

Module de instruire InCyT

Securitatea informațiilor pentru angajați

Unitatea 4 Săptămâna 8

Numele unității: Inginerie socială

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. Roluri în rețelele sociale 2. Funcționalitatea platformelor de rețele sociale 3. Securitate și confidențialitate în rețelele sociale 4. Amenințări la adresa rețelelor sociale online și soluții pentru a le evita 5. Interdisciplinaritatea în rețelele sociale
Abilități de dobândit	• Securitatea rețelei TS3 • Testarea TS4 Penetration (vulnerabile exploatabile). • S5 Detectare intruziuni • 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

Informații scurte despre modul



Descriere

Rețelele sociale ajută oamenii și organizațiile să se conecteze cu prietenii, sunt mijloace de comunicare, ajută la lansarea unei noi idei de afaceri, la vânzarea de produse sau servicii și la extinderea acoperirii unui brand propriu. Sigur, există și dezavantaje ale rețelelor sociale, cum ar fi scăderea abilităților de comunicare față în față. Deoarece organizațiile folosesc intens rețelele sociale, atacatorii folosesc încrederea și natura publică a acestor platforme pentru atacuri. Securitatea rețelelor sociale este importantă pentru succesul în afaceri și privat, astfel încât pregătirea angajaților ca în cadrul acestui modul poate avea o mare contribuție.

Angajații învață despre astfel de aspecte citind textul corespunzător, urmărind webinarii în flux și rezolvând exerciții în propriul ritm și reflectând asupra a ceea ce învață (e-portfolios). Toate documentele modului se află pe platforma digitală interactivă a proiectului.

Cursanții își pot testa răspunsurile la exerciții de autoevaluare. Răspunsurile la alte exerciții ar trebui salvate pe forumurile de discuții corespunzătoare 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 săptămânale.

Conținutul materialului de învățare

Introducere

De asemenea, datorită tehnologiei în creștere, rețelele sociale (online) au devenit foarte populare în ultimii ani. Un motiv este capacitatea lor de a oferi utilizatorilor o platformă pentru a comunica cu familia, prietenii și colegii lor.

Rețelele sociale se referă la utilizarea site-urilor de social media bazate pe internet pentru conectarea și comunicarea cu prietenii, familia, colegii, clienții sau clienții.

Rețelele sociale îi ajută pe oameni să aibă relații mai bune cu familia, prietenii, clienții și dispozitivele mobile care susțin rețelele sociale câștigă din ce în ce mai mult interes în comparație cu alte modalități de acces la internet.

Rețelele sociale își au serverele în centre de date amplasate, atunci când este posibil, cu

principalele puncte de acces la rețea (NAP) ale Internetului, unde marii furnizori de servicii de internet se conectează între ei și unde oferă acces direct la conexiunile rapide ale Internetului.

Roluri în rețelele sociale

Rețelele sociale pot avea un rol social, unul de afaceri sau ambele, folosind site-uri precum Facebook, Twitter, LinkedIn și Instagram. Figura 1 prezintă câteva domenii în care rețelele sociale joacă un rol (Milsova și colab.): divertisment, construirea de oportunități de afaceri, realizarea unei cariere, îmbunătățirea abilităților sociale și dezvoltarea relațiilor cu alți indivizi..

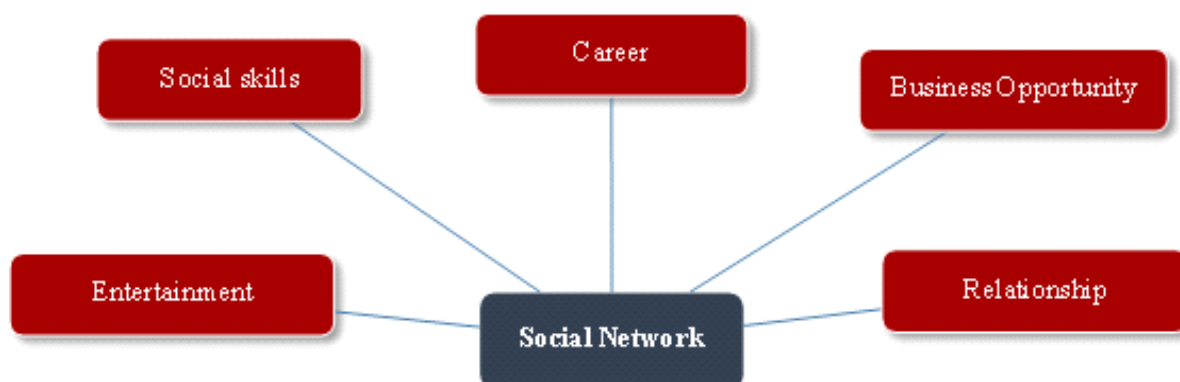


Figura 1: Rolurile rețelelor sociale

Rețelele sociale reprezintă o bază pentru agenții de marketing care caută clienți. Specialiștii în marketing folosesc rețelele sociale, adică pentru a crește recunoașterea mărcii și pentru a încuraja loialitatea mărcii. Rețelele de socializare pot ajuta la conectarea oamenilor și a companiilor și pot contribui la promovarea conștientizării mărcii. De exemplu, un utilizator frecvent Twitter poate afla despre o companie pentru prima dată printr-un flux de știri și poate decide să cumpere un produs sau un serviciu. Șansele companiei de a găsi și reține noi clienți cresc prin intermediul rețelelor de socializare. Specialiștii în marketing folosesc rețelele sociale pentru a îmbunătăți ratele de conversie, oferă acces și interacțiuni cu clienții noi, recent și vechi. Prin partajarea postărilor de blog, imagini, videoclipuri sau comentarii pe rețelele sociale, mai mulți oameni vor vizita site-ul companiei și vor deveni clienți. Dar nu există o singură abordare a strategiilor de marketing: fiecare afacere este unică și are o țintă diferită demografică, istorică și piață competitivă. Deoarece companiile de rețele sociale doresc ca companiile să plătească pentru publicitatea lor, companiile restricționează adesea numărul de companii de acoperire primite prin postări neplătite. De exemplu, dacă o companie are 500 de urmăritori, este posibil ca urmăritorii să nu primească toți aceeași postare. Natura în evoluție a rețelelor sociale face ca este dificil să ții pasul cu schimbările și, de asemenea, influențează rata de succes în marketing a unei companii.

Facebook, Instagram, Facebook Messenger și Twitter sunt cele mai populare site-uri de rețele sociale din Statele Unite și, de asemenea, din Europa. Alții includ Pinterest, Tumblr, Snapchat,

TikTok și YouTube, WhatsApp, Messenger by Google și Tumblr. LinkedIn este un alt site popular, care ajută la conectarea profesioniștilor cu colegii de muncă, contactele de afaceri și angajatorii. Facebook rămâne cea mai mare și cea mai populară rețea de socializare, cu 2,91 miliarde de oameni utilizând platforma lunar, la 31 decembrie 2021. Figura 2 arată numărul de utilizatori pe platforme.

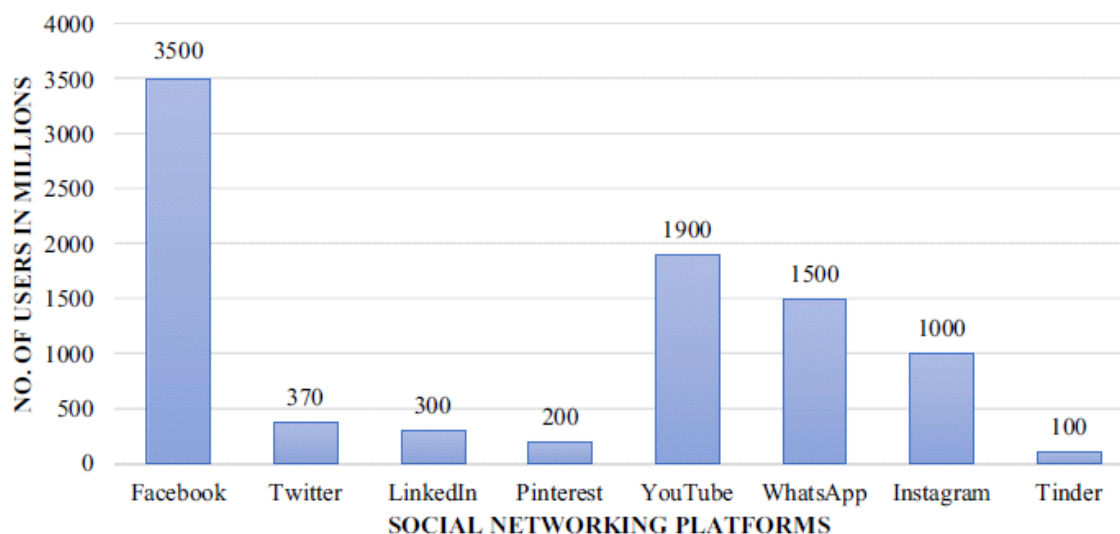


Figura 2: Numărul de utilizatori pe platforme (<https://www.dreamgrow.com/top>)

Funcționalitatea rețelelor sociale

Rețelele sociale se bazează pe dezvoltarea și menținerea relațiilor personale și de afaceri folosind tehnologia prin utilizarea site-urilor de rețele sociale. Aceste site-uri permit oamenilor și corporațiilor să se conecteze între ele, astfel încât să poată dezvolta relații și să poată împărtăși informații, idei și mesaje.

Membrii familiei care sunt departe ar putea rămâne conectați prin intermediul rețelelor sociale personale, cum ar fi Facebook, și pot împărtăși fotografii și trimite alte mesaje din viața lor. Oamenii se pot conecta și cu alții (străini) care împărtășesc aceleași interese. Indivizii se pot găsi unul pe altul prin faptul că sunt membri în grupuri, pe liste și prin utilizarea hashtag-urilor.

Dar există și dezavantaje legate de rețelele sociale, inclusiv răspândirea dezinformării și costul ridicat al utilizării și menținerii profilurilor rețelelor sociale.

Fiecare rețea socială servește de obicei o anumită utilizare, dar funcționalitatea acestor platforme este similară și poate fi clasificată în trei tipuri principale:

- Funcțiile de rețea servesc la stimularea relațiilor sociale între utilizatori în cadrul platformelor virtuale. În special, ele oferă funcționalitate pentru construirea și

Întreținerea graficului rețelei sociale.

- Funcțiile de date sunt responsabile pentru gestionarea conținutului furnizat de utilizator și a comunicațiilor între utilizatori. Varietatea contribuie la îmbunătățirea (extinsă) interacțiunii utilizatorilor și face platforma mai atractivă.
- Funcțiile de control al accesului urmăresc să implementeze măsurile de confidențialitate definite de utilizator și să restricționeze accesul neautorizat la datele și informațiile furnizate de utilizator. Figura 3 prezintă funcționalitatea oferită de o platformă tipică de rețea socială virtuală și oferă mai multe detalii (Cutillo et al. 2010).

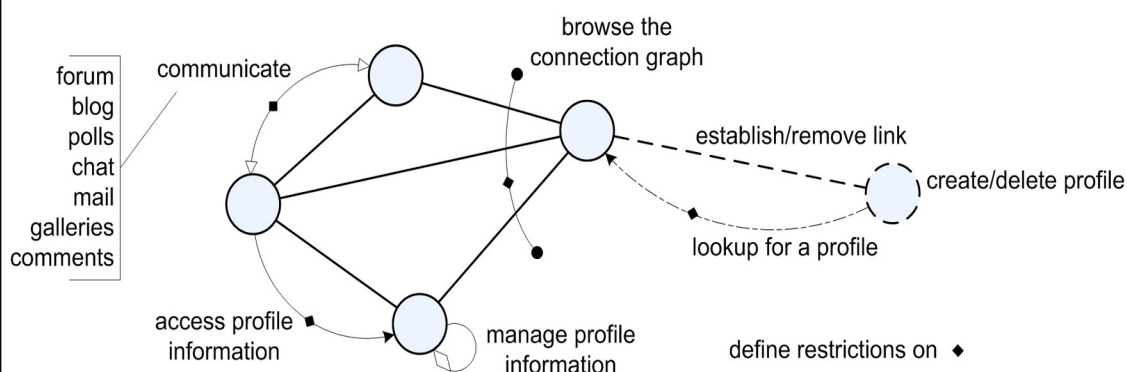


Figura 3: Funcționalitatea principală a unei platforme tipice de rețele sociale (<https://hal.archives-ouvertes.fr/hal-00687145>)

Site-urile de rețele sociale pot fi clasificate în „conexiuni sociale”, „partajare multimedia”, „profesionale” și „foruri de discuții” (Figura 4 Jain și colab., 2021)

