

InCyT træningsmoduler

Informationssikkerhed for medarbejdere Enhed nr: (4) Uge 8 Enhedens (modul) navn: (Social Networking)	
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. Sociale netværksroller 2. Funktionalitet af sociale netværksplatforme 3. Sikkerhed og privatliv i sociale netværk 4. Trusler mod online sociale netværk og løsninger for at undgå dem 5. Tværfaglighed i sociale netværk
Færdigheder, der skal opnås	• TS3 Netværkssikkerhed • TS4 Penetration (udnyttelige sårbarheder) test • TS5 Intrusion detection • SS3 Kognitiv og adfærdsanalyse
Varighed af læringsaktivitet	2 uger
Læring krav	Hvad skal der til? • Internetadgang • Internet browser • MS Office365

Kort information om modulet

 Beskrivelse
Sociale netværk hjælper mennesker og organisationer med at forbinde med venner, er kommunikationsmidler, hjælper med at lancere en ny forretningsside, sælge produkter eller tjenester og udvide rækkevidden af et eget brand. Sikker på, der er også ulemper ved socialt netværk som formindskelse af ansigt-til-ansigt kommunikationsevner. Fordi organisationer bruger intensivt sociale medier, bruger angribere disse platformes tillid og offentlige karakter til angreb. Social netværkssikkerhed er vigtig for erhvervslivet og privat succes, så træning af medarbejdere som inden for dette modul kan have et stort bidrag. Medarbejderne lærer om sådanne aspekter ved at læse den tilsvarende tekst, se streaming-webinarer og løse øvelser i eget tempo og reflektere over, hvad de lærer (e-portfolios). Alle moduldokumenter er på den digitale interaktive projektplatform. Eleverne kan teste deres svar på selvevalueringsøvelser. Svarene på andre øvelser skal gemmes på de tilsvarende diskussionsfora og diskuteres med mentoren på det fælles tilrettelagte møde en gang om ugen. Eleven kan arbejde sammen med andre og vejlede især under de ugentlige møder.

Lærematerialets indhold

Introduktion

Også på grund af voksende teknologi blev (online) sociale netværk meget populære i løbet af de sidste par år. En af grundene er deres evne til at give brugere en platform til at kommunikere med deres familie, venner og kolleger.

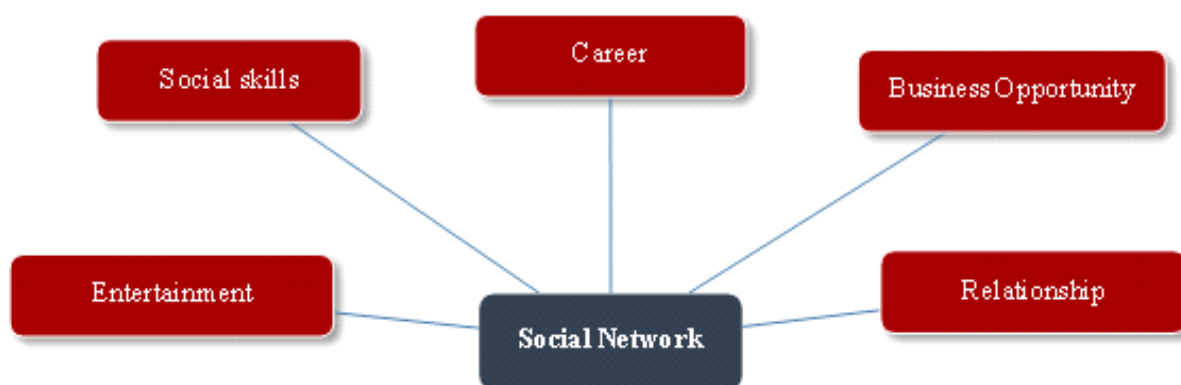
Socialt netværk refererer til brugen af internetbaserede sociale medier til forbindelse og kommunikation med venner, familie, kolleger, kunder eller klienter.

Sociale medier hjælper folk til at få bedre forhold til familie, venner, kunder og mobile enheder, der understøtter sociale medier, vinder mere og mere interesse sammenlignet med andre måder at få internetadgang på.

