Social Engineering: The Manipulated Insider

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Dr. Emeka Ejikeme and Mr. Ronald Brandon

Introduction and Overview

- Introduction to the Presenters
- DITMAC BTAC SME's Domains and Responsibilities
- Existing BTAC Support
- What is Social Engineering (SE)?
- Social Engineering and Insider Threat
- Social Engineering Statistics
- Four phases of a social engineering attack
- Remediation/mitigation
- Summary

Domains and Responsibilities

DoD Directive 5205.16 (2014) mandates the establishment and maintenance of a "multidisciplinary threat management capability" across DoD components

DITMAC SMEs provide an enterprise-level resource to support C-InT programs

- **DITMAC BTAC currently has SMEs in the domains of**:
  - Behavioral Science
  - Law Enforcement & Counterintelligence
  - Threat Assessment & Threat Management
  - Employee Relations
  - Cyber Threat

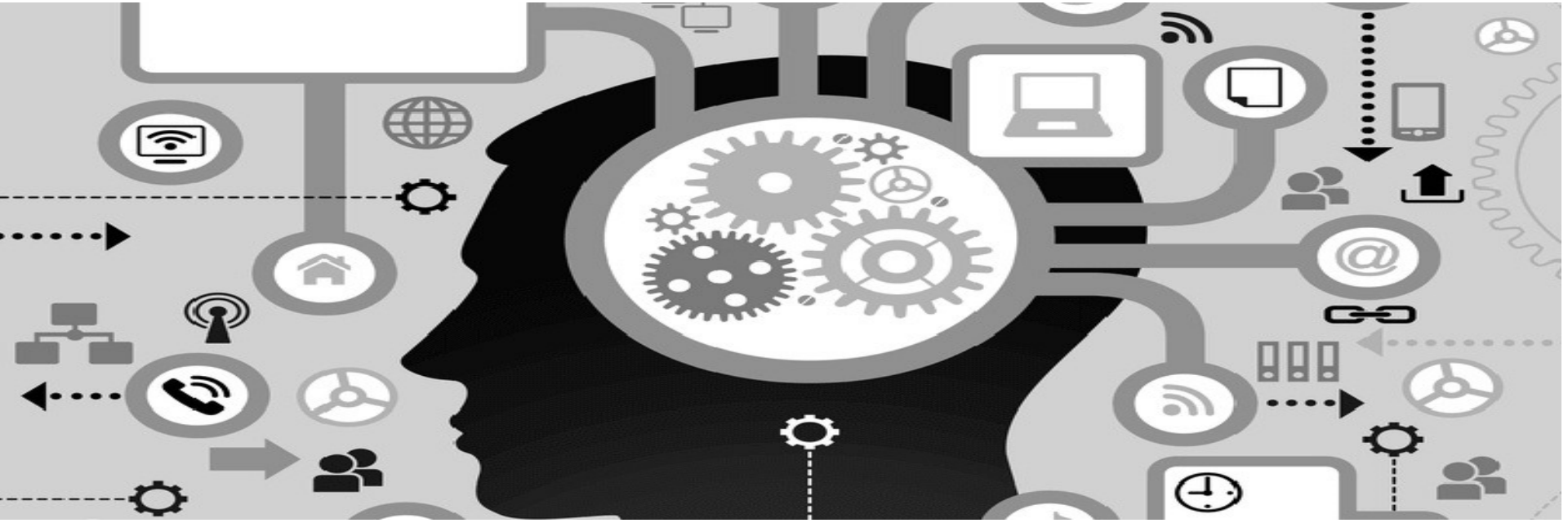
- **SME Primary Responsibilities**:
  - Provide InT consultation to DoD Senior Leadership in response to priority requests and special topics of concern
  - Promote collaboration, information sharing, and development of best practices among DoD component hubs and InT SMEs
  - Review and provide SME consultation to DITMAC InT cases in support of analysis and mitigation
  - Develop training to further professionalize DoD InT community
  - Inform InT research efforts in partnership with OUSD (I&S), the Threat Lab, and DITMAC Office of Performance Standards & Metrics

Existing BTAC Support

- Provide SME consultations on insider threat cases reported to the DITMAC to holistically assess risk and recommend viable mitigation actions to DoD Component Insider Threat Programs;
- Provide direct SME support to the DITMAC Prevention, Assistance, and Response (PAR) Coordinators and Commanders at DoD Joint Bases in the form of tailored risk assessments, comprehensive mitigation recommendations, and training on behaviors and indicators of potential insider threats;
- Develop and conduct training for the DoD Insider Threat Enterprise on past, current, and emerging indicators/trends to mature and professionalize the DoD insider threat workforce; and
- Conduct research and produce awareness products on special topics impacting the DoD insider threat mission

What is Social Engineering (SE)?

