Supporting Trust Decisions Through Anti-Phishing Education

Alessandro Acquisti, Lorrie Cranor, Sven Dietrich, Julie Downs, Jason Hong, Norman Sadeh
Carnegie Mellon University http://cups.cs.cmu.edu/trust/

End-user security education challenges
- Security is a secondary task
- Users are not motivated to spend time learning about security
- It is difficult to teach people to identify security threats without also increasing their tendency to misjudge non-threats as threats

PhishGuru
“Embedded training”
- Users get sent periodic training emails that look like phishing attacks
- If a user clicks a “phishing” link, they are shown succinct and engaging information on protecting themselves from phishing

User study results
- Sending training materials through normal email is ineffective but users are motivated to learn after falling for fake phishing attack
- Users retain and transfer knowledge better when trained after falling for fake phishing attack compared to getting the training materials through normal email
- We are currently testing this method in the real-world

Anti-phishing Phil
- A web-based interactive game to teach people how to avoid phish by paying attention to URLs
- Players move Phil around the screen to examine bait and identify URLs as phishing or legitimate

User study results
- Lab study showed people made better decisions after playing the game compared to reading online training materials
- 4,517 people participated in online study
- Online study results demonstrated that playing the game helped people learn to make better decisions
- People retained the knowledge after one week

Lab study results: mean correctness before, immediate, and after one week delay

Online study results: false negative before, immediate, and after one week delay

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT