Co-funded by the Erasmus+ Programme of the European Union

Module de instruire InCyT

Securitatea informațiilor pentru angajați **Unitatea 4 Săptămâna 7** **Numele unității: Inginerie sociala**	
Activități de învățare	❑ **Webinar** ❑ **Exerciții** ❑ **Workshop** ❑ **Prezentare** ❑ **Alte** Streaming Webinar, Text, Exerciții de autoevaluare, Exerciții cu răspunsuri pe forumurile de discuții și în cadrul sesiunilor organizate cu trainer/mentor, e-portfolii
Responsabil de învățare	• David Sommer • Ileana Hamburg
Obiectivele activității de învățare	1. Tehnici de atac de inginerie socială 2. Importanța instruirii în inginerie socială 3. Cum să vă protejați de atacurile de phishing 4. Ingineria socială dintr-o perspectivă interdisciplinară
Abilități de dobândit	• Securitatea rețelei TS3 • Testarea TS4 Penetration (vulnerabile exploatabile). • SS3 Analiza cognitivă și comportamentală
Durata activității de învățare	2 săptămâni
Cerințe de învățare	***Ce e necesar?***
	• Acces la internet • Motor de cautare • MS Office365

Co-funded by the
Erasmus+ Programme
of the European Union

Informații scurte despre modul

Descriere
Ingineria socială este o amenințare importantă și foarte adesea la adresa securității informațiilor. Acest modul explică pe scurt Ciclul de viață al ingineriei sociale, cum are loc și cum poate fi prevenit un atac. În special phishing-ul este descris ca fiind unul dintre cele mai populare atacuri de inginerie socială. Multe companii folosesc soluții tehnice pentru a preveni atacurile, dar măsurile tehnologice nu sunt foarte eficiente dacă personalul nu este instruit corespunzător. Acesta este unul dintre scopurile acestei unități. Cursanții ar putea fi informați despre astfel de aspecte citind textul corespunzător, urmărind webinarii în flux și rezolvând exerciții în ritm propriu. Toate aceste documente se află pe platforma digitală interactivă a proiectelor. Cursanții își pot testa răspunsurile la exerciții de autoevaluare. Răspunsurile la alte exerciții ar trebui salvate pe forumul de discuții corespunzător și discutate cu mentorul la întâlnirea comună organizată o dată pe săptămână. Cursantul poate lucra în cooperare cu ceilalți și poate îndruma în special în timpul întâlnirilor. Aceștia vor fi sprijiniți să dezvolte un portofoliu electronic important pentru reflecția și evaluarea instruirii

Conținutul materialului de învățare

Ce este ingineria socială?

Ingineria socială poate fi definită ca manipularea ființelor umane, cel mai adesea cu ajutorul metodelor psihologice, pentru a obține acces la date, documente și informații pe care atacatorul nu ar trebui să aibă acces să le obțină. Diferite forme de inginerie socială pot fi găsite cu ani în urmă, dar din cauza utilizării crescute a tehnologiei în principalele aspecte ale afacerii și vieții, amenințările cresc și au devenit un proces complex greu de oprit. Ingineria socială este una dintre principalele amenințări la adresa securității informațiilor în prezent și este o formă eficientă de criminalitate cibernetică. Repercusiunile potențiale ale unui atac social de succes pot fi foarte periculoase pentru oameni și organizații. În 2019, de exemplu, phishingul, o formă de infracțiune de inginerie socială, a fost responsabilă de multe încălcări ale datelor, mai mult decât orice alt tip de atac.

Multe atacuri de inginerie socială au scop financiar, iar organizațiile sop au pierdut sume considerabile de bani. În 2020, de exemplu, SUA pierde 4,2 miliarde de dolari, potrivit FBI (Abbate, 2020).

Companiile ar putea suferi perturbări în afaceri - pierderea productivității, o scădere a moralului angajaților și dificultăți pentru ca organizația să își revină. Acest proces poate avea consecințe, de multe ori o echipă de

răspuns la incident este concediată, ar trebui furnizat software de securitate care să ajute la prevenirea viitoarelor atacuri, iar angajații trebuie recalificați. Companiile, în cazul unui atac de inginerie socială, ar putea suferi și prejudicii reputației, deoarece clienții nu sunt convinși că organizația se poate proteja..