Social engineering is a form of manipulation that individuals or groups use to deceive or manipulate others into divulging confidential or personal information that may be used for fraudulent purposes.



Social Engineering and Insider Threats

Social engineering insider threats involve individuals within an organization who, intentionally or unintentionally, succumb to social engineering techniques designed to compromise security, gain unauthorized access, or attempts to harm the organization.

Common Social Engineering Techniques

- Phishing
- Vishing
- Smishing
- Reverse Social Engineering
- Quid Pro Quo
- Impersonation
- Tailgating
- Whaling
- Dumpster Diving
- Scareware
- Baiting
- Pretexting

Social Engineering Statistics

There are more than 4.5 billion people interconnected via social media

"The Human Element" is the weakest link in the cyberattack kill chain

- 98% of cyberattacks rely on Social Engineering techniques
- Avg. Business: Over 700 Social Engineering attacks each year
- 90% of data breaches target humans
- 83% fall prey to phishing attacks
- 95% of attacks rely on spear phishing techniques
- Only 50% of employees can define this term correctly
- Avg. Cost to Recover: ~ $130,000

Social Engineering Statistics - Continued

- 86% of Org's: At Least One Person Has Clicked a Phishing Link
- Just 56% of Companies Provide Security Awareness Training
- Social Media Attacks Rise: 74% of Org's Targeted in 2021
- Amazon is the Most Impersonated in Emails
- Facebook: Most Impersonated Website w/ 18% of Phishing URLs
- Men Are 225% More Likely to Fall for Phishing Attacks

The Lifecycle of a Social Engineering Attack

Four Stages:

1) Investigation
2) Hook
3) Play
4) Exit

Cybersecurity Awareness Helps

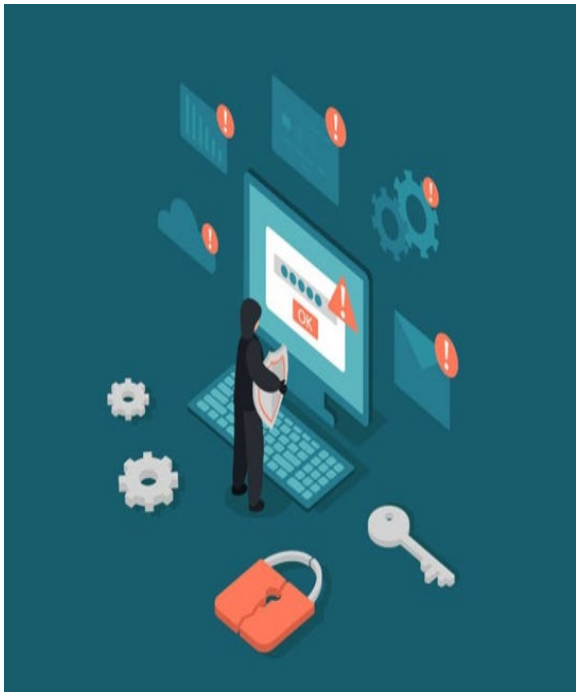
- The Importance of Cybersecurity Awareness

- Ways to Improve Cybersecurity Culture:
  1. Ensure Senior Management promotes cybersecurity
  2. Implement robust cybersecurity policies and procedures
  3. Make cybersecurity training a part of the onboarding process
  4. Conduct regular cybersecurity training and exercises/drills
  5. Ensure training is targeted and easy to consume and engaging

Basic Social Engineering Defenses

- Regularly update and patch software
- Use multi-factor authentication (MFA)
- Foster a culture of security awareness
- Use a spam filter to block phishing emails
- Don't share PII, $, or system access info
- Verify the individual first
- Use strong, unique passwords
- Suspect unexpected contacts

Basic Social Engineering Defenses - Continued



- Verify Sender's Identity
- Avoid Using Public Wi-Fi Networks - Use a VPN
- Suspect Pop-Ups
- Scan Your System
- Don't Click Links From Unfamiliar Sites
  - Beware of S.L.A.M. (Sender, Link, Attachment, and Message)

Advanced Social Engineering Defenses

- Build a positive security culture
- Implement a Multi-Person Authorization Policy
- Counter the attack by using a probe question or a “proof” statement
- Detect Behavioral Inconsistencies in a “Syn-Puppet” Operation

Examples of Real Social Engineering Attacks

CEO Fraud Scam

Chinese plane parts manufacturer FACC lost nearly $60 million in a so-called “CEO fraud scam” where scammers impersonated high-level executives and tricked employees into transferring funds. After the incident, FACC then spent more money trying to sue its CEO and finance chief, alleging that they had failed to implement adequate internal security controls.

