
AGENȚIA DE APĂRARE CIBERNETICĂ

Ghid de bune practici pentru utilizarea platformelor sociale și securizarea conturilor din cadrul acestora

Cuprins

Definiție

Termenul de social media definește un grup de instrumente digitale (site-uri, aplicații, platforme) care facilitează schimbul de idei, gânduri și informații și necesită doar un dispozitiv cu acces la internet.

Rețelele sociale oferă utilizatorilor o comunicare rapidă pentru a împărtăși conținut media, informații personale, documente, fotografii, videoclipuri, etc.

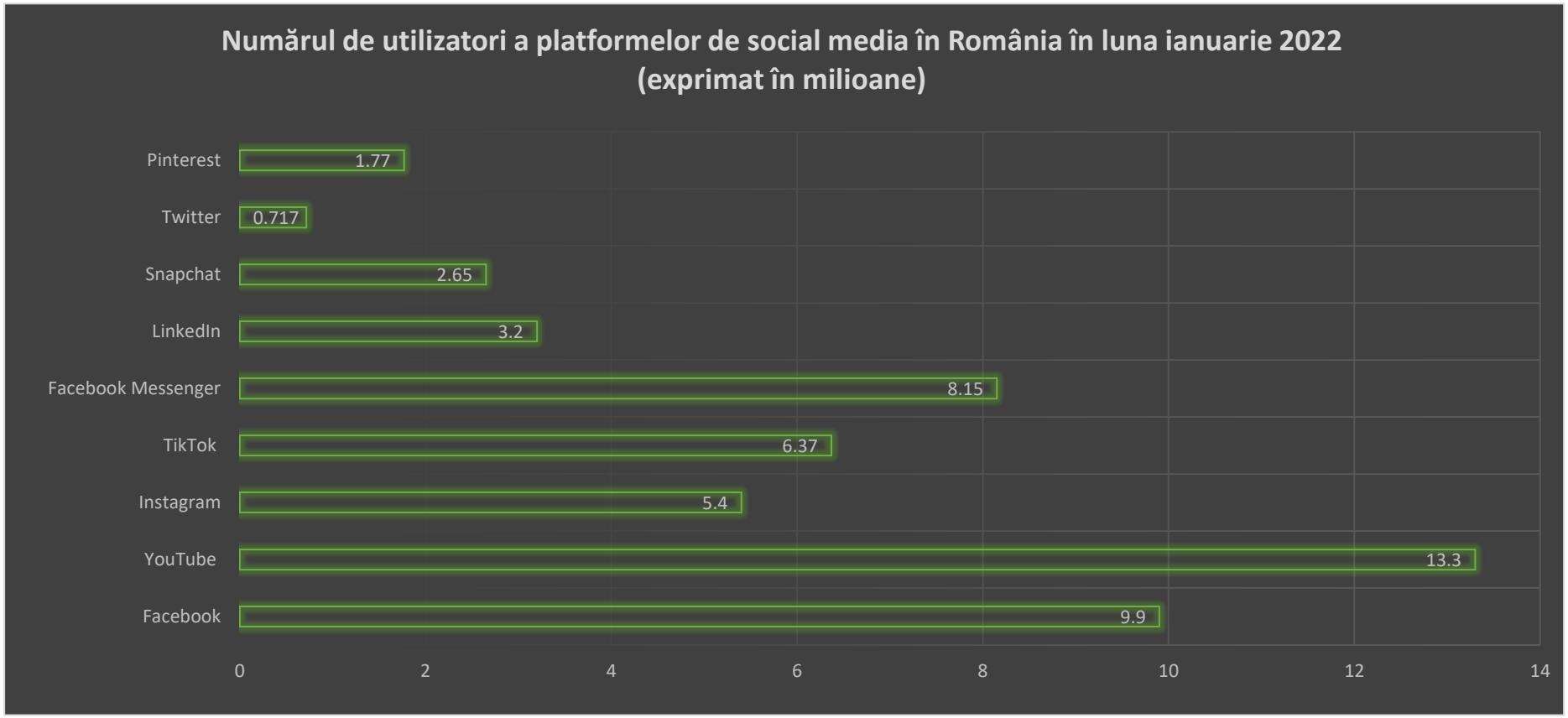
Blogurile, forumurile, rețelele sociale (LinkedIn, Facebook, Instagram, Snapchat, TikTok, etc), platformele cu conținut video (YouTube), serviciile de mesagerie (WhatsApp, Facebook Messenger, Skype, Mattermost, etc), jocurile online, etc sunt exemple de instrumente de social media.