Importanța instruirii în inginerie socială

Este dificil să te protejezi împotriva ingineriei sociale, deoarece tacticile pe care le folosesc atacatorii se bazează pe comportamentul indivizilor și dacă angajații nu au pregătirea corespunzătoare pentru a recunoaște atacurile de inginerie socială, riscul de a deveni victimă este mare.

Formarea de inginerie socială ar putea fi inclusă în programele de conștientizare a securității și oferă angajaților cunoștințele și instrumentele de care au nevoie pentru a recunoaște aceste tipuri de atacuri și pentru a se proteja atât pe ei înșiși, cât și pe organizația lor (Weßelmann, 2008).

Datorită importanței formării de inginerie socială în reducerea la minimum a amenințărilor, multe organizații, în special IMM-urile care au mai puține resurse, ar trebui ajutate să ia foarte în serios formarea de conștientizare cibernetică, inclusiv ingineria socială și să ofere angajaților lor posibilități de a o urma (Mimecast Contributing Writer, 2021).

Până în 2022, de exemplu, este planificat ca 60% dintre organizațiile mari să ia în considerare conștientizarea securității (Gartner Magic Quadrant pentru SAT 2019).

Ciclul de viață al atacului de inginerie socială

Adesea, atacurile de inginerie socială se fac în mai mulți pași. Atacatorul investighează mai întâi victima vizată pentru a aduna informațiile de fundal necesare, cum ar fi punctele de intrare și protocoalele de securitate slabe care sunt necesare pentru atac. Apoi, atacatorul încearcă să câștige încrederea victimei și să ofere stimuli pentru acțiuni care nu sunt de obicei practici de securitate, cum ar fi să devină informații sensibile sau să acorde acces la resurse critice. Figura 1 explică ciclul de viață al unui atac.

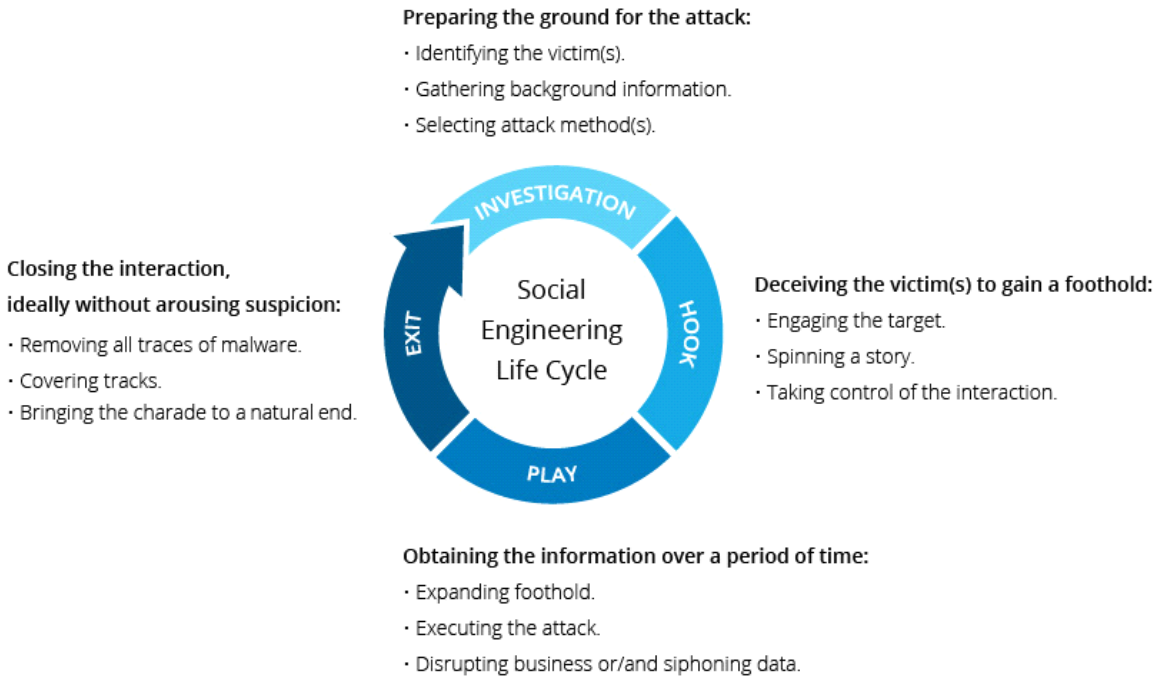

Figura 1: Ciclul de viață al atacului (https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/)

Ingineria socială este deosebit de periculoasă, deoarece se bazează mai mult pe eroarea umană, nu pe vulnerabilități în software și sisteme de operare. Este mai dificil să prezici greșelile făcute de utilizatorii legitimi, să le identifici și să le oprești decât o intruziune bazată pe malware.