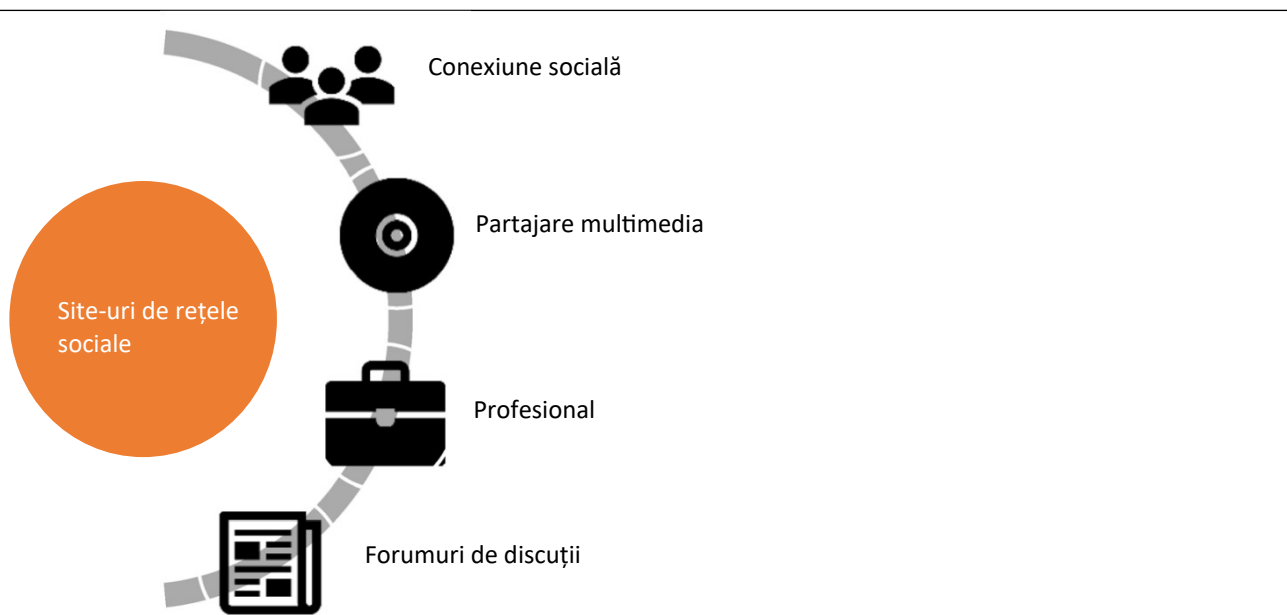


Figura 4: Site-uri de rețele sociale (Jain et al, 2021)

Avantajele și dezavantajele rețelelor sociale

Rețelele sociale au capacitatea de a afecta atât indivizii, cât și corporațiile – atât în mod pozitiv, cât și negativ și, prin urmare, este important să luăm în considerare avantajele și dezavantajele utilizării unor astfel de site-uri de social media..

Avantaje

Rețelele sociale le permit persoanelor să păstreze contactul cu familia și prietenii pe care altfel nu ar fi posibil din cauza distanței sau a pierderii contactului. Oamenii se pot conecta și cu alți indivizi care împărtășesc aceleași interese și pot dezvolta noi relații.

Rețelele sociale permit companiilor să se conecteze cu clienți noi și existenți. Companiile pot folosi, de asemenea, rețelele sociale pentru a crea, promova și crește gradul de conștientizare a mărcii. De asemenea, se bazează pe recenzii și comentarii făcute de clientela lor importantă pentru brand. Poate crește vânzările și un clasament mai ridicat în motoarele de căutare.

Rețelele sociale pot ajuta la stabilirea unui nou brand. O companie poate folosi rețelele sociale pentru a-și demonstra clienților un nivel ridicat de servicii și pentru a îmbunătăți produsele și relațiile cu consumatorii. De exemplu, dacă un client se plânge de un produs sau serviciu pe Twitter, compania își cere scuze și ia măsuri pentru a îmbunătăți situația.

Dezavantaje

Rețelele sociale pot contribui la răspândirea dezinformării. Sahoo și Gupta, 2020, au descoperit că dezinformarea este cu 70% mai probabil să fie partajată decât informațiile corecte pe Twitter.

Rețelele pe rețelele de socializare pot avea un impact negativ asupra companiilor. Critica la adresa unui brand s-a răspândit foarte repede pe rețelele de socializare. Acest lucru are dezavantaje pentru departamentul de relații publice (PR) al unei companii.

