Social Engineering

Martin Stanek

2024

Table of Contents

Introduction, various types of SE attacks

Psychology of social engineering

Prevention and testing

Social engineering – definitions

The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.
NIST SP 800-63-3 (Digital Identity Guidelines)

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
Imperva, ENISA (Threat Landscape 2022 report)

Social engineering – definitions

Attack patterns within this category focus on the manipulation and exploitation of people. The techniques defined by each pattern are used to convince a target into performing actions or divulging confidential information that benefit the adversary, often resulting in access to computer systems or facilities.
MITRE (Common Attack Pattern Enumerations and Classifications, Category 403)

- Attacks rely on human element to succeed
- Common initial vector in attacks

Main attack vectors

The European Union Agency for Cybersecurity (ENISA) – Threat Landscape 2023 report:

Social engineering remains a preferred attack vector for threat actors due to its simplicity, low cost, ease of execution...

1. Phishing – deceiving people using various communication channels
2. Spear-phishing – phishing targeted at individual or organization
3. Whaling – phishing aimed at high position users
4. Smishing – phishing using SMS
5. Vishing – phone calls
6. Business e-mail compromise (BEC) – gaining access to e-mail account
7. Fraud – intentional misrepresentation of an important fact
8. Impersonation – pretending the identity of other entity
9. Counterfeit – fraudulent imitation of something

Other attack vectors (1)

- Baiting – appealing to greed or curiosity
  - file named *Salaries.docx*, USB stick in the lobby
  - free stuff or discounts promised on URL link
- Pretexting – fabricated story to gain trust and manipulate the victim
  - IT support performing a maintenance task
  - romance scams, fake charities
  - pretexting – important part of BEC
- Dumpster diving
  - gathering sensitive documents from trash, discarded computers

Other attack vectors (2)

- Tailgating (piggybacking) – following an authorized person
  - access to restricted area
  - pretexts – forgotten ID, package delivery
- Blackmail – threat to reveal something embarrassing or incriminating
  - example: fake sextortion blackmail

Phishing

- phishing – the most common form of cyber crime
- 2023 was the worst year for phishing
  - APWG: Phishing Activity Trends Report, 4th Quarter 2023
- various forms: spear-phishing, whaling, vishing, BEC
- often sales tactics (based on social psychology) employed: urgency and scarcity
- combined with pretexting
- suspicious links, e-mail address
- suspicious content – request for credentials, payment information, etc.
- foreign language advantage – not anymore
- approx. 10% of people will click on phishing links
  - 2023 Gone Phishing Tournament (Terranova Security)

Spear-phishing

- phishing targeted at individual or organization
- research the target
  - social media – personal information, contacts
  - OSINT
- usually avoid technical controls for spam/phishing detection
- high success rate

Business e-mail compromise (BEC)

- BEC is evolving
- beginning:
  - hacking or spoofing of business and personal email accounts
  - request to send wire payments to fraudulent bank accounts
- a more modern approach:
  - hacking CEO or CFO e-mail
  - requesting virtual meeting participation
  - still picture with no audio or deep fake audio (“not working properly”)
  - instructing employees to initiate wire transfer (or using compromised e-mail)
  - money transferred to cryptocurrency wallets and dispersed

FBI's Internet crime report 2023

- FBI IC3 – Internet Crime Complaint Center
- BEC: 7th according the victim count, 2nd in losses
- various statistics of reported crime complaints
  - number of victims, financial losses reported
  - age groups
  - geography: US states, countries
  - trends
- ransomware financial losses *relatively* low
  - excluded estimates of lost business, time, wages, files, equipment, etc.
  - no losses reported in some cases
  - only losses reported to IC3

Complaint count and loss statistics from the FBI's report

By Complaint Count	
Crime Type	*Complaints*
Phishing/Spoofing	298,878
Personal Data Breach	55,851
Non-payment/Non-Delivery	50,523
Extortion	48,223
Investment	39,570
Tech Support	37,560
BEC	21,489
Identity Theft	19,778
Confidence/Romance	17,823
Employment	15,443
Government Impersonation	14,190
Credit Card/Check Fraud	13,718
Harassment/Stalking	9,587
Real Estate	9,521

By Complaint Loss	
Crime Type	*Loss*
Investment	$4,570,275,683
BEC	$2,946,830,270
Tech Support	$924,512,658
Personal Data Breach	$744,219,879
Confidence/Romance	$652,544,805
Data Breach	$534,397,222
Government Impersonation	$394,050,518
Non-payment/Non-Delivery	$309,648,416
Other	$240,053,059
Credit Card/Check Fraud	$173,627,614
Real Estate	$145,243,348
Advanced Fee	$134,516,577
Identity Theft	$126,203,809
Lottery/Sweepstakes/Inheritance	$94,502,836