Tehnici de atac de inginerie socială

Atacurile de inginerie socială au forme diferite și pot fi făcute oriunde unde este implicată interacțiunea umană. Cele mai comune forme de atacuri de inginerie socială digitală sunt următoarele:

Momeala

Atacurile de momeală încearcă să atragă curiozitatea victimei. Ei atrag utilizatorii într-o capcană, furându-le informațiile personale sau infectându-și sistemele cu programe malware. Cea mai des formă de momeală utilizează medii fizice pentru a dispersa malware. De exemplu, unități flash infectate cu malware, în zone vizibile unde este sigur că potenţialele victime le văd (de exemplu, băi, lifturi, parcarea unei companii vizate). Momeala are un aspect autentic, cum ar fi o etichetă care o prezintă ca lista de salarii a companiei. Victimele ridică momeala și o introduc într-un computer de la serviciu sau de acasă, rezultând o instalare automată a programelor malware pe

sistem. Atacurile de momeală nu se desfășoară neapărat în lumea fizică. Formele online de momeală constau în reclame tentante care duc la site-uri rău intenționate, care încurajează utilizatorii să descarce o aplicație infectată cu malware.

Scareware

Victimele devin alarme false și amenințări fictive. Utilizatorii cred că sistemul lor este infectat cu malware și trebuie să instaleze software care are beneficii numai pentru atacator sau este malware în sine. Scareware este considerat software de înșelăciune, software de scanare necinstiți și software de fraudă. Un exemplu comun de scareware este bannerele pop-up cu aspect legitim din propriul browser în timp ce navigați pe web cu text precum „Computerul dumneavoastră poate fi infectat cu programe spyware dăunătoare”. Acesta oferă fie să instaleze instrumentul (adesea infectat cu malware), fie să direcționeze victima către un site rău intenționat unde propriul computer va fi infectat. Scareware este distribuit și prin e-mail spam, care oferă utilizatorilor să cumpere servicii fără valoare/dăunătoare.

Pretexting

Atacatorul obține informații printr-o serie prin minciuni. Înșelătoria (fraudă) este adesea inițiată de un făptuitor care are nevoie de informații sensibile de la o victimă pentru a îndeplini o sarcină critică. Atacatorul începe, de obicei, prin a stabili încredere în victima sa prin uzurparea identității colegilor, poliției, oficialilor bănci și fiscali sau altor persoane care au autoritate de a cunoaște. Atacatorul pune întrebări care sunt necesare pentru a confirma identitatea victimei, prin care adună date personale importante. Multe informații și înregistrări importante pot fi adunate folosind această fraudă, și anume numere de securitate socială, adrese și numere de telefon personale, înregistrări telefonice, date de vacanță a personalului, înregistrări bancare și chiar informații de securitate legate de o fabrică fizică..

Phishing

Este unul dintre cele mai populare tipuri de atac de inginerie socială; Înșelătoriile de tip phishing (fraude) sunt campanii de e-mailuri și mesaje text menite să atragă curiozitatea sau teama victimelor și să le încurajeze să ofere informații sensibile, făcând clic pe linkuri către site-uri web rău intenționate sau deschizând atașamente care conțin malware. Un exemplu este un e-mail trimis utilizatorilor unui serviciu online care îi avertizează cu privire la o încălcare a politicii care necesită o acțiune imediată, cum ar fi modificarea necesară a parolei. Include un link către un site web nelegitim – aproape identic ca aspect cu versiunea sa legitimă – iar utilizatorul introduce datele de conectare actuale și noua parolă. Informația este trimisă atacatorului. Deoarece mesajele identice sau aproape identice sunt trimise către mulți utilizatori în campaniile de phishing, detectarea și blocarea acestora este mai ușoară pentru serverele de e-mail care au acces la platformele de

partajare a amenințărilor.

