Social Engineering

May 18, 2016

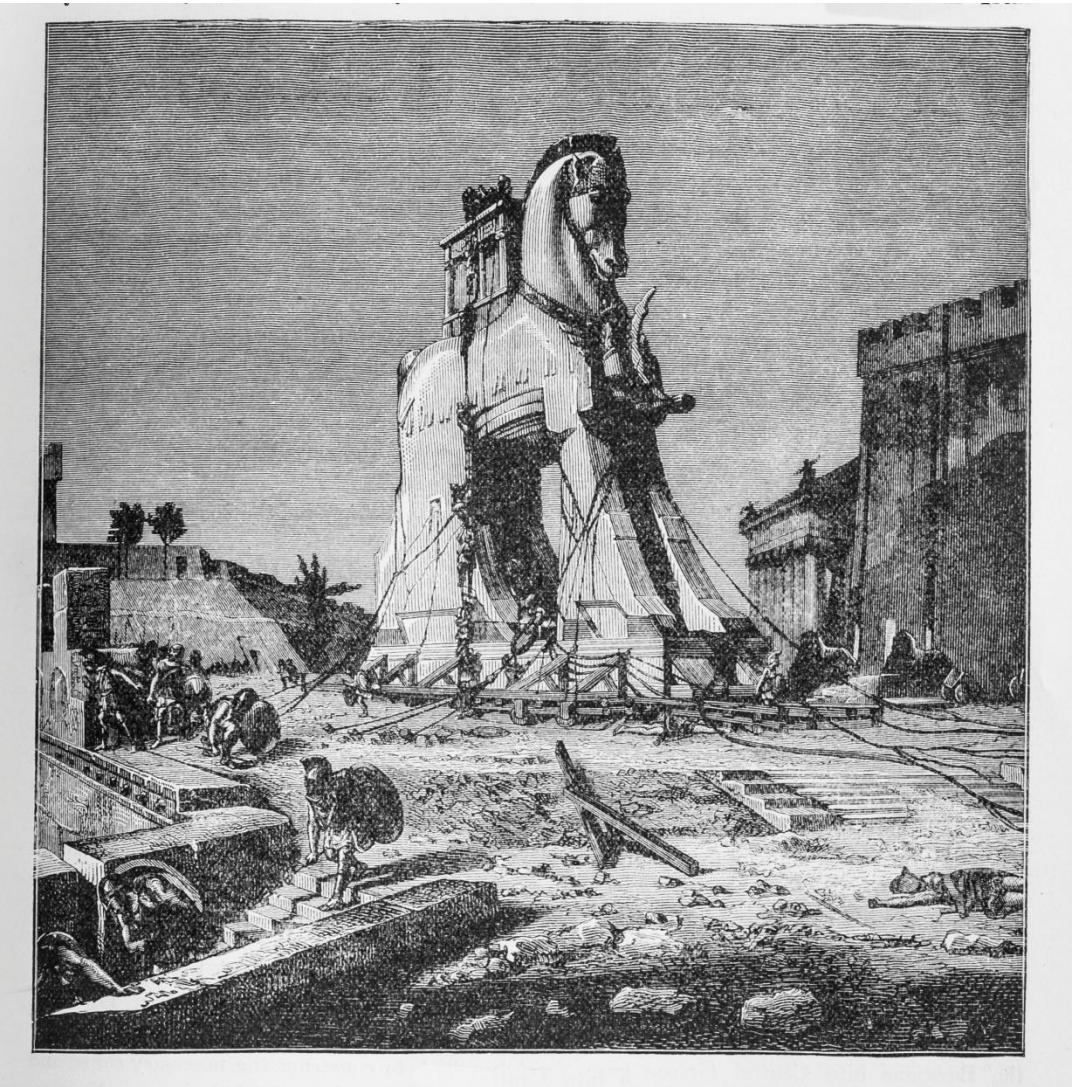
SERVE | ADD VALUE | INNOVATE

Social Engineering: Definition

Social Engineering or "human hacking" is most commonly defined as the psychological manipulation of people into performing actions or divulging confidential information.

Social Engineering has been around a long time.

What is the most famous historical social engineering attack of all time?



Types of Social Engineering Attacks

1. Pretexting
2. Baiting
3. Quid Pro Quo
4. Tailgating
5. Diversion Theft
6. Ransomware
7. Dumpster Diving
8. Phishing

Types of Social Engineering Attacks

1. **Pretexting** is a form of social engineering where attackers focus on creating a convincing fabricated scenario using email or phone to steal their personal.
2. **Baiting** is similar to phishing, except it uses – click on this link for free stuff.
3. **Quid Pro Quo** is like baiting. The difference is baiting offers a good, this offers a service.

Types of Social Engineering Attacks

4. **Tailgating** is when someone who lacks proper security clearance following someone who does into a building or area.
5. **Diversion theft** involves misdirecting a courier or transport company and arranging for a package or delivery to be taken to another location.
6. **Ransomware** is a type of malware that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction.
7. **Dumpster Diving** is collecting information from discarded materials such as old computer equipment (e.g., hard drives, thumb drives, DVDs, CDs) and company documents that were not disposed of securely.