Rețelele sociale în sine sunt gratuite, dar construirea și menținerea unui profil de companie necesită ore de muncă și costuri în fiecare săptămână. Afacerile au nevoie de mulți adepți înainte ca o campanie de marketing pe rețelele sociale să înceapă să genereze o rentabilitate pozitivă a investiției (ROI). De exemplu, trimiterea unei postări la 15 urmăritori nu are același efect ca trimiterea postării către 15.000 de urmăritori.

Securitate și confidențialitate în rețelele sociale

Informațiile partajate în rețelele sociale și media se răspândesc foarte rapid, ceea ce face atractivă pentru atacatori să le câștige. Există probleme de securitate și confidențialitate legate de informațiile partajate de utilizator atunci când un utilizator încarcă conținut personal, cum ar fi fotografii, videoclipuri și audio. Atacatorul poate folosi în mod rău intenționat informațiile partajate în scopuri nelegitime.

Câteva amenințări diferite de securitate și confidențialitate și soluții existente care pot oferi securitate utilizatorilor rețelelor sociale sunt prezentate pe scurt.

Datorită utilizării intensive a tehnologiei, interacțiunile au fost extinse prin internet. Din păcate, lipsa de conștientizare a utilizatorilor cu privire la securitate și confidențialitate are potențialul de a duce la diferite atacuri cibernetice prin intermediul rețelelor sociale. Amenințările pe care utilizatorii le-au detectat de la începutul rețelelor sociale pot fi împărțite în trei categorii și anume, amenințări convenționale, amenințări moderne și amenințări vizate (Fig. 5, Jain și Gupta, 2018). Amenințările convenționale includ amenințările pe care utilizatorii le-au întâmpinat încă de la începutul rețelei sociale. Amenințările moderne sunt atacuri care utilizează tehnici avansate pentru a compromite conturile utilizatorilor, iar atacurile direcționate sunt atacuri care sunt vizate asupra unui anumit utilizator care pot fi comise de orice utilizator pentru diverse răzbunări personale.

