June 26, 2024

Coronavirus Social Engineering Attacks: Issues and Recommendations

Presented by:
Joe Alequin, Rashondric Evans, Michael Gonzalez, Brandon McFarlane

Introduction

- **COVID-19** Pandemic
- Cybercriminals taking advantage
- Social Engineering Attacks:
  - **Types:** Physical, Technical, Social, and Socio-Technical
  - **Methods:** Human-based and Computer-based
- Recommendations for both individuals and industry

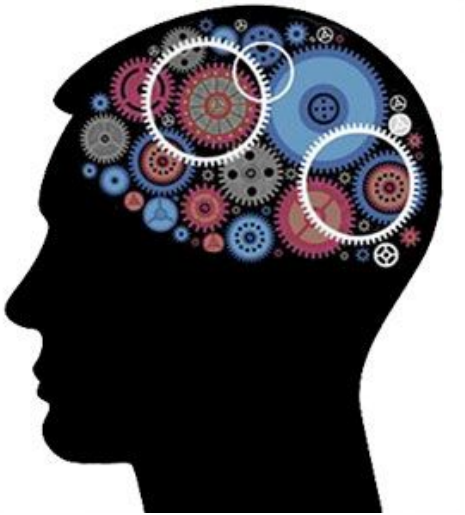
Background

- Social engineering focuses on the manipulation of users
- 33% of actions used during attacks come from social engineering
- Understand factors affecting human behavior
- Key actors at play:
  - Cybercriminal
  - End user (victim)

Background

- Human Security Behavior
  - Careless Attack
  - Comfort Zone Attack
  - Helpful Attack
  - Fear Attack

- Security Awareness Methods
  - Conventional
  - Instructor-Led
  - Online
  - Simulation-Based
  - Game-Based



Evaluation

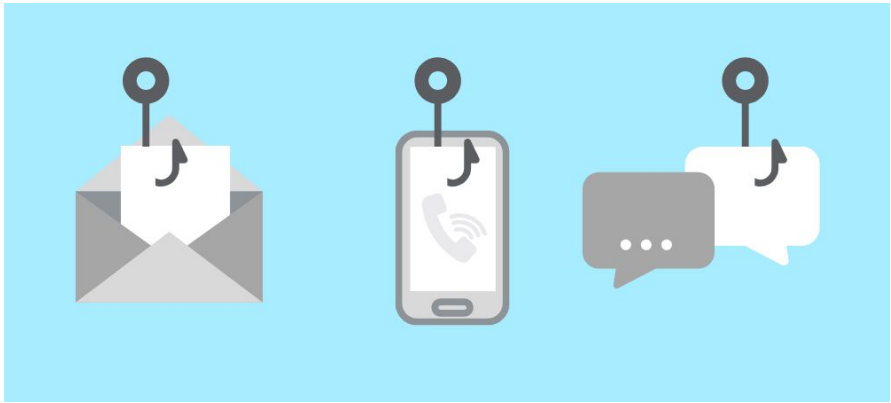
Malicious Attachments & Malware

- Attachments and links via email or social media applications which download malware
- Claim to be from known or familiar source
- Steal personal information (e.g., personal details, banking)
- Coronavirus Map

Evaluation

Key Terms & Concepts

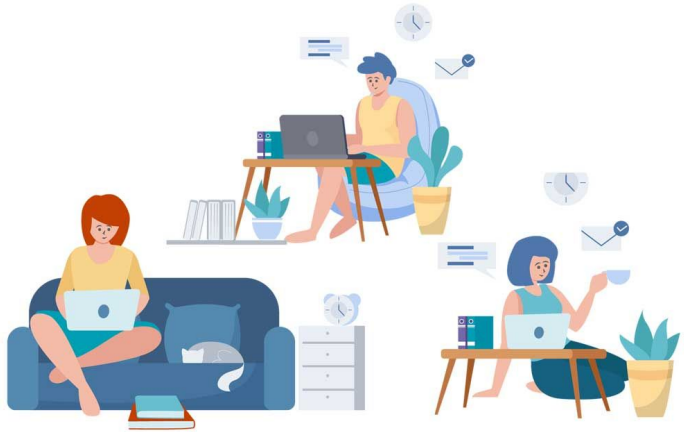
- Social Engineering
- Spear Phishing
- SMS Phishing (Smishing)
- Voice phishing (Vishing)
- Remote Work



Evaluation

Remote Work

- Staff under pressure and working remotely
- Stealing credentials to gain access to network (VPN)
- Deployment of ransomware



Proposed Solutions

Technical Recommendations

- SPAM and phishing filters
- Make sure of anti-virus software (i.e., endpoint security)
- Disable macros by default on Microsoft Office documents
- Configure screen locks for when devices are left unattended
- Install patches/updates
- Enforce MFA, especially for remote connections
- Encrypt sensitive data at rest and in transit, including Wi-Fi connections
- Disable the use of removable media
- Perform regular backups

Proposed Solutions

Security Awareness

- Educate staff about social engineering tactics
- Provide ongoing training
  - Security awareness is not a “one-time” task
- Provide clear guidelines of what is “acceptable behavior”

Proposed Solutions

Detection of “Red Flags”

- Authority (CEO, bank, government)
- Urgency (respond immediately)
- Emotion (fear, hope, etc.)
- Scarcity (limited quantity)
- Current Events (tax refunds, disasters, etc.)

Questions

Thank you