Types of Social Engineering Attacks

8. Phishing
   a) Spear phishing
   b) Whaling
   c) IVR phishing
   d) Business Email Compromise (BEC)

Types of Social Engineering Attacks

8. Phishing

- Most common social engineering attack
- Using email or phone to obtain personal or corporate information
- Seek to obtain names, addresses, emails, ss#, passwords, etc.
- Get employee to type or tell them info
- Either download or click on link to bring malware into computer and system
- Random or mass accounts

Types of Social Engineering Attacks

8. Phishing

a) **Spearphishing** – phishing which targets an individual or select group

b) **Whaling** – spearphishing where the target is a big fish (C-Suite)

c) **IVR Phishing** – uses IVR system (obstensibly from bank or legitimate business) to get individual to enter confidential information

d) **Business email Compromised (BEC)** – mutation of whaling where the scan is researched, funded and con is patient

Types of Social Engineering Attacks

Business Email Compromised (BEC)

The Set-up: Research the company

- GAIN ACCESS TO CORPORATE EMAIL
- ACCESS CALENDAR OF C-SUITE EXECS
- REVIEW CORPORATE WEB PAGES FOR CONTACTS
- MIMICS LANGUAGE OF PAST EMAILS
- READ PROFESSIONAL WRITINGS TO UNDERSTAND CORPORATE CULTURE
- PERTAINS TO GOOD, SERVICES & VENDORS COMPANY USUALLY USES
- CORRECT PAYMENT SCHEDULE
- CC SOMEONE IN ACCOUNTING (SLIGHT ERROR)

Phishing | Spear phishing | Whaling | IVR Phishing | BEC

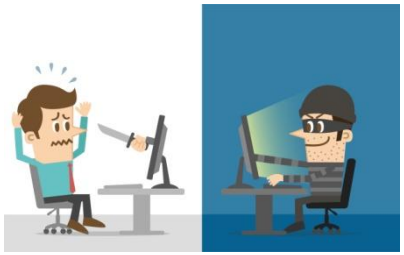
Types of Social Engineering Attacks

Business Email Compromised (BEC)

The Set-up: Research the target

- TROLL SOCIAL MEDIA SITES OF THE TARGET EMPLOYEE
- READ PROFESSIONAL WRITINGS TO UNDERSTAND TARGET
- ACCESS CALENDAR OF TARGET
- AMOUNT OF MONEY REQUESTED RESEARCHED - WITHIN RANGE OF MARK'S AUTHORIZATION

Types of Social Engineering Attacks



Business Email Compromised (BEC)

The Wire: How do hackers gain access?

- GET EMPLOYEE TO CLICK ON EMAIL ATTACHMENT OR LINK THAT COMPROMISES NETWORK (MALWARE)
- SPOOFING EMAIL OF HIGH-RANKING OFFICIAL IN THE COMPANY
- RESEARCH COMPANY AND TARGET TO CRAFT HIGHLY CONVINCING EMAIL
- MINES CORPORATE WEBPAGES AND SOCIAL NETWORKS TO CREATE EMAILS AND WEBSITES THAT ARE HIGLY CONVINCING.

Phishing → Spear phishing → Whaling → IVR Phishing → BEC

Types of Social Engineering Attacks

Business Email Compromised (BEC)

The Hook: Using trust, urgency and social engineering

- USING EXECUTIVE'S CALENDAR- SEND EMAIL WHEN OUT OF OFFICE
- COMPROMISES TARGET'S EMAIL AS WELL AS SOMEONE IN ACCOUNTING
- AMOUNT OF MONEY REQUESTED RESEARCHED - WITHIN RANGE
- LANGUAGE MIMICS PAST EMAILS
- CORRECT PAYMENT SCHEDULE
- CC SOMEONE IN ACCOUNTING (SLIGHT ERROR)
- INSERT A SENSE OF URGENCY TO GET TARGET TO ACT QUICKLY.
- EMAIL LOOKS OFFICIAL
- FROM HIGH CORPORATE OFFICER
- ATTACHMENT ON COMPANY LETTERHEAD

Phishing | Spear phishing | Whaling | IVR Phishing | BEC

Types of Social Engineering Attacks

Business Email Compromised (BEC)

The Sting

- GOAL
  - CASH
  - DIRECTS TRANSFER OF FUNDS TO A PARTICULAR PERSON AT AN OVERSEAS BANKS
  - CLOSE ACCOUNT PROMPTLY
  - CONFIDENTIAL INFORMATION

Phishing | Spear phishing | Whaling | IVR Phishing | BEC

Types of Social Engineering Attacks

Business Email Compromised (BEC)

Prevention

- Specify and train personnel when/where/why/how sensitive information should be handled)
- Identify which information is sensitive and evaluate its exposure to social engineering and breakdowns in security systems (building, computer system, etc.)
- Establish security protocols, policies, and procedures for handling sensitive information.
- Train employees in security protocols relevant to their position. (e.g., in situations such as tailgating, if a person's identity cannot be verified, then employees must be trained to politely refuse.)
- Perform unannounced, periodic tests of the security framework.
- Using a waste management service that has dumpsters with locks on them, with keys to them limited only to the waste management company and the cleaning staff. Locating the dumpster either in view of employees such that trying to access it carries a risk of being seen or caught or behind a locked gate or fence where the person must trespass before they can attempt to access the dumpster.
- Never provide confidential information or, for that matter, even non-confidential data and credentials via email, chat messenger, phone or in person to unknown or suspicious sources.

Types of Social Engineering Attacks

Business Email Compromised (BEC)

Prevention

– Hopefully this will result in:

Phishing → Spear phishing → Whaling → IVR Phishing → BEC

Types of Social Engineering Attacks

Phishing | Spear phishing | Whaling | IVR Phishing | BEC

www.verisk.com/iso