Spear phishing

Aceasta este o formă specială de atac de tip phishing, deoarece un atacator alege anumite persoane sau întreprinderi. Atacatorii își adaptează mesajele la caracteristicile, posturile de muncă și contactele victimelor lor pentru a face atacul lor mai puțin vizibil. Spear phishing necesită mai mult efort din partea făptuitorului (persoana care comite actul ilegal) și poate dura săptămâni și luni pentru a-l pregăti. Este mult greu de detectat astfel de atacuri și au rate de succes mai bune. De exemplu, un scenariu de spear phishing implică un atacator care, în calitate de consultant IT al unei organizații (existente), trimite un e-mail unuia sau mai multor angajați. Este semnat exact așa cum o face în mod normal consultantul, iar destinatarii cred că este un mesaj autentic. Mesajul cere victimelor să-și schimbe parola și le oferă un link care le redirecționează către o pagină rău intenționată în care atacatorul le fură acreditările..

Detect Phishing

Escrocii (persoanele care fac afaceri frauduloase) folosesc e-mailurile sau mesajele text pentru a păcăli persoanele să-și comunice informațiile personale. Ei încearcă să fure parole, numere de cont sau numere de securitate socială. Dacă primesc aceste informații, ar putea avea acces la e-mail, la bancă sau la alte conturi. Escrocii lansează mii de atacuri de tip phishing ca în fiecare zi - și au adesea succes. Escrocii își actualizează adesea tacticile, dar există câteva semne care ajută victimele să recunoască un e-mail sau un mesaj text de phishing, cum ar fi urmărirea:

- E-mailurile și mesajele text de tip phishing pot părea de la o companie pe care o cunoașteți sau în care aveți încredere. Arată de parcă provin de la o bancă, o companie de card de credit, un site de rețea socială, un site web sau o aplicație de plată online sau un magazin online.

- E-mailurile de phishing și mesajele text spun adesea o poveste pentru a păcăli victimele să facă clic pe linkul unei persoane sau să deschidă un atașament. Ei pot spune că au observat activități suspecte sau încercări de conectare, susțin că există o problemă cu contul sau informațiile de plată, spun că persoana respectivă trebuie să confirme anumite informații personale, să includă o factură falsă, să dorească ca persoana să facă clic pe un link către efectuați o plată, spuneți că persoana este eligibilă să se înregistreze pentru o rambursare guvernamentală etc.

Figura 2 prezintă un exemplu real de phishing.

E-mailul pare să provină de la o companie despre care persoana știe că ar putea și în care are încredere: Netflix. Folosește chiar și o siglă Netflix și un antet.

E-mailul spune că propriul cont este în așteptare din cauza unei probleme de facturare.

E-mailul are un salut generic, „Bună dragă”. Dacă persoana are un cont la companie, probabil că nu ar folosi un astfel de salut generic.

E-mailul invită persoana să facă clic pe un link pentru a vă actualiza detaliile de plată.

Acest e-mail poate părea real, dar nu este. Escrocii care trimit e-mailuri ca acesta nu au nimic de-a face cu companiile pe care se prefac a fi. E-mailurile de tip phishing pot avea consecințe reale pentru persoanele care oferă escrocilor informațiile lor. Și pot afecta reputația companiilor pe care le falsifică.

Protejați-vă împotriva phishingului

Filtrele proprii de e-mail-uri de spam ar putea păstra multe e-mailuri de phishing din propria căsuță de e-mail. Dar escrocii încearcă mereu să depășească filtrele de spam, așa că este util să adăugați straturi suplimentare de protecție.

Metode de protejare:

- Pentru a proteja propriul computer prin utilizarea software-ului de securitate, software-ul trebuie actualizat automat pentru a face față amenințărilor de securitate.
- Pentru a proteja propriul telefon mobil, software-ul ar trebui să se actualizeze automat.
- Pentru a proteja propriile conturi, ar trebui utilizată autentificarea cu mai mulți factori.
- Acreditările suplimentare pentru a vă conecta la propriul cont pot fi grupate în:
- O parolă se obține printr-o aplicație de autentificare sau o cheie de securitate.
- O scanare a propriei amprente, a retinei sau a feței.

Autentificarea cu mai mulți factori îngreunează escrocii să se conecteze la alte conturi dacă primesc numele de utilizator și parola corespunzătoare. Este important să protejați propriile date prin copii de siguranță care nu sunt conectate la propria rețea de acasă. Fișierele proprii ale computerului trebuie copiate pe un hard disk extern sau pe un spațiu de stocare în cloud. De asemenea, datele de pe telefonul propriu ar trebui copiate.