Sociale netværk har deres servere i datacentre samlokaliseret, når det er muligt, med store Internets Network Access Points (NAP'er), hvor store internetudbydere opretter forbindelse til hinanden, og hvor de giver den direkte adgang til internettets hurtige forbindelser.

Sociale netværksroller

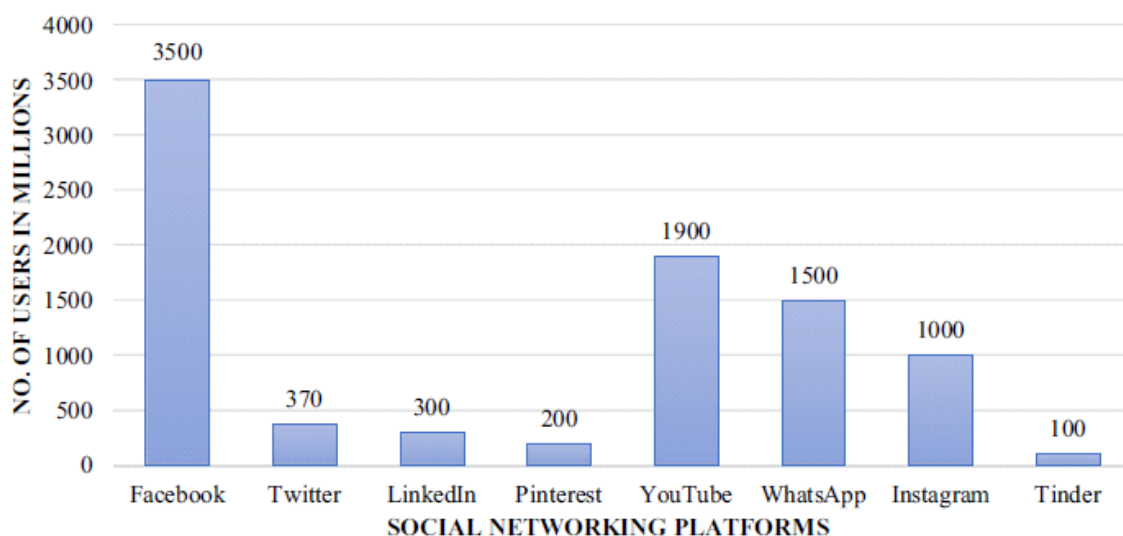
Sociale netværk kan have en social rolle, en virksomhed eller begge dele, ved at bruge websteder som Facebook, Twitter, LinkedIn og Instagram. Figur 1 viser nogle områder, hvor sociale netværk spiller en rolle (Milsova et al.): underholdning, opbygning af forretningsmuligheder, karriere, forbedring af sociale færdigheder og udvikling af relationer til andre individer.



Figur 1: Roller i sociale netværk

Sociale netværk er en base for marketingfolk, der søger kunder. Markedsførere bruger sociale netværk, dvs. til at øge mærkegenkendelse og tilskynde til brandloyalitet. Sociale medier kan hjælpe med at forbinde mennesker og virksomheder og kan hjælpe med at fremme brand awareness. For eksempel kan en hyppig Twitter-bruger lære om en virksomhed for første gang gennem et nyhedsfeed og beslutte at købe et produkt eller en tjeneste. Virksomhedens muligheder for at finde og fastholde nye kunder øges gennem sociale netværk. Marketingfolk bruger sociale netværk til at forbedre konverteringsraterne, giver adgang til og interaktion med nye, nye og gamle kunder. Ved at dele blogindlæg, billeder, videoer eller kommentarer på sociale medier vil flere mennesker besøge virksomhedens hjemmeside og blive kunder. Men der er ikke én tilgang til markedsføringsstrategier :_hver virksomhed er unik og har et andet mål, demografisk, historie og konkurrencedygtig markedsplads. Fordi sociale netværksvirksomheder ønsker, at virksomheder skal betale for deres annoncering, begrænser virksomheder ofte antallet af virksomheder, der modtages via ubetalte indlæg. For eksempel, hvis en virksomhed har 500 følgere, modtager følgere muligvis ikke alle det samme opslag. Den udviklende karakter af sociale netværk gør det udfordrende at følge med ændringer og påvirker også en virksomheds succesrate for markedsføring.