Examples of Real Social Engineering Attacks

Microsoft 365 Phishing Scam Steals User Credentials

In April 2021, security researchers discovered a Business Email Compromise (BEC) scam that tricks the recipient into installing malicious code on their device. The target receives a blank email with a subject line about a “price revision.” The email contains an attachment that looks like an Excel spreadsheet file (.xlsx). However, the “spreadsheet” is most likely a .html file in disguise. Upon opening the (disguised) .html file, the target is directed to a website containing malicious code. The code triggers a pop-up notification, telling the user they’ve been logged out of Microsoft 365 and inviting them to re-enter their login credentials.

Examples of Real Social Engineering Attacks

Ransomware Gang Hijacks Victim's Email

In April 2021, several employees of U.K. rail operator Merseyrail received an unusual email from their boss's email account with the subject line "Lockbit Ransomware Attack and Data Theft."

The email sent by a fraudster impersonating Merseyrail's director revealed that the company had been hacked and had tried to downplay the incident. The email also included an image of a Merseyrail employee's personal data.

The "Lockbit" gang not only exfiltrated Merseyrail's personal data and demanded a ransom to release it—the scammers used their access to the company's systems to launch an embarrassing publicity campaign on behalf of its director.

Examples of Real Social Engineering Attacks

US Department of Labor Attack

In January 2022, "Bleeping Computer" described a sophisticated attack designed to steal Office 365 credentials in which the attackers imitated the US Department of Labor (DoL). The scam is a noteworthy example of how convincing these attacks have become.

The attack used two methods to impersonate the DoL's email address—spoofing the actual DoL email domain (**reply@dol[.]gov**) and buying look-a-like domains, including "**dol-gov[.]com**" and "**dol-gov[.]us**." Using these domains, the attack emails passed through the target organizations' security gateways.

Examples of Real Social Engineering Attacks

Example continued

On clicking the link, targets were redirected to a phishing site that looked identical to the actual DoL site, hosted at a URL such as bid-dolgov[.]us. The fake bidding site instructed users to enter their Office 365 credentials. The site even displayed an “error” message after the first input, ensuring the target would enter their credentials twice and thus reducing the possibility of mis-typed credentials.

Examples of Real Social Engineering Attacks

Russian Hacking Group Targets Ukraine

As world leaders debated the best response to the increasingly tense situation between Russia and Ukraine, Microsoft warned in Feb 2022 of a new social engineering attack campaign by a Russian hacking group targeting Ukrainian government agencies and NGOs. This group targeted “organizations critical to emergency response and ensuring the security of Ukrainian territory” since 2021. The initial phase of their attack relied on sending emails containing malware. The emails also contained a tracking pixel that informed the cybercriminals whether it had been opened.

Questions & Answers

- While at Starbucks, you are approached by a person that asks about your job and where you work. They ask what type of clearance do you have. What do you do?

- What should you do if a co-worker from the past contacts you and wants your address and phone number via email, Facebook, or X?

- Who do you contact if you accidently click on a suspicious link while trying to delete it?

- How can you validate if you receive an email requesting your recall data (e.g., home phone, address, cell)? The email was sent from your 'HR department.'

Summary

- Social engineering attacks can have serious consequences
- Do not click on any links
- IF there's an incident, report it

Protect One Another. Help is Out There.

- BTAC Team of SME's can help answer your questions
- Reporting cybercrimes:
  - Call the nearest FBI Field Office
  - Online: **Tips.fbi.gov**
  - Online: **IC3.gov**

- Other Resources and contacts:
  - Local/Regional ISSO/ISSM
  - SSO Office/FSO
  - Enterprise Helpdesk
  - Cybersecurity POC
  - OPSEC and Cyber Awareness Training

Contact Information

Thank You

DITMAC-BTAC Cyber Threat SME Team

Dr. Emeka Ejikeme emeka.v.ejikeme.ctr@mail.mil
Ronald Brandon ronald.m.brandon.ctr@mail.mil

Social Engineering Resources:

https://www.splunk.com/en_us/blog/learn/social-engineering-attacks.html
https://www.tessian.com/blog/examples-of-social-engineering-attacks/
https://www.youtube.com/watch?v=gSH2jkEPXSc&feature=youtu.be
https://firewalltimes.com/social-engineering-statistics/
https://www.stationx.net/social-media-hacking-statistics/
https://tips.fbi.gov/home
https://www.ic3.gov/
https://www.dcita.edu/
https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
https://dodcio.defense.gov/Portals/0/Documents/Library/CSResourceReferenceGuide.pdf
https://www.defense.gov/social-media-policy/
https://www.army.mil/socialmedia/personal/
https://internetsafety101.org/Respondingtocyberbullying