Comportați unui suspect un atac de phishing

- Dacă vine un e-mail sau un mesaj text care vă cere să faceți clic pe un link sau să deschideți un atașament, întrebați: Am un cont la companie sau cunosc persoana care m-a contactat?

- Dacă răspunsul este „Nu”, ar putea fi o înșelătorie de tip phishing. Trebuie să revizuiți sfaturile din Cum să recunoașteți phishingul, să căutați semne de înșelătorie de phishing, să raportați mesajul și apoi să-l ștergeți.

- Dacă răspunsul este „Da”, contactați compania folosind un număr de telefon sau un site web real, fără a introduce informațiile în e-mail, deoarece atașamentele și linkurile pot instala programe malware dăunătoare.

Răspunsul la un e-mail de phishing

Există pași specifici de urmat pe baza informațiilor pierdute

- Rulați o scanare.
- Dacă se primește un e-mail sau un mesaj text de phishing, raportați-l.

Ingineria socială dintr-o perspectivă interdisciplinară

Lumea de astăzi conectată în rețea și utilizarea intensivă a internetului și a tehnologiei sunt catalizatori pentru atacurile de inginerie socială. Protecțiile de sistem sunt utile pentru a atenua unele atacuri de inginerie socială, dar nu sunt suficiente. Crima pe internet a Biroului Federal de Investigații a subliniat că utilizarea sporită a ingineriei sociale și a schemelor de fraudă prin e-mail de afaceri au dus la pierderi de miliarde de dolari în ultimii câțiva ani (Abbate, 2020). Din nou, metodele hackerilor, este necesar să folosim o abordare interdisciplinară pentru a înțelege acest fenomen și toate complexitățile sale, mai ales în contextul modului în care acesta afectează afacerile. Recenzile de literatură evidențiază perspective din diferite discipline: tehnologia informației, psihologie, afaceri și etică. Figura 3 ilustrează această vedere (Washo, 2021).

Disciplina tehnologiei informației

Ingineria socială nu poate fi discutată decât în contextul sistemelor informaționale actuale și al utilizării lor în afaceri. Apărările tehnice pot fi utilizate ca formă de diminuare a riscurilor și se recomandă utilizarea strategiilor de control. Autentificarea cu mai mulți factori este o modalitate comună și adesea eficientă pentru organizații de a confirma că persoana care accesează sistemele ar trebui să aibă de fapt acel acces. De exemplu, un proces de conectare cu un nume de utilizator și o parolă ar fi o modalitate de autentificare a utilizatorului. Un factor suplimentar ar putea fi utilizarea unei rețele private virtuale (VPN) pentru a valida în continuare utilizatorul.

Disciplina psihologie

Ingineria socială este legată de înșelăciune, așa că o abordare psihologică a înțelegerii conceptului este importantă pentru a înțelege gândurile și comportamentele atât ale atacatorului, cât și ale victimei. Utilizarea metodelor psihologice este importantă pentru ingineria socială, deoarece acestea sunt utilizate pentru a susține protecții precum firewall-urile și sistemele utilizate pentru a identifica intrușii (Bullee, Montoya, Pieters, Junger și Hartel, 2018). Întreaga rețea de tehnologie a informației la o anumită companie este la fel de puternică ca și utilizatorul individual al unui anumit sistem. De fapt, comportamentul și acțiunile angajaților sunt una dintre principalele cauze ale încălcării datelor.

Perspectivă de afaceri

Ingineria socială afectează multe tipuri de afaceri și are implicații asupra modului în care organizațiile sunt structurate și gestionate. Subiectul poate fi luat în considerare din perspectiva afacerii pentru a determina factorii care influențează atacurile de inginerie socială. Acest punct de vedere este benefic dacă este legat de următoarele domenii de afaceri: instruire și dezvoltare, politici documentate, proceduri de audit intern, bugete și cultură organizațională. O deficiență în

oricare dintre aceste zone poate contribui la atacuri.