Facebook, Instagram, Facebook Messenger og Twitter er de mest populære sociale netværkssider i USA og også Europa. Andre inkluderer Pinterest, Tumblr, Snapchat, TikTok og YouTube, WhatsApp, Messenger af Google og Tumblr. LinkedIn er et andet populært websted, som hjælper med at forbinde fagfolk med kolleger, forretningsforbindelser og arbejdsgivere. Facebook er fortsat det største og mest populære sociale netværk, med 2,91 milliarder mennesker, der bruger platformen på månedsbasis, pr. 31. december 2021. Figur 2 viser antallet af brugere på platforme.



Figur 2: Antal brugere på platforme (<https://www.dreamgrow.com/top/>)

Funktionalitet af sociale netværk

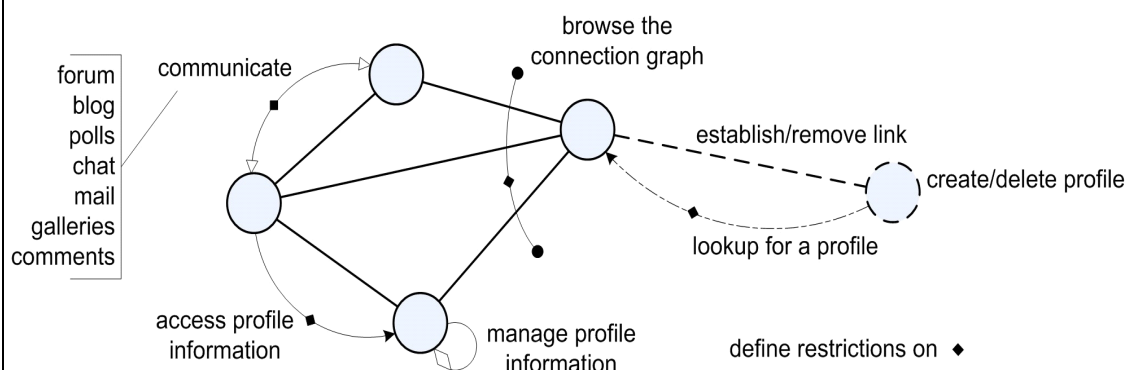
Socialt netværk er baseret på udvikling og vedligeholdelse af personlige og forretningsmæssige relationer ved hjælp af teknologi ved brug af sociale netværkssider. Disse websteder giver folk og virksomheder mulighed for at forbinde med hinanden, så de kan udvikle relationer, og de kan dele information, ideer og budskaber.

Familiemedlemmer, der er langt væk, kan forblive forbundet via personlige sociale netværkssider som Facebook og dele billeder og sende andre beskeder fra deres liv. Folk kan også forbinde sig med andre (fremmede), der deler de samme interesser. Enkelt personer kan finde hinanden ved at være medlemmer i grupper, på lister og brug af hashtags.

Men der er også ulemper forbundet med sociale medier, herunder spredning af misinformation og de høje omkostninger ved at bruge og vedligeholde sociale netværksprofiler.

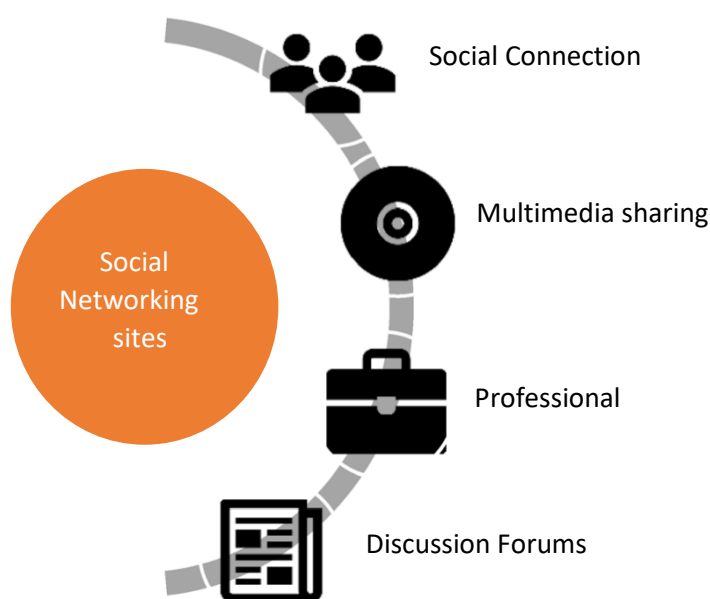
Hvert socialt netværk tjener normalt en bestemt brug, men funktionaliteten af disse platforme er ens og kan klassificeres i tre hovedtyper:

