studies
  - Laboratory
  - Real-world
- Anti-Phishing Working Group landing page
- PhishGuru commercialized by Wombat Security
- Technologies, Inc., acquired by Proofpoint in 2018

Lab Study Result

- Protecting people from phishing: the design and evaluation of an embedded training email system [Kumaraguru, 2007]
- Security notices are an ineffective medium for training users
- Users educated with embedded training make better decisions than those sent security notices

Real-World Follow-up Study

- A Real- World Evaluation of Anti-Phishing Training [2009 Kumaraguru]
- Evaluate effectiveness of PhishGuru training in the real world
- Investigate retention after 1 week, 2 weeks, and 4 weeks
- Compare effectiveness of 2 training messages with effectiveness of 1 training message

Study Design

- 515 participants in three conditions
  - Control
  - One training message
  - Two training messages
- Emails sent over 28 day period
  - 7 simulated spear-phishing messages
  - 3 legitimate messages from ISO (cyber security scavenger hunt)
- Exit survey

Implementation

- Unique hash in the URL for each participant
- Demographic and department/status data linked to each hash
- Form does not POST login details
- Campus help desks and all spoofed organizations were notified before messages were sent

Results

- People trained with PhishGuru were less likely to click on phishing links than those not trained
- People retained their training for 28 days
- Two training messages are better than one
- PhishGuru training does not make people less likely to click on legitimate links
- Age was most significant factor in determining vulnerability

Results (cont.)

- Students significantly more likely to fall for phish than staff before training
- No significant differences based on student year, department, or gender
- 18-25 age group were consistently more vulnerable to phishing attacks on all days of the study than older participants

Training User Satisfaction

- 280 completed post study survey
- 80% recommended continuing PhishGuru training
  - “I really liked the idea of sending CMU students fake phishing emails and then saying to them, essentially, HEY! You could’ve just gotten scammed! You should be more careful - here’s how....”
  - “I think the idea of using something fun, like a cartoon, to teach people about a serious subject is awesome!”

ANTI-PHISHING PHIL

Anti-Phishing Phil

- https://www.youtube.com/watch?v=c1Es2qza1II

User Study

- Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish [Sheng 2007]
- Online game
- Teaches people how to protect themselves from phishing attacks
  - identify phishing URLs
  - use web browser cues
  - find legitimate sites with search engines

User Study

- Test participants' ability to identify phishing web sites before/after training
  - 10 URLs before training, 10 after, randomized
  - Up to 15 minutes of training
- Three conditions:
  - Web-based phishing education
  - Tutorial
  - Game
- 14 participants in each condition
  - Screened out security experts
  - Younger, college students

Results

- No significant difference in false negatives among the three groups
- Game group performed best in false positives
- All training we tested made people more suspicious
  - but only the game helped people distinguish phish from legitimate web sites

What contributed to Phil's success?

- Addresses a problem people are concerned about
- Fun to play
- People like to win things (or even just get points)
- Get trained fast (about 10 minutes)
- Teaches actionable steps
- Interactive, reinforces learning

Conclusions

- Security user education is possible
- Conventional wisdom: end-user security training does not work
- Anti-phishing work shows otherwise
  - You can teach Johnny not to fall for phish
- We should still aim to reduce or eliminate computer security threats through technology
  - and enforcement
- But complement these with user education

User education in other security/ privacy areas

- What types of user education have you experienced that you think it effective?
- Ineffective?
- What areas would most benefit from user education?

PhishTank

- Evaluating the Wisdom of Crowds in Assessing Phishing Websites [Moore & Clayton, 2008]
- Studied ‘PhishTank’, a crowd online community
  - Created for fighting phishing
- Users submitted suspicious emails or voted on suspicious emails

PhishTank

- Findings:
  - A few highly-active users carry the load
  - Most users participate very little, but their aggregated contribution is substantial
  - Nearly all (97%) submitted URL's verified as phishing
  - Very few false positive (39 out of over 100K submissions) and false negatives (3)
  - Users with bad voting record vote together

PhishTank

- Voting introduces significant delays to verification
  - 46 hr average delay (15 hr median)
  - Company, by contrast, uses employees to verify immediately
  - Impact can be seen by examining sites reported to both feeds

PhishTank

- While leveraging the wisdom of crowds sounds appealing, it may not always be appropriate for information security tasks
- After examining one such effort, we found its decisions to be mostly accurate but vulnerable to manipulation
- Compared to a similar proprietary effort, PhishTank is less complete and less timely

Personality and Phishing

- Real-world phishing study [HJM13]
- User with certain personality traits shown to be more susceptible to phishing attacks
  - Gender also found to be a factor

Personality and Spear-Phishing

- Follow-up real-world spear-phishing study [HMN15]
- Showed that tailored messages can lure even cautious users
  - Most unlikely users to respond to such attacks
- Raises possibility of creating tailored education to personality traits

USABILITY FOR DEVELOPERS

Usability for Developers

- Developers Deserve Security Warnings, Too [Gorski et. Al, 2018]

Usability for Developers

- Controlled online experiment with 53 participants
- Examines the effectiveness of API-integrated security advice:
  - informs about an API misuse
  - places secure programming hints as guidance close to the developer.
- Examines insecure cryptographic choices including:
  - encryption algorithms, key sizes, modes of operation and hashing algorithms
    - with helpful documentation in the guise of warnings. Whenever possible,

Usability for Developers

- the security advice proposes code changes to x theresponsible security issues.
- Found that the approach proposed significantly improves code security
- 73% of the participants
- who received the security advice fixed their insecure code

Questions?