Social Media în România

Devenit un trend la nivel global, peste jumătate din populația planetei este activă pe cel puțin o platformă de social media. Conform statisticilor, în medie, un utilizator normal petrece în fiecare zi aproximativ 145 de minute pe o astfel de platformă.

În România, platforma Facebook, fondată în anul 2004, a fost vârful de lance al conceptului de social media. Facebook a adus interacțiunea socială la un nou nivel, iar oamenii au fost imediat atrași. Acest lucru s-a văzut imediat în cifrele înregistrate. În ianuarie 2010, platforma înregistra 500.000 de conturi de utilizatori, iar un an mai târziu, numărul de conturi a ajuns la 2,4 milioane.

În prezent sunt 13,3 milioane de utilizatori ai platformelor de social media în România, echivalentul a 69,7% din populația totală a țării (19,08 milioane de oameni).



Beneficiile social media

Posibilități de comunicare 24/24

Platformele de social media oferă utilizatorilor un canal de comunicare disponibil 24 de ore din 24 și posibilitatea de a comunica cu o persoană, sau un grup de persoane, indiferent de locația geografică. Acest lucru facilitează schimbul de informații cu privire la diverse teme. Totodată, rețelele de social media pot fi folosite pentru a organiza diferite activități și evenimente, pentru a reuni grupuri de oameni cu interese comune sau pentru a lansa diverse campanii (de conștientizare a anumitor probleme sau de strângere de fonduri).

Divertisment

Rețelele de social media oferă posibilitatea de a lua parte la un eveniment dedicat divertismentului, precum piese de teatru sau spectacole de comedie în timp real. Platforme precum YouTube sau Twitch au încurajat ideea de a transmite astfel de activități, iar oamenii, îndeosebi tinerii, au folosit această oportunitate pentru a-și expune creațiile, gândurile și trăirile.

Posibilități de angajare

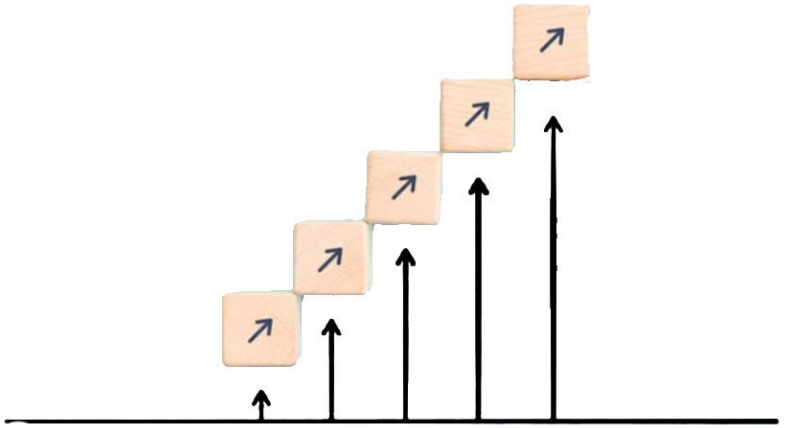
Odată cu evoluția tehnologică a fost revoluționat și sistemul de angajare al oamenilor în cadrul întreprinderilor sau companiilor. Multe companii își caută potențiali angajați prin intermediul rețelelor de social media, analizând profilurile acestora de pe platforme precum LinkedIn, Facebook sau Twitter.

Partajarea informațiilor și a cunoștințelor

Pe lângă celelalte avantaje, rețelele sociale mai oferă și o mare bază de cunoștințe pentru majoritatea subiectelor și problemelor existente. Cu ajutorul acestor platforme oamenii cer sfaturi sau împărtășesc rezolvările la diverse probleme din cotidian.