- Netværksfunktionerne tjener til at fremme sociale relationer mellem brugere på de virtuelle platforme. De giver især funktionalitet til at bygge og vedligeholde grafen for det sociale netværk.
- Datafunktionerne er ansvarlige for styring af brugerleveret indhold og kommunikation mellem brugerne. Variationen bidrager til forbedring (udvidet) af brugernes interaktion og gør platformen mere attraktiv.
- Adgangskontrolfunktionerne har til formål at implementere de brugerdefinerede privatlivsforanstaltninger og at begrænse uautoriseret adgang til de brugerleverede data og informationer. Figur 3 viser funktionaliteten leveret af en typisk virtuel social netværksplatform og giver flere detaljer (Cutillo et al. 2010).



Figur 3: Hovedfunktionalitet af en typisk social netværksplatform (<https://hal.archives-ouvertes.fr/hal-00687145>)

Sociale netværkssider kan klassificeres i 'sociale forbindelser' 'multimediedeling', 'professionel' og 'diskussion' fora' (Figur 4 Jain et al., 2021)



Figur 4: Sociale netværkssider (Jain et al, 2021)

Fordele og ulemper ved sociale netværk

Sociale netværk har evnen til at påvirke både enkeltpersoner og virksomheder – både positivt og negativt, og det er derfor vigtigt at tage hensyn til fordele og ulemper ved at bruge sådanne sociale medier.

Fordele

Sociale netværk giver enkeltpersoner mulighed for at holde kontakten med familie og venner, som de ellers ikke ville være mulige på grund af afstand eller mistet kontakt. Folk kan også forbinde med andre individer, der deler de samme interesser og udvikle nye relationer.

Sociale netværk giver virksomheder mulighed for at forbinde med nye og eksisterende kunder. Virksomheder kan også bruge sociale medier til at skabe, promovere og øge brandbevidstheden. De stoler også på anmeldelser og kommentarer fra deres kunder, der er vigtige for brandet. Det kan øge salget og en højere placering i søgemaskinerne.

Sociale netværk kan være med til at etablere et nyt brand. En virksomhed kan bruge sociale netværk til at demonstrere sin kundes høje serviceniveau og forbedre produkter og relationer til forbrugerne. For eksempel, hvis en kunde klager over et produkt eller en tjeneste på Twitter, undskylder virksomheden og tager skridt til at forbedre situationen.

Ulemper

Sociale netværk kan bidrage til spredningen af misinformation Sahoo og Gupta, 2020 fandt ud af, at misinformation er 70 % mere tilbøjelig til at blive delt end rigtig information på Twitter.

Netværk på sociale medier kan have en skadelig indvirkning på virksomheder. Kritikken af et brand bredte sig meget hurtigt på de sociale medier. Dette har ulemper for en virksomheds PR-afdeling.

