Phishing

Matthew Kunzman
Information Security Lead
Clearwater Analytics, LLC
http://www.mattkunzman.com

Biggest Threats to Business Today

Misconfigured Systems

Unpatched Systems

Users

What is Phishing

- A subclass of **social engineering**
- The attempt to obtain sensitive information through electronic communication by disguising as a trustworthy entity.

Common Vectors Include

- Email
- Smishing (SMS)
- Vishing (VOIP)
- Pharming (DNS-Based)
- Host file poisoning (DNS)
- Site Cloning
- Content Manipulation (XSS, SQLi, etc)
- Rogue Access Points
- And much more

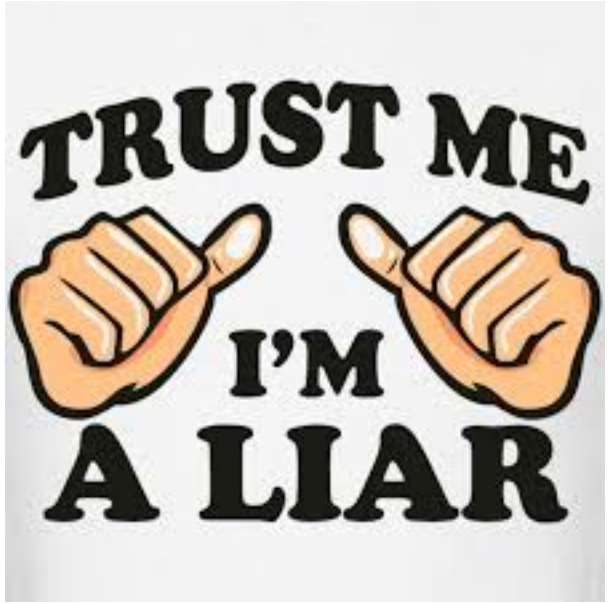
How can you protect against it?

Training

Technical Controls

Generic Legal Disclaimer

- Talk to your **legal department** before starting phishing training
- Make sure you have the right policies in place
- Make sure employee handbook includes security training



Run test from hacker’s position

- Information gathering for pretexting
  - The harvester
  - Maltego
  - LinkedIn
  - Facebook
  - Google dorking
- Different attack types
- Payloads
  - Reverse shells vs link to training site
- Metrics
  - Anonymize data

Hacking Humans

- Exploiting Trust
- Exploiting Greed
- Exploiting Ignorance
- Exploiting the Desire to Help

**** These are common categories in social engineering, I did not invent these.**

Exploiting Trust

- Joke website link email from a coworker
- Survey from the HR department
- Clone phishing email from hacked client/vendor
- Job application with malicious attachment
- Rogue access points
- Site Cloning
- Host file attacks
- RFID Badge cloning

Exploiting Greed

- Surveys for free day of parking
- Mailing user a quirky USB device
- Surveys for free lunch
  - Pretexting a restaurant close to the office
- Leaving USB sticks in the elevator
  - Marked with something enticing
- Benefit change emails from HR

Exploiting Ignorance (not stupidity)

- Posing as IT department
  - asking someone to
    - run commands
    - click on a link
    - install/update a program
  - attacking VOIP can make this dangerous
- New employees are the easiest to exploit
  - Monitor sites like LinkedIn
- Multiple employee attack
  - 1 → 2 → A

Exploiting the Desire to Help

- **Most people want to be productive and help others. This can also be exploited.**

- Pretexting as someone important
- Pretexting as someone needing something for someone important
- Pretending to being a new employee
- Ask a question about a LinkedIn skill from spoofed contact
- Disaster relief donations/videos/articles

Technical Mitigations

- AKA... Why a “people” problem problem may need more than just a “security awareness training” solution.

Technical Mitigations

- IDS rules
- Rogue Access Point Detection
- Behavior Analytics
- Application Whitelisting
- Limited Local Admin
- SSL Proxy
- Network Segregation
- Much, Much, More...

Technical Staff Training

- Train with reverse shells
  - Can analysts catch them?
- Fox hunts
- RFID attack detection. (Brute Force)
- Malicious behavior detection
- Reverse Engineering Malware (Static and Dynamic)
- Tabletop exercises
- etc.

Thanks