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

InCyT træningsmoduler

Informationssikkerhed for medarbejdere **Enhed nr: (4) Uge 7** **Enhedens (modul) navn: (Social Engineering)**	
Læringsaktiviteter	❑ **Webinar** ❑ **Øvelser** ❑ **Værksted** ❑ **Præsentation** ❑ **Andet** Streaming af webinar, tekst, selvevalueringsøvelser, øvelser med svar på diskussionsfora og inden for de organiserede sessioner med træner/mentor, e-porteføljer
Læringsansvarlig	• David Sommer • Ileana Hamborg
Læringsaktivitetsmål	1. Social engineering angrebsteknikker 2. Betydningen af socialingeniøruddannelse 3. Sådan beskyttes mod phishing-angreb 4. Social ingeniørkunst ud fra et tværfagligt synspunkt
Færdigheder, der skal opnås	• **TS3 Netværkssikkerhed** • **TS4 Penetration (udnyttelige sårbarheder) test** • **SS3 Kognitiv og adfærdsanalyse**
Varighed af læringsaktivitet	2 uger
Læring krav	***Hvad skal der til?*** • Internetadgang • Internet browser • MS Office365

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

Kort information om modulet

Beskrivelse
Social engineering er en vigtig og meget ofte trussel mod informationssikkerheden. Dette modul forklarer kort Lifecycle of social engineering, hvordan et angreb opstår og kan forebygges. Især phishing beskrives som et af de mest populære social engineering-angreb. Mange virksomheder bruger tekniske løsninger til at forhindre angreb, men teknologiske tiltag er ikke særlig effektive, hvis personalet ikke er uddannet korresponderer. Dette er et af formålene med denne enhed. Eleverne kunne blive informeret om sådanne aspekter ved at læse den tilsvarende tekst, se streaming webinarer og løse øvelser i eget tempo. Alle disse dokumenter er på den digitale interaktive projektplatform. Eleverne kan teste deres svar på selvevalueringsøvelser. Svarene på andre øvelser skal gemmes på det tilsvarende diskussionsforum og diskuteres med mentoren på det fælles tilrettelagte møde en gang om ugen. Eleven kan arbejde sammen med andre og vejlede især under møderne. De vil blive støttet til at udvikle e-portfolio, der er vigtig for refleksion og evaluering af træningen

Lærematerialets indhold

Hvad er social engineering?

Social engineering kan defineres som at manipulere mennesker, oftest ved brug af psykologiske metoder, for at få adgang til data, dokumenter og information, som angriberen ikke burde have adgang til at få. Forskellige former for social engineering kan findes for år siden, men på grund af øget brug af teknologi i hovedaspekter af erhvervslivet og livet vokser truslerne og blev en kompleks proces, der er svær at stoppe. Social engineering er en af de førende trusler mod informationssikkerhed i dag og er en effektiv form for cyberkriminalitet. Potentielle følger af et vellykket socialt angreb kan være meget farligt for mennesker og organisationer. I 2019, for eksempel, var phishing, en form for social ingeniørkriminalitet, ansvarlig for mange databrud, mere end nogen anden form for angreb.

Mange social engineering angreb har økonomiske scops og sop organisationer tabt betydelige pengebeløb. I 2020 taber USA for eksempel 4,2 milliarder dollars ifølge FBI (Abbate, 2020).

Virksomheder kan lide forretningsforstyrrelser - tab af produktivitet, et fald i medarbejdernes moral og vanskeligheder for organisationen at komme sig. Denne proces kan have konsekvenser, ofte bliver et hændelsesteam fyret, sikkerhedssoftware til at forhindre fremtidige angreb bør stilles til rådighed, og

medarbejdere skal omkvalificeres. Virksomheder kan i tilfælde af et socialt ingeniørangreb også lide skade på deres omdømme, fordi kunderne ikke er overbeviste om, at organisationen kan beskytte sig selv .

Betydningen af socialingeniøruddannelse

Det er svært at beskytte sig mod social engineering, fordi den taktik, som angriberne bruger, er baseret på individers adfærd, og hvis medarbejderne ikke har tilsvarende uddannelse til at genkende social engineering angreb, er risikoen for at blive offer stor.