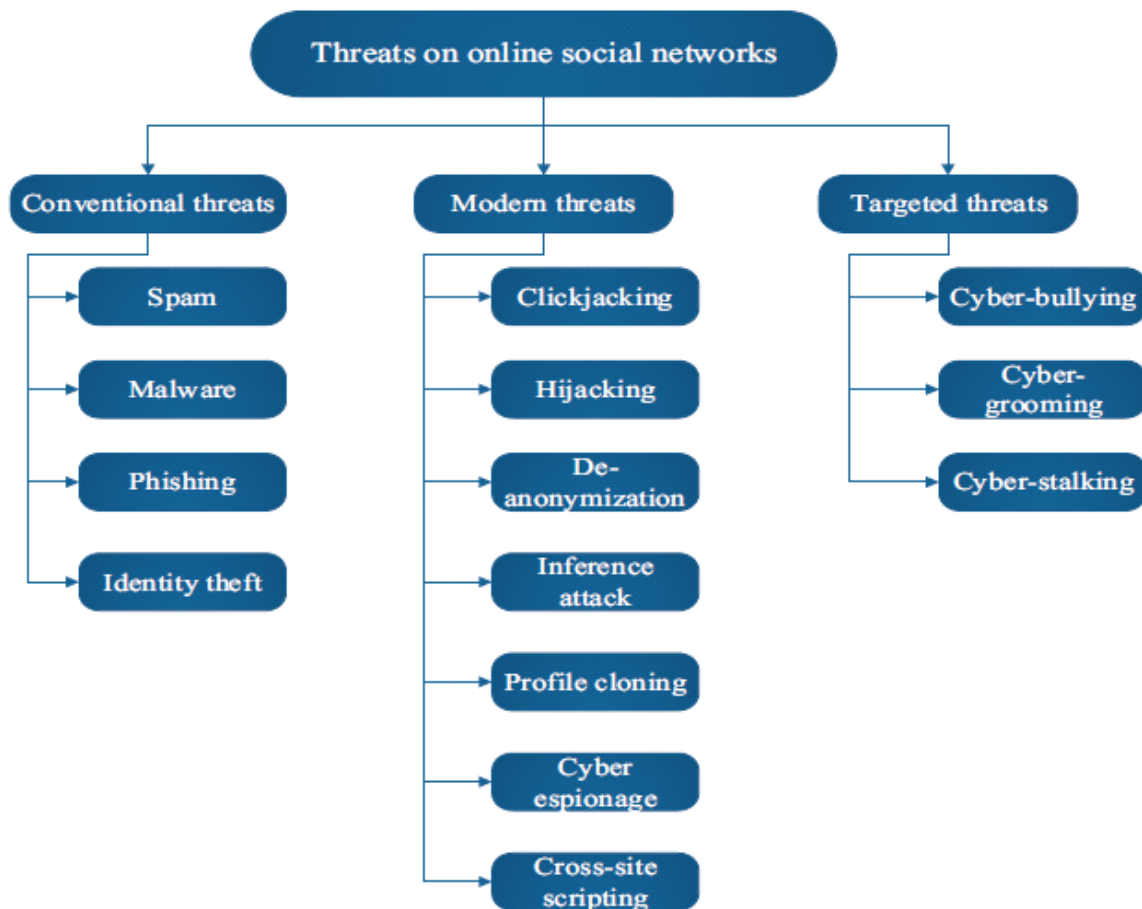
Socialt netværk i sig selv er gratis, men opbygning og vedligeholdelse af en virksomhedsprofil kræver timers arbejde og omkostninger hver uge. Virksomheder har brug for mange følgere, før en markedsføringskampagne på sociale medier begynder at generere et positivt investeringsafkast (ROI). For eksempel har det ikke samme effekt at sende et opslag til 15 følgere som at sende indlægget til 15.000 følgere.

