Merging Big Data and Behavioral Risk Analysis to Demystify Phishing and Derive Actional Behavioral Risk Intelligence

Joshua Crumbaugh

peoplesec.org

We Know Phishing

- PeopleSec Provides Advanced & Intelligent Phishing Training for Enterprises Around the Globe
  - 3 Years of Research
  - Users in 4 Continents & 11 Countries
  - We Literally Wrote the Book on Security Awareness Training.

peoplesec.org

Gaining a Better Understanding of Phishing Susceptibility

- What are organization's greatest phishing attack vectors?
- How can we improve organizational security against phishing attack vectors?
- How do demographics impact phishing susceptibility?
- How do job roles/functions impact phishing susceptibility?

peoplesec.org

About Me

- Joshua Crumbaugh
- Chief Hacker/CEO of PeopleSec
- Career Social Engineer & Ethical Hacker
- Internationally Acclaimed SME & Keynote Speaker
- Published Author

peoplesec.org

Disclaimer

- These findings are based on data PeopleSec's phishing emulations and behavioral intelligence.
- Your findings may vary
- The purpose of reporting our findings is to stimulate conversation and get others sharing their trend and demographics data

No Two Departments Are The Same

The Most at Risk Departments

- Sales
  - Social Media Themed Phishes
- HR
  - Business Communications Themed Phishes
- Marketing
  - Social Media Themed Phishes
- Developers
  - Business Communications Themed Phishes
- Senior Management
  - Ego Themed Phishes

peoplesec.org

How Does Gender Impact Susceptibility?

- Women
  - Tend to be more engaged in educational activities
  - Less susceptible over time
  - Higher rate of initial susceptibility
- Men
  - Lower educational engagement than women
  - Initially less susceptible than women
  - Long term women tend to overtake men as most secure

peoplesec.org

Does Age Impact Phishing Susceptibility?

- Phishing Susceptibility
  - 26-35 Tend to be Most Susceptible
  - 56-65 2nd Most Susceptible
  - 18-25 Tend to be Least Susceptible
- Educational Engagement
  - 46-65 Tend to be Most Engaged
  - 18-25 Leads Engaged
  - All other age groups were very similar

peoplesec.org

Why Small Percentages Matter

1.23% of Users Represent 89.82% of Total Phish Risk

What About Sensitive Information Users?

- In most organizations users with access to sensitive information and systems tend to create a disproportionate amount of phishing susceptibility.
  - Due to HR and Developers Exhibiting Greater Susceptibility?
  - Greater Responsibility == More Distractions

peoplesec.org

What About Locations

- France & Australia == Biggest Skeptics
  - Loves to Open Phishes, but Rarely Clicks
- India == Chronic Clickers
  - They tend to be one of the most susceptible workforce locations
  - USA is a close second

peoplesec.org

Most Clicked Types of Phishes

- Social Media & Spear Phishes Neck to Neck
- Business Communications Themed Phishes are @ 3rd Place
- Ego Based Phishing is Highly Effective @ 4th Place
- Security Themed Phishes are @5th Place
- Current Events Themed Phishes are @ 6th Place
- Personal Business Themed Phishes are @ 7th Place

peoplesec.org

Go Figure...

- On average the less users engage in education the more they click on phishes
- The more users engage in education the less they click on phishes

peoplesec.org

Lessons Learned

- Phishing is a complex threat
- Phishing behavioral intelligence is key to remediating the threat
- Demographics can serve as a phishing susceptibility indicator and should be monitored and investigated at a great level
- Trends change over time

peoplesec.org

So How Do We Fix It?