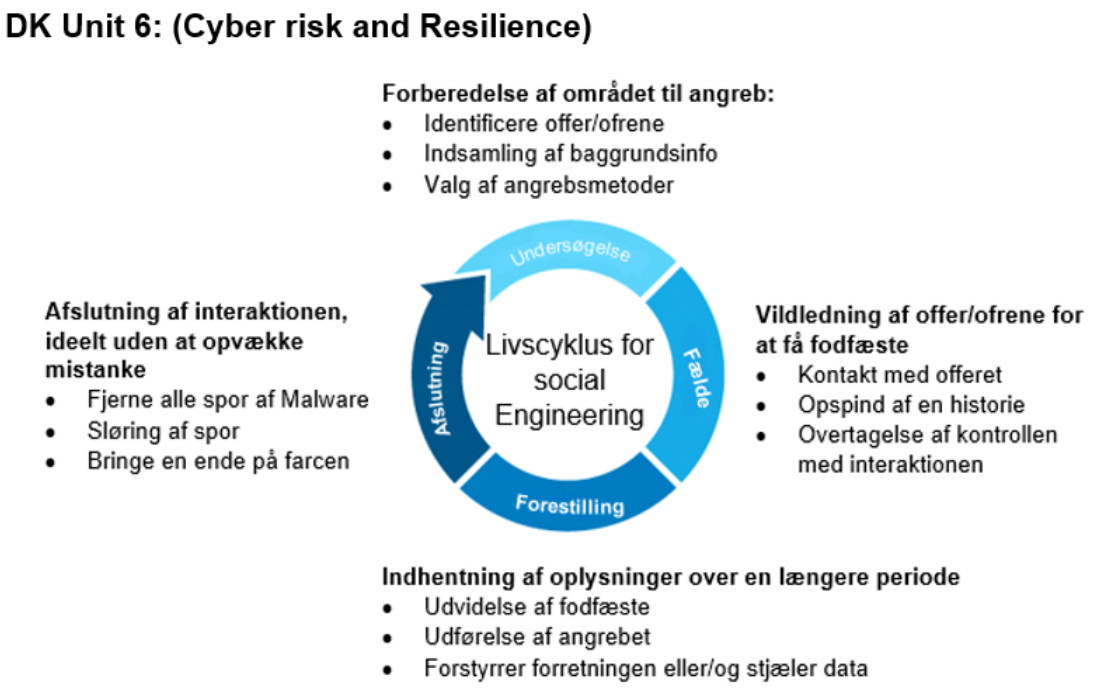
Social ingeniøruddannelse kunne inkluderes i sikkerhedsbevidsthedsprogrammer og giver medarbejderne den viden og de værktøjer, de har brug for til at genkende disse typer angreb og beskytte både sig selv og deres organisation (Weßelmann, 2008).

På grund af vigtigheden af social ingeniøruddannelse for at minimere trusler, bør mange organisationer, især SMV'er, der har færre ressourcer, hjælpes til at tage cyberbevidsthedstræning, herunder social ingeniørvidenskab, meget alvorligt og tilbyde deres medarbejdere muligheder for at følge den (Mimecast Contributing Writer, 2021).

I 2022 er det for eksempel planlagt, at 60% af store organisationer vil overveje sikkerhedsbevidsthed (Gartner Magic Quadrant for SAT 2019).

Social Engineering Attack Lifecycle

Ofte udføres sociale ingeniørangreb i flere trin. Angriberen undersøger først det påtænkte offer for at indsamle nødvendige baggrundsoplysninger, såsom adgangspunkter og svage sikkerhedsprotokoller, som er nødvendige for angrebet. Derefter forsøger angriberen at vinde ofrets tillid og give stimuli til handlinger, der ikke normalt er sikkerhedspraksis, såsom at blive følsomme oplysninger eller give adgang til kritiske ressourcer . Figur 1 forklarer livscyklussen for et angreb.



Figur 1: Attack Lifecycle (https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/)

Social engineering er særlig farlig, fordi den er baseret mere på menneskelige fejl, ikke på sårbarheder i software og operativsystemer. Det er sværere at forudsige fejl begået af legitime brugere, identificere og stoppe disse end en malware-baseret indtrængen.