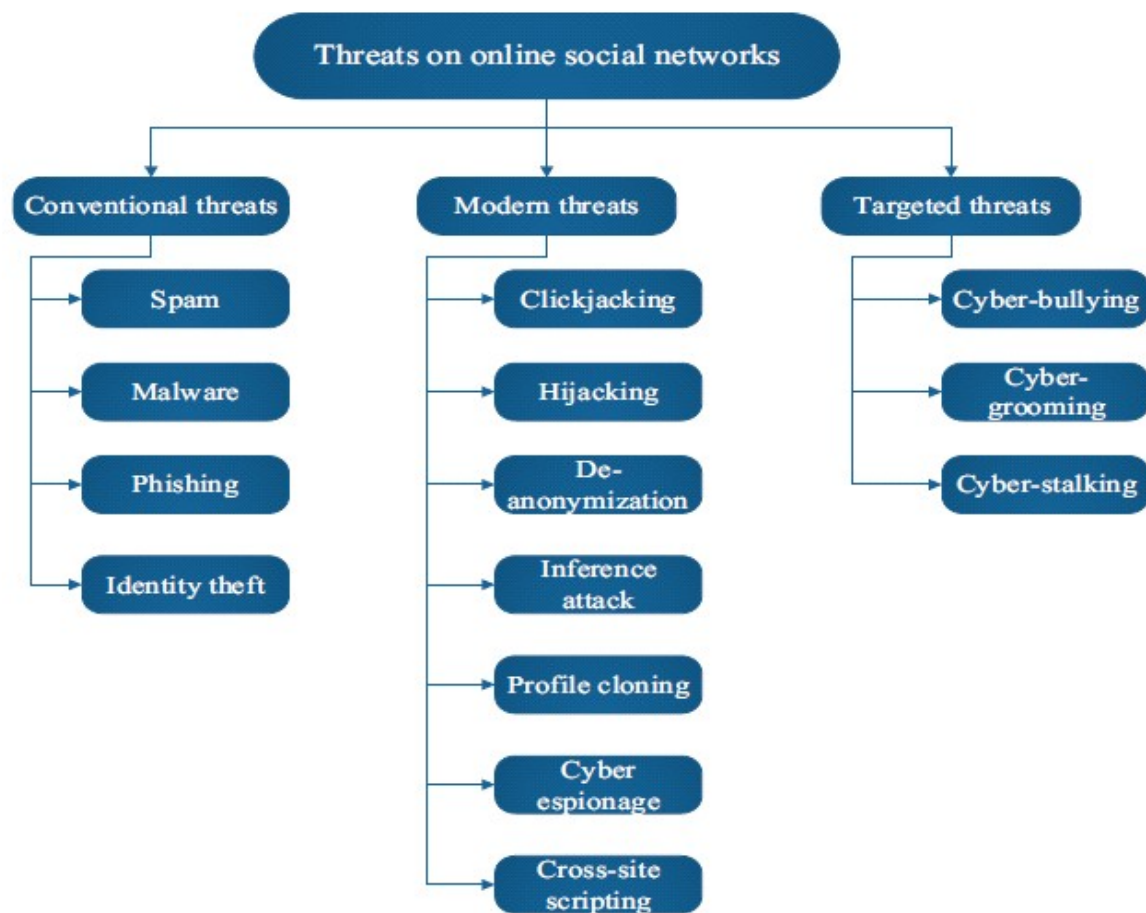


Figura 5: Clasificarea amenințărilor (Jain et al, 2018)

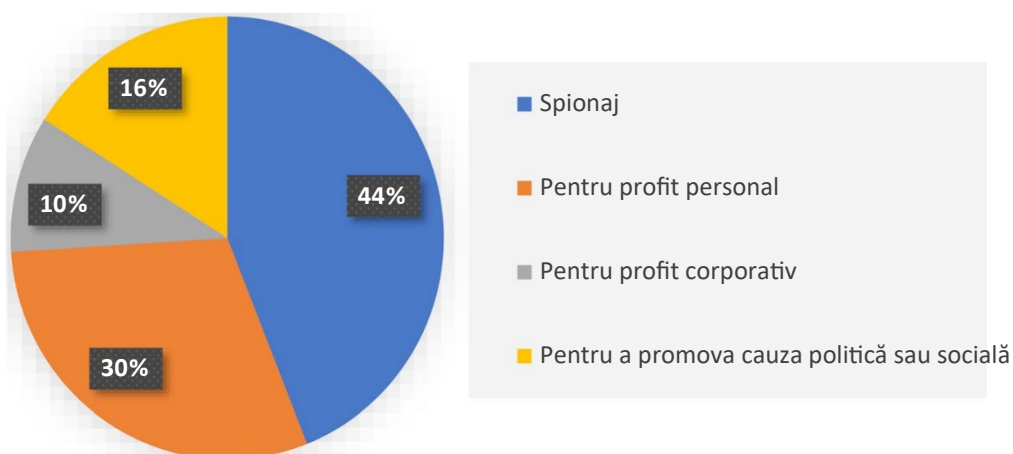


Figura 6: Cele mai multe tipuri de hacking în 2021 (Jain et al, 2021)

Soluții la amenințări

Cercetătorii din mediul academic și din industrii încearcă să găsească soluții pentru amenințările

din rețelele sociale pentru diferite tipuri de hacking, așa cum se arată în Figura 6. Soluții și unele abordări au fost propuse și ar putea fi clasificate în două grupe: soluții pentru operatori de rețele sociale și soluții academice (Jain et al, 2021). Figura 7 prezintă clasificarea. O scurtă descriere este prezentată mai jos.

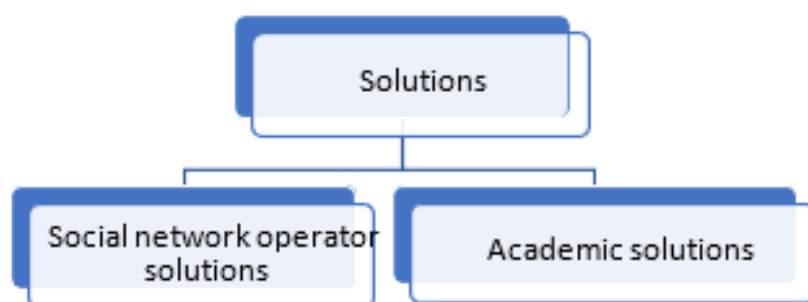


Figura 7: Clasificarea soluțiilor la amenințări (Jain et al, 2021)

Soluții pentru operatorii de rețele sociale

Mecanism de autentificare

Pentru a vă asigura că numai un utilizator legitim se conectează sau se înregistrează într-o rețea de socializare și nu într-un bot social, au fost propuse proceduri de autentificare precum CAPTCHA, autentificare cu mai mulți factori și identificare cu fotografiile unui prieten. De exemplu, rețelele sociale precum Twitter și Facebook folosesc principii de autentificare cu doi factori. Acest principiu folosește o parolă de conectare și un cod de verificare primit prin intermediul unui dispozitiv mobil. Acest lucru ajută la atenuarea riscului ca un cont să fie compromis și împiedică un atacator să deturneze un cont legitim și să posteze conținut rău intenționat.