Perspectivă etică

Etica este importantă în contextul ingineriei sociale și al cercetării aferente pe această temă. Ideea de a manipula o altă ființă umană încalcă multe principii etice. În cazul unui eveniment de inginerie socială, tratamentul victimelor poate varia, dar adesea, acestea nu sunt tratate suficient pentru a permite atacul să aibă loc. Din păcate, calitățile întâlnite de obicei la angajații ideali, cum ar fi încrederea, dorința de a-i mulțumi pe alții, cum ar fi managerii, clienții, colegii de muncă și vizitatorii, și disponibilitatea de a se supune autorității, sunt de obicei aceleași caracteristici care îl fac pe un individ susceptibil la socializare. inginerie (Mouton, Malan, Kimppa și Venter, 2015).

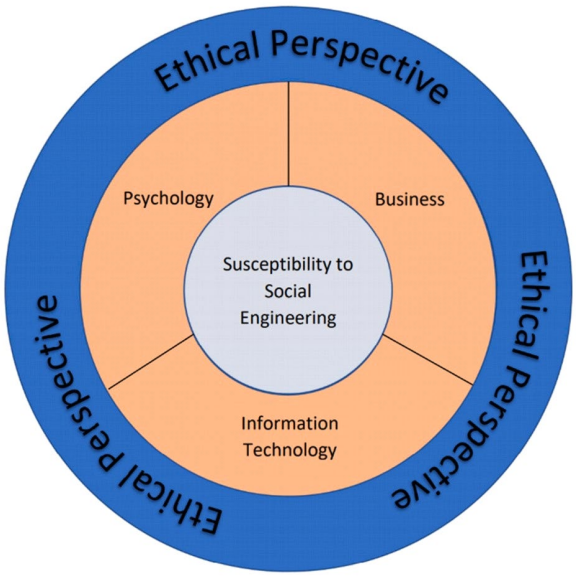

Figura 3: Inginerie socială dintr-o perspectivă interdisciplinară (Washo, 2021)

Revizuirea literaturii de specialitate din diferite discipline explică necesitatea unei abordări integrate pentru a studia subiectul complex al ingineriei sociale. Fiecare disciplină oferă informații despre cum să înțelegeți și să interpretați subiectul, să vă protejați împotriva diferitelor tipuri de atacuri și să înțelegeți impactul ingineriei sociale din punct de vedere uman și organizațional. Cu toate acestea, interpretarea fiecărei discipline a subiectului este utilă numai atunci când este privită în contextul celorlalte discipline.

Întrebări:

Forumul de discuții la care se răspunde cu o scurtă explicație. Răspunsurile vor fi discutate cu mentorul în timpul sesiunilor de mentorat

1. Cum să recunoașteți phishingul: adică e-mailurile și mesajele text de phishing spun adesea o poveste pentru a determina victimele să facă clic pe un link sau să deschidă un atașament.
2. Cum să vă protejați de atacurile de phishing
3. Vă rugăm să numiți câteva discipline legate de Inginerie Socială și să explicați pe scurt aceste conexiuni

Atasamente:

1. Prezentare
2. Filme video

Referințe:

Abbate, P., (2020). Internet Crime Report 2020
URL: (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)

Bullee, J., Montoya, L., Pieters, W., Junger, M., HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"&HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14" Hartel, P. (2018). On the anatomy of social engineering attacks: A literature-based dissection of successful attacks. HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"Journal of Investigative Psychology and Offender Profiling, 15HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"(1), 20HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14"–45.

Lee, T. (2020). Hire the Right Teachers for the Better Security Awarness. URL: https://www.gartner.com/smarterwithgartner/hire-the-right-teachers-for-better-security-awareness

Mimecast Contributing Writer (2021). Social Engineering Awarness Training for Emploeyees. URL: https://www.mimecast.com/blog/what-is-social-engineering/

Mouton, F., Malan, M., Kimppa, K., & Venter, H. (2015). Necessity for ethics in social engineering research. Computers & Security, 55, 114–127. https://doi.org/10.1016/j. HYPERLINK "https://doi.org/10.1016/j.cose.2015.09.001"cose.2015.09.001

Washo, A. (2021). An interdisciplinary view of social engineering: A call to action for research. URL: https://www.researchgate.net/publication/353448049_An_interdisciplinary_view_of_social_engineering_A_call_to_action_for_research

Weßelmann, B. (2008). Maßnahmen gegen Social Engineering: Training muss Awareness-Maßnahmen ergänzen. In: Datenschutz und Datensicherheit. DuD. 601–604.