Social engineering angrebsteknikker

Sociale ingeniørangreb har forskellige former og kan udføres overalt, hvor menneskelig interaktion er involveret. De mest almindelige former for digital social engineering-angreb er følgende:

Lokkemad

Lokkeangreb forsøger at opnå et offers nysgerrighed. De tiltrækker brugere i en fælde, der stjæler deres personlige oplysninger eller inficerer deres systemer med malware. De fleste ofte form for lokkemad bruger fysiske medier til at sprede malware. For eksempel malware-inficerede flashdrev i iøjnefaldende områder, hvor det er sikkert, at potentielle ofre ser dem (f.eks. badeværelser, elevatorer, parkeringspladsen for en målrettet virksomhed). Lokkemaden har et autentisk udseende, såsom en etiket, der præsenterer den som virksomhedens lønliste. Ofre samler lokket

op og indsætter det i en arbejds- eller hjemmecomputer, hvilket resulterer i en automatisk malwareinstallation på systemet. Lokkeangreb udføres ikke nødvendigvis i den fysiske verden. Online former for lokkemad består af fristende annoncer, der fører til ondsindede websteder, som opfordrer brugere til at downloade en malware-inficeret applikation.

Scareware

Ofre bliver til falske alarmer og fiktive trusler. Brugere tror, at deres system er inficeret med malware, og de skal installere software, der kun er til gavn for angriberen eller selve malware. Scareware betragtes som bedragerisoftware, useriøs scannersoftware og bedrageri. Et almindeligt eksempel på scareware er de legitimt udseende popup-bannere i egen browser, mens du surfer på nettet med tekst som "Din computer kan være inficeret med skadelige spywareprogrammer." Det tilbyder enten at installere værktøjet (ofte malware-inficeret) eller dirigere offeret til et ondsindet websted, hvor egen computer vil blive inficeret. Scareware distribueres også via spam-e-mail, der tilbyder brugere at købe værdiløse/skadelige tjenester.

Påskud

Angriberen får information gennem en serie gennem løgne. Fidusen (svindel) er ofte initieret af en gerningsmand, der har brug for følsomme oplysninger fra et offer for at kunne udføre en kritisk opgave. Angriberen starter normalt med at skabe tillid til sit offer ved at udgive sig for kolleger, politi, bank- og skatteembedsmænd eller andre personer, der har ret til at vide autoritet. Angriberen stiller spørgsmål, der er nødvendige for at bekræfte ofrets identitet, hvorigennem de indsamler vigtige personlige data. Mange vigtige oplysninger og registreringer kan indsamles ved hjælp af denne svindel, dvs. personnumre, personlige adresser og telefonnumre, telefonoptegnelser, personaleferiedatoer , bankoptegnelser og endda sikkerhedsoplysninger relateret til et fysisk anlæg.

Phishing

Er en af de mest populære sociale ingeniørangrebstyper; Phishing -svindel (svindel) er e-mails og sms-kampagner, der har til formål at opnå nysgerrighed eller frygt hos ofrene og tilskynde dem til at give følsomme oplysninger, klikke på links til ondsindede websteder eller åbne vedhæftede filer, der indeholder malware. Et eksempel er en e-mail sendt til brugere af en onlinetjeneste, som advarer dem om en politikovertrædelse, der kræver øjeblikkelig handling, såsom en påkrævet adgangskodeændring. Det inkluderer et link til et ikke-legitimt websted - næsten identisk med dets legitime version - og brugeren indtaster deres nuværende legitimationsoplysninger og nye adgangskode. Oplysningerne sendes til angriberen. Fordi identiske eller næsten identiske beskeder sendes til mange brugere i phishing-kampagner, er det nemmere at opdage og blokere dem for mailservere, der har adgang til trusselsdelingsplatforme .

Spyd phishing

Dette er en særlig form for phishing-angreb, fordi en angriber vælger bestemte personer eller virksomheder. Angribere tilpasser deres budskaber til deres ofres egenskaber, jobstillinger og kontakter for at gøre deres angreb mindre iøjnefaldende. Spear phishing kræver mere indsats fra gerningsmanden (person, der begår den ulovlige handling) og kan tage uger og måneder at forberede det. Det er meget vanskeligt at opdage sådanne angreb, og de har bedre succesrater. Som et eksempel involverer et spear phishing-scenarie en angriber, der som en (eksisterende) organisations it-konsulent sender en e-mail til en eller flere medarbejdere. Det er underskrevet præcis som konsulenten plejer, og modtagerne synes, det er en autentisk besked. Meddelelsen kræver, at ofrene ændrer deres adgangskode og giver dem et link, der omdirigerer dem til en ondsindet side, hvor angriberen stjæler deres legitimationsoplysninger.