Sikkerhed og privatliv i sociale netværk

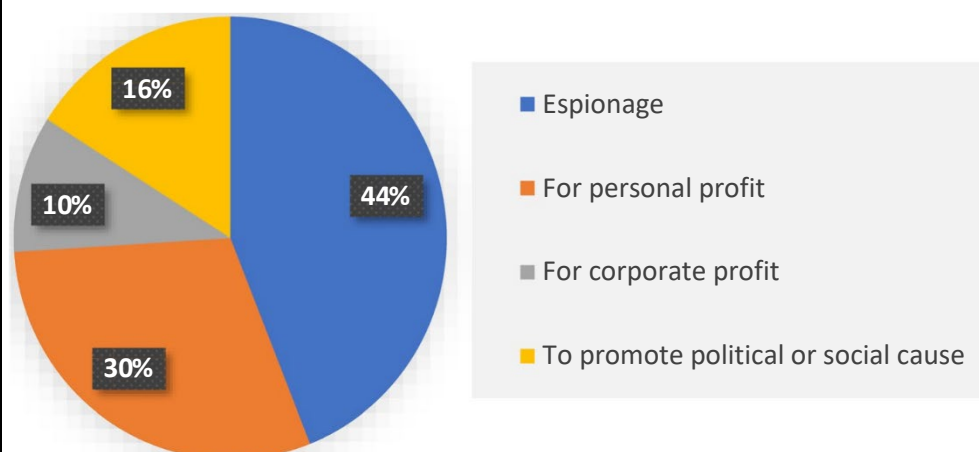
Den information, der deles på sociale netværk og medier, spredes meget hurtigt, hvilket gør det attraktivt for angribere at få dem. Der er sikkerheds- og privatlivsproblemer relateret til brugerens delte oplysninger, når en bruger uploader personligt indhold såsom billeder, videoer og lyd. Angriberen kan ondsindet bruge delt information til illegitime formål.

Nogle forskellige sikkerheds- og privatlivstrusler og eksisterende løsninger, der kan give sikkerhed til brugere af sociale netværk, præsenteres snart.

På grund af intensiv brug af teknologi er interaktioner blevet udvidet via internettet. Desværre har manglende bevidsthed blandt brugerne om sikkerhed og privatliv potentialet til at føre til forskellige cyberangreb gennem sociale medier. De trusler, som brugerne opdagede fra begyndelsen af sociale netværk, kan opdeles i tre kategorier, dvs. konventionelle trusler, moderne trusler og målrettede trusler (fig. 5, Jain og Gupta, 2018). Konventionelle trusler omfatter trusler, som brugere har oplevet fra begyndelsen af det sociale netværk. Moderne trusler er angreb, der bruger avancerede teknikker til at kompromittere brugernes konti, og målrettede angreb er angreb, der er rettet mod en bestemt bruger, som kan begås af enhver bruger til forskellige personlige vendettaer.



Figur 5: Klassificering af trusler (Jain et al, 2018)

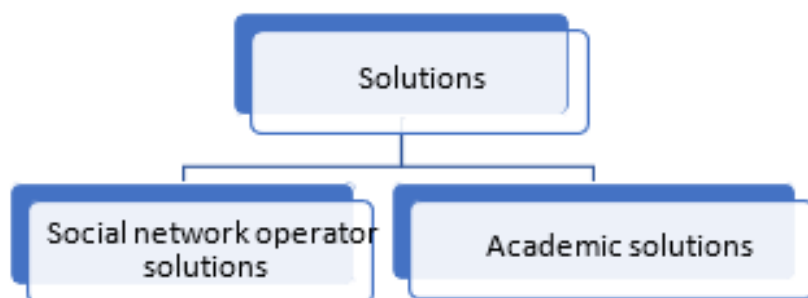


Figur 6: De fleste typer hacking i 2021 (Jain et al, 2021)

Løsninger på trusler

Forskere i den akademiske verden og industrier forsøger at finde løsninger på truslerne i sociale netværk for forskellige typer hacking som vist i figur 6. Løsninger og nogle tilgange er blevet foreslået og kan klassificeres

i to grupper: sociale netværksoperatørløsninger og akademiske løsninger (Jain et al., 2021). Figur 7 viser klassifikationen. En kort beskrivelse er præsenteret nedenfor.



Figur 7: Klassificering af løsninger på trusler (Jain et al, 2021)

Løsninger til sociale netværksoperatører

Autentificeringsmekanisme

For at sikre, at det kun er en legitim bruger, der logger eller registrerer sig på et socialt netværk og ikke en social bot, er der blevet foreslået godkendelsesprocedurer såsom CAPTCHA, multi-faktor-godkendelse og foto-af-ven-identifikation. For eksempel bruger sociale netværk som Twitter og Facebook to-faktor autentificeringsprincipper. Dette princip bruger en login-adgangskode og en bekræftelseskode modtaget via en mobilenhed. Dette er med til at mindske risikoen for, at en konto bliver kompromitteret og forhindrer en hacker i at kapre en legitim konto og poste skadeligt indhold.