Psychology of social engineering (6 principles)

R. Cialdini, *Influence: Science and Practice*

1. Reciprocity – return the favor (e.g. a gift)
2. Scarcity – limited supply increases a perceived value (e.g. limited time)
3. Authority – obeying authority even if the given instructions are questionable (e.g. Milgram experiment, CEO's e-mail)
4. Commitment and Consistency – people honor their commitment/agreement (e.g. asking for something small first and more later); age positively correlated with consistency
5. Liking – proposal is more persuasive if originates from someone we known or like (e.g. phishing from compromised accounts); liking people like us
6. Consensus / Social Proof – (if uncertain) do as other people do (e.g. charity when natural disaster occurs)

Why social engineering works

- empathy
- social contract (expected behavior)
- conflict aversion
- politeness
- trusting by default
- greed
- curiosity
- fear ...

OSINT and SE

- OSINT tools and methods in SE tasks
  - help build the pretexts
  - identify the most efficient way to perform the SE
  - prepare for the task
- DEFCON Vishing Competition
  - two parts: OSINT phase and live Vishing phase
  - objectives defined for both parts
  - coaching for participants
  - Code of Ethics

DEFCON social engineering competition (2022)

Chris Kirsch report

- OSINT part (several weeks)
  - 25 pieces of information (“objectives”)
  - proving the gathered information is no older than 2019
  - written OSINT report
  - Vishing report (who do they want to call and pretexts)
    - flag any unethical (e.g. based on fear) or illegal pretexts
    - the most frequent planned pretexts: IT/security audit, IT helpdesk reaching out, IT/security survey
- Vishing (live) – the most frequent used pretexts:
  - IT helpdesk reaching out, IT/security survey, Software satisfaction survey
- observations (see the web page)

Prevention and testing

- user training and awareness
- required by every sufficiently comprehensive standard and framework
- Security and Privacy Controls for Information Systems and Organizations
  - NIST Special Publication 800-53r5 (2020)
  - AT-2(1): Provide practical exercises in literacy training that simulate events and incidents.

    Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.
- people will always click, be helpful, etc.
- the goal
  - reduce the frequency
  - prevent the most obvious attacks
  - train people what to do when they notice a suspicious e-mail, event

Tools for practical exercises and testing

- SET (Social-Engineer Toolkit)
  - various attack types: Web Attack, Mass Mailer Attack, Phishing Attacks
  - ability to create payload and listener
  - can be performed by separate tools (e.g. MSF)
- Gophish – a platform for phishing campaigns
  - e-mail templates (with attachments, tracking images)
  - landing pages
  - users and groups
  - reporting: e-mail opened, link clicked, data submitted, etc.

Tools (cont.)

- many security vendors offer awareness training and phishing simulations
- Maltego, Spiderfoot, Recon-ng and others – OSINT part of SE testing
- Wifiphisher – a rogue Access Point framework
  - MITM attack on victim's WiFi connection
  - Evil Twin – fake Wireless network (similar to the real one)
  - Known Bacon – broadcasting common ESSIDs (devices likely connected in the past)
  - forging *Deauthenticate* or *Disassociate* packets etc.

Some technical controls

- useful but limited
- MFA (multifactor authentication)
- fully patched systems
- verifying DMARC, DKIM and SPF
- endpoint antimalware, EDR (Endpoint Detection and Response)
- e-mail scanning, evaluating links and attachments, sandboxing

Exercises

1. Prepare the best phishing e-mail for employees of “Bear Bank” or “Bear University”. The e-mail will contain a link that leads to
   `https://secure.eicar.org/eicar.com.txt`
   Your goal is to achieve the highest click rate. Justify your approach.
2. Prepare the best spear-phishing e-mail for the lecturer. Do not you use mail that pretends to be a submission of any homework/project. The goal is to get the click on the link. Justify your approach.

Resources

1. ENISA, *Threat Landscape 2023 report*, 2023
2. C. Hadnagy, *Social Engineering: The Science of Human Hacking*, Wiley, 2018
3. R. Heartfield, G. Loukas, *A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks*, Article No. 37, ACM Computing Surveys, 2015
4. F. Salahdine, N. Kaabouch, *Social Engineering Attacks: A Survey*, Future Internet 2019, 11(4), 89, 2019