Opdag phishing

Svindlere (folk, der laver svigagtige forretninger) bruger e-mail eller tekstbeskeder til at narre personer til at kommunikere deres personlige oplysninger. De forsøger at stjæle adgangskoder, kontonumre eller cpr-numre. Hvis de får disse oplysninger, kan de få adgang til e-mail, bank eller andre konti. Svindlere lancerer tusindvis af phishing-angreb som hver dag – og de er ofte vellykkede. Svindlere opdaterer ofte deres taktik, men der er nogle tegn, der hjælper ofrene med at genkende en phishing-e-mail eller tekstbesked, såsom følgende:

- Phishing-e-mails og sms-beskeder kan se ud, som om de er fra en virksomhed, du kender eller stoler på. De ser ud som om de er fra en bank, et kreditkortselskab, et socialt netværkssite, et online betalingswebsted eller en app eller en onlinebutik.
- Phishing-e-mails og tekstbeskeder fortæller ofte en historie for at narre ofrene til at klikke på et personlink eller åbne en vedhæftet fil. De kan sige, at de har bemærket en mistænkelig aktivitet eller log-in-forsøg, hævde, at der er et problem med kontoen eller betalingsoplysningerne, sige, at personen skal bekræfte nogle personlige oplysninger, inkludere en falsk faktura , have personen til at klikke på et link til foretage en betaling, sige, at personen er berettiget til at registrere sig for en offentlig refusion osv.

Figur 2 viser et virkeligt eksempel på et phishing.

E-mailen ser ud som om den er fra et firma, som personen kender kunne og stole på: Netflix. Den bruger endda et Netflix-logo og en header.

E-mailen siger, at egen konto er i venteposition på grund af et faktureringsproblem.

E-mailen har en generisk hilsen "Hej kære." Hvis personen har en konto i virksomheden, ville den sandsynligvis ikke bruge en sådan generisk hilsen.

E-mailen inviterer personen til at klikke på et link for at opdatere dine betalingsoplysninger.

Denne e-mail ser måske ægte ud, men det er den ikke. Svindlerne, der sender e-mails som denne, har ikke noget at gøre med de virksomheder, de udgiver sig for at være. Phishing-e-mails kan have reelle konsekvenser for folk, der giver svindlere deres oplysninger. Og de kan skade omdømmet for de virksomheder, de spoofer.

Beskyt mod phishing

Egne e-mail-spamfiltre kunne holde mange phishing-e-mails ude af egen indbakke. Men svindlere forsøger altid at overliste spamfiltre, så det er nyttigt at tilføje ekstra lag af beskyttelse.

Metoder til beskyttelse:

- For at beskytte egen computer ved at bruge sikkerhedssoftware, bør software opdateres automatisk for at håndtere sikkerhedstrusler .
- For at beskytte egen mobiltelefon bør software opdateres automatisk.
- For at beskytte egne konti bør der bruges multifaktorgodkendelse.

De yderligere legitimationsoplysninger for at logge ind på egen konto kan grupperes i:

- En adgangskode hentes via en godkendelsesapp eller en sikkerhedsnøgle.
- En scanning af eget fingeraftryk, nethinde eller ansigt.

Multifaktorgodkendelse gør det sværere for svindlere at logge ind på andre konti, hvis de får tilsvarende brugernavn og adgangskode. Det er vigtigt at beskytte egne data med sikkerhedskopier, som ikke er forbundet til eget hjemmenetværk. Egne computerfiler skal kopieres til en ekstern harddisk eller skylager. Ligeledes skal data på egen telefon kopieres.

Handle mod en mistænkt et phishing-angreb

- Hvis der kommer en e-mail eller en sms, der beder om at klikke på et link eller åbne en vedhæftet fil, så spørg: Har jeg en konto hos virksomheden eller kender jeg den person, der kontaktede mig?
- Hvis svaret er "Nej", kan det være et phishing-svindel. Du skal gennemgå tipsene i Sådan genkender du phishing , se efter tegn på phishing-svindel, rapportere beskeden og derefter slette den.
- Hvis svaret er "Ja", skal du kontakte virksomheden ved hjælp af et telefonnummer eller et rigtigt websted uden at angive oplysningerne i e-mailen, fordi vedhæftede filer og links kan installere skadelig malware.