Setări de securitate și confidențialitate

Multe site-uri de rețele sociale oferă setări de securitate și confidențialitate configurabile pentru a permite clientului să pună informații personale de la accesul nedorit al persoanelor din exterior sau al aplicațiilor. De exemplu, clientul Facebook își poate modifica setarea de securitate și poate selecta publicul (cum ar fi prietenii, prietenii prietenilor și toată lumea) din rețea, care își poate vedea detaliile, imaginile, postările și alte informații sensibile..

Raportați utilizatori

Rețelele sociale protejează oamenii de atacuri, oferind posibilitatea de a raporta orice formă de abuz sau încălcare a politicilor de către orice utilizator din rețeaua lor. De exemplu, dacă un utilizator vede ceva pe Facebook care corespunde sentimentelor persoanei, dar nu încalcă termenii Facebook, atunci utilizatorul poate utiliza un raport (linkuri) pentru a trimite un mesaj

celui care l-a postat, cerându-i să facă acest lucru. dați-l jos sau îndepărtați.

Când Facebook primește un raport de utilizator, acesta este revizuit și eliminat conform standardelor comunității Facebook.

Soluții bazate pe cercetare academică

Detectare phishing

Phishing-ul a îngrijorat confidențialitatea și securitatea multor aplicații web tradiționale, cum ar fi site-uri web, site-uri de rețele sociale, e-mailuri și bloguri. În consecință, au fost dezvoltate mai multe tehnici anti-phishing pentru a detecta atacurile de phishing. De exemplu, Aggarwal et al. a propus tehnica PhishAri pentru identificarea în timp real a atacurilor de phishing care au loc pe Twitter. A folosit funcții specifice Twitter, cum ar fi vârsta contului și numărul de urmăritori, pentru a detecta dacă tweetul postat este phishing sau sigur.

Detectarea hărțuirii cibernetice

Hărțuirea cibernetică este utilizarea mijloacelor electronice, cum ar fi e-mailurile, chat-urile, conversațiile telefonice și rețelele sociale online pentru a oprima o persoană. Spre deosebire de hărțuirea tradițională, hărțuirea cibernetică este un proces continuu menținut prin intermediul rețelelor sociale. Deși detectarea hărțuirii cibernetice este mai complexă decât detectarea limbajului rasist și a spam-ului, unii cercetători au încercat să-l detecteze folosind reprezentarea documentelor mai complexe și informații suplimentare despre victime și bătăuși. Tehnicile de învățare automată pot fi aplicate pentru a detecta hărțuirea cibernetică.

Clickjacking

Un sistem automatizat poate analiza paginile web pentru a proteja utilizatorul împotriva atacurilor de tip clickjacking. Este alcătuit dintr-un cod care poate detecta elemente care se suprapun pe care se poate face clic. Și pe lângă această soluție, au adoptat și instrumentul NoScript, care are inclusă o funcție anti-clickjacking..

Cyberstalking

Tehnicile de criptare sunt disponibile pentru dispozitivele pe versiunile recente de Android și iOS. Dacă un dispozitiv este furat, hoțul nu poate citi conținutul dacă criptarea este activată. În plus, orice încercare de a citi informațiile din memoria internă sau externă este împiedicată de existența unei parole a dispozitivului. Există diverse tehnologii care pot fi folosite împotriva urmăritorilor, cum ar fi blocarea cu amprentă a smartphone-ului.

Detectare spam

Un cadru numit Spam Spotter poate ajuta împotriva unui atac de spam pe Facebook. Se bazează pe sistemul inteligent de sprijin pentru decizii (IDSS). Acesta adună toate informațiile relevante din profilul utilizatorului cu ajutorul unui proces de decizie în IDSS și apoi le analizează prin maparea datelor utilizatorului la clasificarea unui profil de utilizator ca spammer sau legitim..