Dezvoltarea unei afaceri

La nivel de business, rețelele sociale pot oferi o promovare mult mai mare afacerii dezvoltate, iar produsele companiei pot fi aduse în atenția clienților într-un mod mult mai dinamic. Totodată, noua companie poate monitoriza mult mai ușor dorințele și necesitățile utilizatorilor și poate crea oferte personalizate fiecărui client.

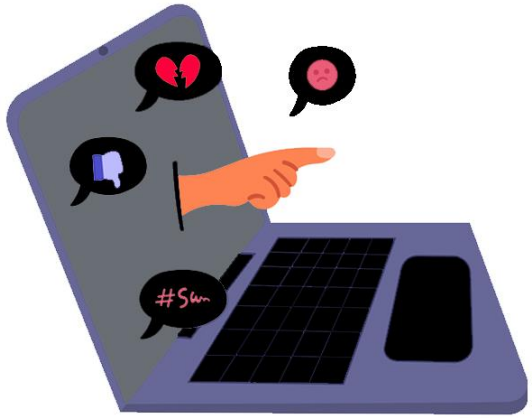


Riscurile din spatele social media

Pentru a maximiza beneficiile oferite de platformele de social media, utilizatorii ar trebui să recunoască și să ia măsurile adecvate împotriva riscurilor asociate utilizării acestora.

Feedback negativ, hărțuire și cyberbulling

Oamenii folosesc platformele de social media pentru a distribui conținut, dar și pentru a-și exprima nemulțumirea cu privire la o postare, o imagine sau un videoclip anume. De asemenea, aceste platforme sunt folosite de către persoanele publice pentru a-și ține la curent urmăritorii cu ultimele acțiuni întreprinse. Cu toate acestea, nu toate persoanele abonate la paginile respective apreciază acțiunile întreprinse și drept consecință apar comentariile negative și mesajele de hărțuire la adresa persoanei respective.



În cazul în care vă simțiți agasat sau amenințat de anumite persoane nu uitați că puteți să le restricționați accesul la postările dumneavoastră sau le puteți bloca contul. Totodată, aveți posibilitatea de a raporta aceste conturi sau diverse postări din motive precum: cont fals, nume fals, informații false, conținut neadecvat, instigare la violență, etc.

O categorie aparte care trebuie monitorizată atent sunt copiii. Mesajele de intimidare pe care aceștia le pot primi îi pot afecta profund din punct de vedere emoțional și le pot provoca traume. Este recomandat ca aceștia să nu fie lăsați singuri să navigheze în Internet, cel puțin la început, și să le fie explicate pe larg pericolele pe care le pot întâlni în spațiul cibernetic.

Furt de identitate

Lipsa confidențialității este una dintre caracteristicile platformelor de social media. Utilizatorii ar trebui să acorde o deosebită atenție informațiilor pe care aleg să le posteze deoarece sunt foarte multe persoane rău intenționate care pot prelua aceste date pentru a le folosi în diverse scopuri.

Zi de zi sunt create zeci de conturi false, care arată identic cu cele originale, însă în urma unei analize amănunțite se dovedesc a fi nelegitime. Spre exemplu, compania Facebook declara în anul 2020 că numărul conturilor false create pe această platformă este estimat undeva la 1,5 miliarde, aproximativ 5% din numărul total de conturi create.

Multe persoane rău intenționate folosesc diferite tehnici de inginerie socială pentru a câștiga încrederea unei persoane pentru ca, ulterior, să obțină acces la informațiile personale ale acesteia. Fiți precaut atunci când primiți mesaje, deoarece se poate întâmpla ca uneori, conturile prietenilor sau cunoștințelor să fie compromise. Dacă o conversație vi se pare ciudată, iar interlocutorul dumneavoastră devine foarte curios despre viața dumneavoastră personală sau vă solicită din senin o sumă de bani, este foarte posibil ca acel cont să fie compromis și o persoană rău intenționată să se folosească de el în scopuri ilicite.