Indstilling af sikkerhed og privatliv

Mange sociale netværkssider giver konfigurerbare sikkerheds- og privatlivsindstillinger for at give klienten mulighed for at fjerne personlige oplysninger fra uønsket adgang for udenforstående eller applikationer. For eksempel kan Facebook-klienten ændre deres sikkerhedsindstillinger og vælge publikum (som venner, venners venner og alle andre) på netværket, som kan se deres detaljer, billeder, opslag og andre følsomme oplysninger.

Rapportér brugere

Sociale netværk beskytter folk mod angreb ved at give mulighed for at rapportere enhver form for misbrug eller politikovertrædelser fra enhver bruger i deres netværk. For eksempel, hvis en bruger ser noget på Facebook, der svarer til den enkeltes følelser, men det ikke overtræder Facebooks vilkår, så kan brugeren bruge en rapport (links) til at sende en besked til den, der postede den, og bede ham om at tage den ned eller fjerne.

Når Facebook modtager en brugerrapport, bliver den gennemgået og fjernet i henhold til Facebooks community-standards.

Akademisk forskningsbaserede løsninger

Phishing-detektion

Phishing bekymrede privatlivet og sikkerheden for mange traditionelle webapplikationer såsom websteder, sociale netværkssider, e-mails og blogs. Derfor er der udviklet adskillige anti-phishing-teknikker til at opdage phishing-angreb. For eksempel har Aggarwal et al. foreslog PhishAri-teknikken til realtidsidentifikation af phishing-angreb, der forekommer på Twitter. Den brugte specifikke Twitter-funktioner som kontoalder og antal følgere til at opdage, om det udsendte tweet er phishing eller sikkert.

Opdagelse af cybermobning

Cybermobning er brugen af elektroniske medier såsom e-mails, chats, telefonsamtaler og online sociale netværk til at undertrykke en person. I modsætning til traditionel mobning er cybermobning en kontinuerlig proces, der vedligeholdes gennem sociale medier. Selvom det er mere komplekst at opdage cybermobning end at opdage racistisk sprogbrug og spam, har nogle forskere forsøgt at opdage det ved hjælp af mere kompleks dokumentrepræsentation og yderligere information om ofre og mobbere. Maskinlæringsteknikker kan anvendes til at opdage cybermobning.

Clickjacking

Et automatiseret system kan analysere websider for at beskytte brugeren mod clickjacking-angreb. Den består af en kode, der kan detektere overlappende klikbare elementer. Og udover denne løsning, tog de også i brug NoScript-værktøjet, som har en anti-clickjacking-funktion inkluderet.

Cyberstalking

Krypteringsteknikker er tilgængelige for enheder på nyere versioner af Android og iOS. Hvis en enhed bliver stjålet, kan tyven ikke læse indholdet, hvis kryptering er aktiveret. Yderligere bliver ethvert forsøg på at læse informationen fra intern eller ekstern hukommelse forpurret af eksistensen af en enhedsadgangskode. Der er forskellige teknologier, der kan bruges mod stalkere som smartphone fingeraftryksslås.

Spam detektion

En ramme kaldet Spam Spotter kan hjælpe mod et spam-angreb på Facebook. Det er baseret på det intelligente beslutningsstøttesystem (IDSS). Den samler al relevant information fra brugerprofilen ved hjælp af en beslutningsproces i IDSS og analyserer den derefter ved at kortlægge brugerdata til klassificeringen af en brugerprofil som spammer eller legitim.

