

Social Engineering

Martin Stanek

2026

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 encompasses a broad range of activities intended to exploit human error or human behaviour with the objective of gaining access to information or services. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information.

ENISA (Threat Landscape 2024 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 2025 report:
social engineering tactics remain the primary entry point for threat actors, with phishing accounting for about 60% of observed cases

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

- 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
- 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
- APWG: [Phishing Activity Trends Report, 4th Quarter 2025](#)
- 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)
- other sources:
 - approx. 17% for general phishing, more than 50% for targeted spear-phishing

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 2025

- FBI IC3 – [Internet Crime Complaint Center](#)
- BEC: 9th according the victim count, 2nd in losses – [report](#)
- various statistics of reported crime complaints
 - number of victims, financial losses reported
 - age groups, US states
 - 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
- look at (1) some recent IC3 alerts, (2) AI assisted crimes in the report

Complaint count and loss statistics from the FBI's report (top 12)

By Complaint Count		By Complaint Loss	
Crime Type	Complaints	Crime Type	Loss
Phishing/Spoofing	191,561	Investment	\$8,648,617,756
Extortion	89,129	Business Email Compromise	\$3,046,598,558
Investment	72,984	Tech/Customer Support	\$2,134,675,818
Personal Data Breach	67,456	Personal Data Breach	\$1,314,923,988
Non-Payment/ Non-Delivery	56,478	Confidence/Romance	\$929,287,469
Tech/Customer Support	47,794	Government Impersonation	\$797,943,193
Government Impersonation	32,424	Other	\$512,146,819
Identity Theft	31,675	Non-Payment/ Non-Delivery	\$503,373,587
Business Email Compromise	24,768	Data Breach	\$435,240,992
Employment	24,688	Employment	\$362,934,762
Confidence/Romance	23,159	Credit Card/Check Fraud	\$282,670,235
Harassment/Stalking	21,557	Real Estate	\$275,110,419

Psychology of social engineering (6 principles)

R. Cialdini, *Influence: Science and Practice*

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

Why social engineering works

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

- 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

- DEFCON 2022
 - Chris Kirsch [report](#) (2022)
 - OSINT part (several weeks)
 - 25 pieces of information (“objectives”); proving the gathered information is no older than 2019
 - 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)
- DEFCON 2025 ([info](#) from the winning team)
 - Battle of the Bots: Vishing Edition
 - AI-powered agents, live voice phishing calls in real-time

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.

1. ENISA, *Threat Landscape 2025 report*, 2025
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