fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Federal Information Systems Security Education Association

Spear Phishing

Systegra

Agenda

- Definition of spear phishing
- Why is spear phishing so valuable to attackers
- Spear phishing defenses / countermeasures
- Training concepts and delivery

Spear Phishing, What is it?

- A type of phishing attack
- Uses email messages to trick users to clicking a link, downloading a file, entering data, etc.
- Malware may be downloaded / executed to hijack the user's computer
- May appear to come from a trusted source (e.g., colleague, supervisor, employer, vendor, etc.)
- **More targeted than phishing, not random**
- **Attacker is targeting you and your organization's data**

Spear Phishing, Why?

- Bypasses many network perimeter security controls – targets the human
- Provides access to the user's computer and thereby the organization's internal network and data
- Often made easier with information about users often available online facilitating attack
  - E.g., Social Media

Spear Phishing, Defenses

- System / network IT security controls
  - Spam filters
  - Antivirus
  - Content filtering
  - Digital signatures
- User / personnel training

Spear Phishing, Training

- Training concepts
  - Social media
  - Knowing which emails to trust / validate source
  - Don’t click URL’s, download files from emails
  - Pay attention to grammar, greeting, look and feel of the email – identify suspicious emails
  - Confirm via telephone call, reporting
- Training delivery methods
  - Part of user awareness/onboarding and annual security awareness training (e.g., web based)
  - Exercises online
  - Commercial services to perform testing. Provides user training (e.g., this was a test), and provide metrics

Conclusion

- Spear Phishing is real and has led to numerous compromises
- Commonly used vector, bypasses perimeter defenses, access to internal networks and data

- Training the user is essential !

Questions