- Users Are a Lot Like Computers
- Difficult to Train Easy to Program

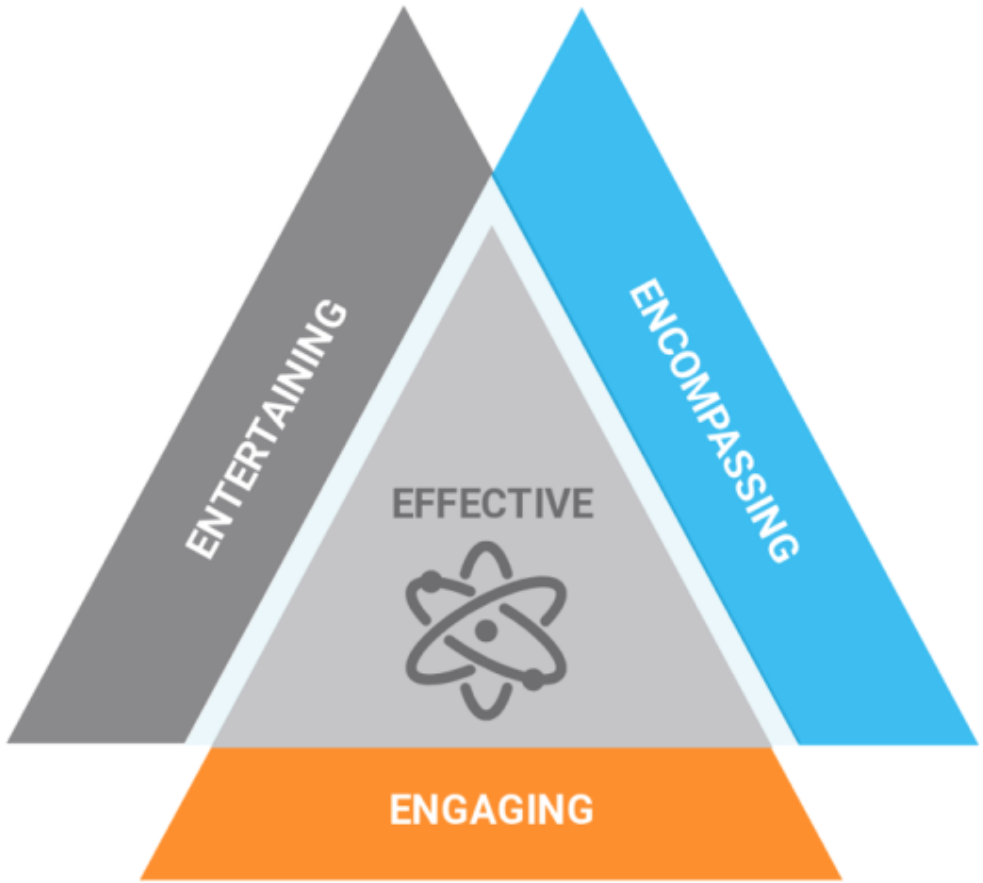
peoplesec.org

The Science and Psychology of Learning and Behavioral Change

- Most Companies Do Not Have Adequate Internal Talent to Run Their Security Awareness Programs
- A Good Candidate
  - Understands The Intricacies of Security Awareness
  - Understands The Psychology Behind Behavioral Change
  - Understands The Science of Learning
  - Has an Understanding of CyberSecurity

peoplesec.org

The FOUR E's of security awareness



ENTERTAINING

We must entertain our users to make them want to learn

ENCOMPASSING

Does the program address all human security weaknesses?

ENGAGING

Users must be engaged in security monitoring and protection

EFFECTIVE

Programs need to be measured by results not compliance.

Missing Engagement

- Average Users Don’t
  - Understand Their Impact on Security
  - Understand Their Role in Security
  - Want to be the Weakest Link
  - Will Try Harder if With Better Understanding

peoplesec.org

Missing User & Phishing Risk Insight

- Did They Click & What Did They Click On Is Not Enough
- These Are Some Insights I Have Found
  - What Other Questions Should We Be Asking?
  - How Can We Use This Insight?

peoplesec.org

Infrequent Training

- Annual or Even Quarterly Training Does Not Keep Security Front of Mind
- Threats Evolve Daily - Not Annually
- Not Taking Advantage of All Touch Points
- Infrequent Training Causes Overly Complex Messaging
- Retention Take Repetition - Think Marketing/Advertising

peoplesec.org

Bad & Boring Content

- We NEED To Entertain Users
- We Need Emotional Anchoring
- We Need Shorter Points of Contact
- We Need Simplified Education

peoplesec.org

Not Phishing Enough

- Phishing For The Purpose of Education:
  - Don’t Exploit Users
  - Ensure You Phish Your Users With All Types of Phishing Attacks
  - The Cure to Spear Phishing is Spear Phishing
  - Life Circumstances Can Impact Security
  - Helps Identify Risk Users Before The Bad Guys Do

Ask Yourself This:

DO YOU WANT THE BAD GUYS TO BE THE ONLY ONES IN YOUR USER’S INBOX OR DO YOU WANT TO BE THERE TOO?

peoplesec.org

QUESTIONS?

Joshua Crumbaugh

joshua@peoplesec.org

844-40-PHISH x700

Twitter: @NagaSecurity

peoplesec.org