Cybersecurity Awareness

Social Engineering
What is Social Engineering?

- The art of exploiting human psychology and behaviors to manipulate people into performing actions or divulging confidential information.
Social Engineering Principles

- Authority
- Intimidation
- Consensus
- Scarcity
- Urgency
- Familiarity
- Trust
Social Engineering Process

Targeted

- Attacker gathers information about the subject
- Attacker plans the attack (may be from multiple vectors)
- Acquires tools and resources
- Initiates the attack
- Uses acquired knowledge

Blanketed

- Attacker creates an attack
- Attacker sends it to as many people as possible
- Attacker waits for someone to take the bait
Social Engineering Attack Vectors

- Open-Source Intelligence Gathering (OSINT)
- Baiting
- Pretexting
- Phishing
  - Spear Phishing
  - Whaling
- Vishing and Smishing
Open-source Intelligence (OSINT)

• Gathering “publicly” available information
• Often used in the planning stages of a targeted attack
• Sources of information
  • Public records (census data, home sales)
  • Social Media
  • News articles/Publications
  • Casual Observation
  • Public Events/Meetings
Protecting Yourself From OSINT

• Be mindful of what information you share
• Keep social media accounts private
• Contact your government representative about Data Protection Laws
  • GDRP

DATA PRIVACY IN THE US

- States with passed data privacy legislation
- Proposed and pending legislation
- Postponed data privacy legislation
- No proposed legislation as of 2020
- Failed data privacy legislation
Baiting

• Luring the victim with an attractive offer or playing on fear, greed, or obligation
• Baiting can be a virtual (digital) or physical attack
• Often used to install malware on victims' devices
• Common baiting techniques
  • Free downloads
  • Device drops (USB Drives)
Pretexting

• Attacker creates a plausible scenario or story to get the victim to divulge information
• Can take place via e-mail, text, phone calls, and in person
• Attacker often impersonates a person you know or should trust
• Examples:
  • An innocent looking e-mail asking for a simple response
  • Unfamiliar Co-worker or boss calling asking for help
  • A person asking you to take a survey or sign a petition
Phishing

• A fraudulent “spoofed” message designed to trick you
  • Revealing information (username/password)
  • Clicking a link
  • Downloading an attachment
• Often sophisticated
  • Use company logos and images
  • May contain personal information
  • Links may take you to a cloned site
Spear Phishing and Whaling

- Phishing attacks that are targeted
  - Specific Organization
  - Specific Person
  - High-level executive (Whaling)
- Target is well researched
- Harder to detect
Common Phishing Tactics

- Suspicious activity or log-in attempts
- Claim there’s a problem with your account or your payment information
- Say you must confirm some personal information
- Include a fake invoice
- Want you to click on a link to make a payment
- Say you’re eligible to register for a government refund
- Offer a coupon for free stuff
Ways to Spot a Phishing E-mail

- Bad grammar or spelling mistakes
- Unfamiliar or incorrect greeting
- Inconsistencies in e-mail address, links, or domain names
- Suspicious attachments
- Requesting sensitive information
  - Login credentials
  - Payment information
- Too good to be true
- Creates a sense of urgency or fear
SMishing and Vishing

Variants of Phishing using Text Messages and Voice Calls

Protect yourself

- Don’t click links in unknown text messages
- Don’t share sensitive information over the phone
- Call back a verified phone number
- Use call/text blocking tools from your provider