Malware

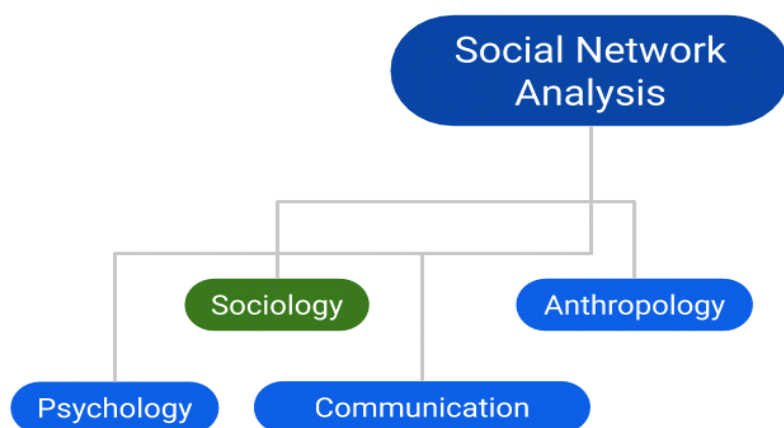
Cross Site Scripting Worms (XSS-orme) er ondsindede programmer, der spreder sig gennem besøgende på et websted, der hopper for at inficere andre besøgende gradvist .

Ormen formerer sig langsommere, når medlemmer for det meste besøger deres venner frem for fremmede. Det kan også bremses af sociale netværks grupperede karakter.

Selvom den akademiske verden har udviklet sådanne innovative løsninger til at løse sikkerhedsforanstaltningerne i forbindelse med social netværkssikkerhed, mangler de implementering og gennemførlighed i den virkelige verden. Der er således et presserende behov for løbende og iterativt at gennemgå sikkerhedsproblemer i sociale netværk under hensyntagen til den teknologiske udvikling.

Tværfaglighed i sociale netværk

Det tværfaglige felt, der refererer til sociale netværk, er social netværksanalyse (SNA) og omfatter indsigt fra andre samfundsvidenskabelige discipliner såsom sociologi, antropologi, psykologi, kommunikation og andre. SNA er en del af et endnu større tværfagligt felt med ansvar for at studere alle typer netværk kaldet netværksvidenskab, som omfatter arbejde inden for fysik, datalogi, datavidenskab, biologi, teknik, matematik og andre områder. Forholdet mellem disse felter er vist i figur 8 (https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html).



Figur 8: Relationer mellem felter i SNA (https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html)

Spørgsmål :

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

1. Roller i sociale netværk
2. Sociale netværkssider
3. Tværfaglige felter i forbindelse med sociale netværk

Vedhæftede filer:

1. Præsentation
2. Video film

Referencer:

Referencer

- Aggarwal A., Rajadesingan A & Kumaraguru P. (2012). PhishAri: automatisk realtime phishing-detektion på twitter. eCrime Res. Topmøde, e-kriminalitet. 1-12.
- Ankit Kumar J., Somya Ranjan S. & Kaubiyal J. (2021). Databrud forårsager verden over. URL: <https://www.statista.com/statistik/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/>
- Cuttillo, A., Manulis, M. & Strute, T.(2010). Sikkerhed og privatliv i online sociale netværk. EUROCOM. TU Darmstadt.
- Gupta B. & Sahoo, S. (2021). Online sociale netværkssikkerhed: principper, algoritme, applikationer og perspektiver. CRC Tryk.
- Jain A. & Gupta B. (2018). Detektering af phishing-angreb på finans- og e-bankwebsteder ved hjælp af link og visuel lighedsrelation. Int J Inf Comp Secur 10(4):398–417.
- Jain, A., Sahoo, SR & Kaubiyal, J. (2021). Online sociale netværk sikkerhed og privatliv: omfattende gennemgang og analyse. Komplex Intell. Syst. 7, 2157-2177.
- Kangur, K. (2022). De 15 største sociale medier og apps. URL: <https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/>.
- Mislove A., Viswanath B., Gummadi K. & Druschel, P. (2010). Du er den du kender. I: Proceedings af den tredje ACM internationale konference om websøgning og datamining—WSDM '10, 251.
- Rydstedt, G. (2018). Clickjacking – OWASP. URL: <https://owasp.org/www-community/attacks/Clickjacking>.
- Sahoo SR, Gupta BB (2020). Registrering af falsk profil i multimediebig data på sociale online netværk. Int J Inf Comput Secur 12(2–3), 303–331.