Svar på en phishing-e-mail

Der er specifikke skridt at tage baseret på de tabte oplysninger

- Kør en scanning.
- Hvis der modtages en phishing-e-mail eller sms, skal du rapportere det.

Social ingeniørkunst ud fra et tværfagligt synspunkt

Den netværksforbundne verden i dag og den intensive brug af internettet og teknologi er katalysatorer for social engineering-angreb. Systembeskyttelse er nyttige til at afbøde nogle sociale ingeniørangreb, men det er ikke nok. Federal Bureau of Investigation's internetkriminalitet understregede den øgede brug af social engineering og e-mail-svindelordninger, der har resulteret i milliarder af dollars i tab i løbet af de sidste mange år (Abbate, 2020). Igen, metoder for hackere, er det nødvendigt at bruge en tværfaglig tilgang til at forstå dette fænomen og alle dets kompleksiteter, især i sammenhæng med, hvordan det påvirker virksomheder. Litteraturanmeldelser fremhæver perspektiver fra forskellige discipliner: informationsteknologi, psykologi, forretning og etik. Figur 3 illustrerer dette billede (Washo, 2021).

Informationsteknologi disciplin

Social engineering kan ikke diskuteres, medmindre det er i sammenhæng med de faktiske informationssystemer og deres brug i virksomheden. Tekniske forsvar kan bruges som en form for risikoreduktion, og kontrolstrategier anbefales at blive brugt. Multi-faktor autentificering er en almindelig og ofte effektiv måde for organisationer at bekræfte, at den person, der får adgang til systemerne, faktisk skal have denne adgang. For eksempel vil en login-proces med et brugernavn og en adgangskode være en måde for brugeren at blive autentificeret. En yderligere faktor kunne være brugen af et virtuelt privat netværk (VPN) login for yderligere at validere brugeren.

Psykologisk disciplin

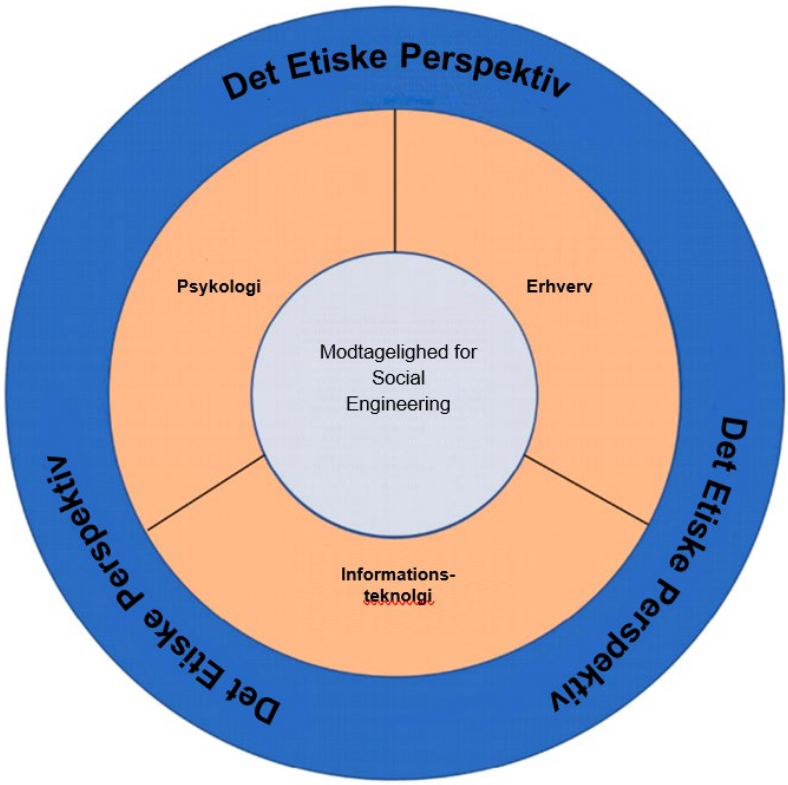
Social engineering er forbundet med bedrag, så en psykologisk tilgang til at forstå begrebet er vigtig for at forstå både angriberens og offerets tanker og adfærd. Brugen af psykologiske metoder er vigtige for social engineering, fordi de bruges til at understøtte beskyttelsen såsom firewalls og systemer, der bruges til at identificere ubudne gæster (Bullee, Montoya, Pieters, Junger, & Hartel, 2018). Hele informationsteknologinetværket hos en bestemt virksomhed er kun så stærkt som den enkelte bruger af et bestemt system. Faktisk er medarbejdernes adfærd og handlinger en af de førende årsager til databrud.