Programe malware

Cross Site Scripting Worms (worms XSS) sunt programe rău intenționate care se propagă prin vizitatorii unui site web hoping pentru a infecta alți vizitatori progresiv.

Viermele se propagă mai lent atunci când membrii își vizitează mai degrabă prietenii decât străinii. De asemenea, poate fi încetinit de natura grupată a rețelelor sociale.

Deși mediul academic a dezvoltat astfel de soluții inovatoare pentru a aborda măsurile de securitate în legătură cu securitatea rețelelor sociale, le lipsește implementarea și fezabilitate în lumea reală. Astfel, există o nevoie urgentă de a revizui în mod continuu și iterativ problemele de securitate din rețelele sociale, ținând cont de evoluțiile tehnologice..

Interdisciplinaritatea în rețelele sociale

Domeniul interdisciplinar care se referă la rețelele sociale este analiza rețelelor sociale (SNA) și include perspective din alte discipline ale științelor sociale, cum ar fi sociologia, antropologia, psihologia, comunicarea și altele. SNA face parte dintr-un domeniu interdisciplinar și mai mare responsabil de studierea tuturor tipurilor de rețele numite știința rețelelor, care include activități în fizică, informatică, știința datelor, biologie, inginerie, matematică și alte domenii. Relația dintre aceste câmpuri este prezentată în Figura 8 (https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html).

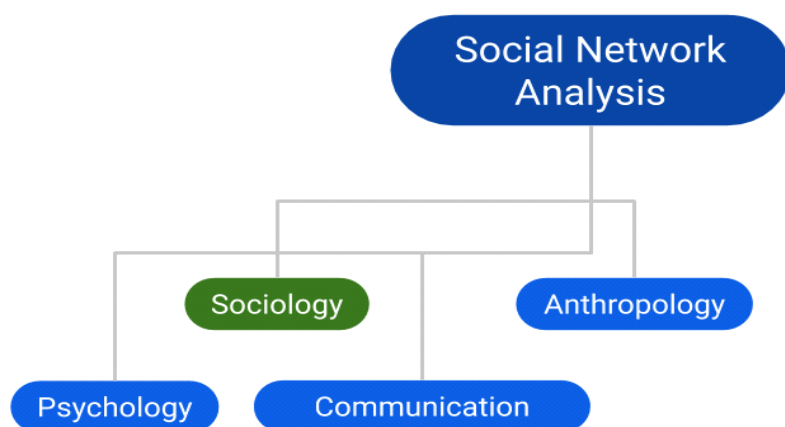




Figura 8: Relațiile dintre câmpurile din SNA (https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html)

Întrebări:

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

1. Rolurile rețelelor sociale
2. Site-uri de rețele sociale
3. Domenii interdisciplinare în legătură cu rețelele sociale

Atasamente:

1. Prezentare
2. Filme video

Referințe:

- Aggarwal A., Rajadesingan A & Kumaraguru P. (2012). PhishAri: automatic realtime phishing detection on twitter. eCrime Res. Summit, eCrime. 1–12.
- Ankit Kumar J., Somya Ranjan S. & Kaubiyal J. (2021). Data breach causes worldwide. URL: <https://www.statista.com/statistics/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/>
- Cutillo, A., Manulis, M. & Strute, T.(2010). Security and Privacy in Online Social Networks. EUROCOM. TU Darmstadt.
- Gupta B. & Sahoo, S. (2021). Online social networks security: principles, algorithm, applications, and perspectives. CRC Press.
- Jain A. & Gupta B. (2018). Detection of phishing attacks in financial and e-banking websites using link and visual similarity relation. Int J Inf Comp Secur 10(4):398–417.
- Jain, A., Sahoo, S.R. & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex Intell. Syst. 7, 2157–2177.
- Kangur, K. (2022). The 15 Biggest Social Media Sites and Apps. URL: <https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/>.
- Mislove A., Viswanath B., Gummadi K. & Druschel, P. (2010). You are who you know. In: Proceedings of the third ACM international conference on Web search and data mining—WSDM '10, 251.
- Rydstedt, G. (2018). Clickjacking – OWASP. URL: <https://owasp.org/www-community/attacks/Clickjacking>.



This work is licensed under CC BY-NC 4.0. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/4.0/>



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

Sahoo SR, Gupta BB (2020). Fake profile detection in multimedia big data on online social networks. *Int J Inf Comput Secur* 12(2–3), 303–331.