Forretningsperspektiv

Social engineering påvirker mange typer virksomheder og har konsekvenser for den måde, organisationer struktureres og ledes på. Emnet kan betragtes fra et forretningsperspektiv for at bestemme de faktorer, der påvirker social engineering-angreb. Dette synspunkt er fordelagtigt, hvis det er relateret til følgende forretningsområder: uddannelse og udvikling, dokumenterede politikker, interne revisionsprocedurer, budgetter og organisationskultur. En mangel på et af disse områder kan bidrage til angreb.

Etisk perspektiv

Etik er vigtig i forbindelse med social engineering og den relaterede forskning om emnet. Ideen om at manipulere et andet menneske krænker mange etiske principper. I tilfælde af en social ingeniørhændelse kan behandlingen af ofrene variere, men ofte bliver de ikke behandlet tilstrækkeligt til, at angrebet kan forekomme. Desværre er de egenskaber, der normalt findes hos ideelle medarbejdere, såsom tillid, villigheden til at behage andre såsom ledere, kunder, kolleger og besøgende, og villigheden til at adlyde autoriteter, som regel de samme egenskaber, der gør en person modtagelig for sociale engineering (Mouton, Malan, Kimppa, & Venter, 2015).



Figur 3: Social ingeniørkunst ud fra et tværfagligt synspunkt (Washo, 2021)

Litteraturgennemgangen fra forskellige discipliner forklarer behovet for en integreret tilgang til at studere det komplekse emne social engineering. Hver disciplin giver information om, hvordan man forstår og fortolker emnet, beskytter mod forskellige typer angreb og forstår virkningen af social engineering fra både et menneskeligt og organisatorisk synspunkt. Hver disciplins fortolkning af emnet er dog kun nyttig, når den ses i sammenhæng med de andre discipliner.

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

Spørgsmål :

Spørgsmål Diskussionsforum skal besvares med en kort forklaring. Svarene vil blive drøftet med mentoren under mentorsessionerne

1. Sådan genkender du phishing: dvs. phishing-e-mails og tekstbeskeder fortæller ofte en historie for at finde ud af, at ofrene skal klikke på et link eller åbne en vedhæftet fil.
2. Sådan beskyttes mod phishing-angreb
3. Nævn nogle discipliner forbundet med Social Engineering og forklar kort disse forbindelser

Vedhæftede filer:

1. Præsentation
2. Video film

Referencer:

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). Om anatomien af social engineering angreb: En litteraturbaseret dissektion af vellykkede angreb. HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14" Journal of Investigative Psychology and Offender Profiling, 15 HYPERLINK "http://refhub.elsevier.com/S2451-9588(21)00074-9/sref14" (1), 20 HYPERLINK "http://refhub.elsevier.com/S2451 -9588(21)00074-9/sref14" – 45.

Lee, T. (2020). Ansæt de rigtige lærere for at opnå bedre sikkerhedsbevidsthed. URL: https://www.gartner.com/smarterwithgartner/hire-the-right-teachers-for-better-security-awareness

Mimecast-bidragende forfatter (2021). Social Engineering Awareness Training for Emloeyee. URL: https://www.mimecast.com/blog/what-is-social-engineering/

Mouton, F., Malan, M., Kimppa, K., & Venter, H. (2015). Nødvendighed for etik i social ingeniørforskning. Computere og sikkerhed, 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). Et tværfagligt syn på social engineering: En opfordring til handling for forskning. URL: https://www.researchgate.net/publication/353448049_An_interdisciplinary_view_of_social_engineering_A_call_to_action_for_search

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