Informații false

Când vine vorba de răspândirea unei informații, rețelele de social media sunt un instrument puternic, atât pentru companii, cât și pentru persoanele fizice. Cu toate acestea, nu toate informațiile încărcate sunt reale. Termenul de informații false sau fake news se referă la dezinformări care acoperă o gamă variată de subiecte precum sănătatea, mediul, economia, politica etc.

Sunt mai multe tipuri de informații false. Acestea se pot clasifica în:

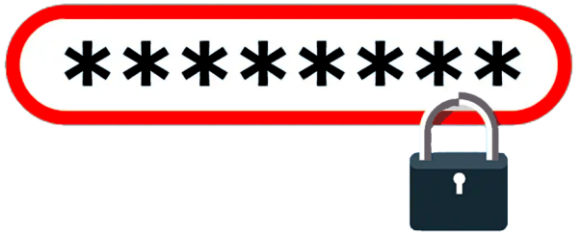
- **Clickbait** – Sunt articole care folosesc titluri senzaționale pentru a atrage atenția a cât mai mulți cititori, astfel încât venitul din reclame al site-ului web să fie cât mai mare. De cele mai multe ori aceste articole prezintă informații eronate sau lipsite de acuratețe.
- **Propagandă** – Reprezintă articolele care sunt create pentru a induce în mod deliberat publicul în eroare prin promovarea unui punct de vedere părtinitor sau pentru o anumită cauză politică.
- **Satiră / Parodie** – Sunt foarte multe site-uri web și conturi pe rețelele sociale care publică știri false doar pentru amuzament.
- **Jurnalism neglijent** – Uneori, reporterii sau jurnaliștii pot publica o poveste cu informații neverificate care pot induce publicul în eroare.
- **Titluri false** – Acest tip de știri se pot răspândi rapid pe platformele de social media, acolo unde sunt afișate doar titlurile sau mici fragmente scoase din context existent în articol.
- **Știri părtinitoare** – Multe persoane sunt atrase de știri sau povești care le confirmă propriile convingeri, iar știrile false sunt modul ideal de distribuție a acestor informații. Fluxurile de știri afișate pe platformele de social media sunt personalizate în funcție de căutările recente ale utilizatorilor.

Cum putem identifica informațiile false?

- **Analizați conținutul** – Verificarea sursei poveștii sau a site-ului reprezintă primul pas pentru a combate răspândirea de informații false. În mod normal, pentru transparență, la secțiunea Despre a unui site se pot găsi mai multe informații despre autor, scop etc.
- **Treci dincolo de titlu** – Se recomandă parcurgerea întregului articol deoarece multe știri folosesc titluri senzaționale sau șocante pentru a atrage atenția. Adesea, titlurile de povești false folosesc majuscule sau semne de exclamare
- **Verificați informația și din alte surse** – Pentru a fi sigur de corectitudinea informației, verificați dacă sunt și alte știri despre același subiect sau alte trusturi de presă care prezintă această informație. Dacă există surse citate în cadrul articolului verificați dacă acestea sunt de încredere.
- **Acordați atenție datelor cronologice** – De foarte multe ori, informațiile false conțin date incorecte sau modificate din punct de vedere cronologic. De asemenea, ar putea fi utilă verificarea datei publicării articolului, deoarece știrea prezentată ar putea fi de fapt un eveniment desfășurat cu mult timp în urmă.
- **Prea amuzant pentru a fi adevărat** – Site-urile satirice sunt populare în mediul online și de multe ori nu este clar dacă povestea prezentată este reală sau este o glumă / parodie. Verificați dacă site-ul accesat este cunoscut pentru satiră.

Îmbunătățirea securității conturilor de social media

Setări de confidențialitate și complexitatea parolei



Majoritatea utilizatorilor folosesc setările implicite de confidențialitate atunci când își creează un nou profil sau o nouă pagină. Potrivit unei statistici realizate în anul 2017 de către Statista, utilizatorii au declarat că nu au încredere că setările de confidențialitate alese funcționează așa cum ar trebui.

Pentru un plus de securitate este necesară setarea unei parole complexe și unice pentru fiecare cont din mediul online. Aceasta ar trebui să fie formată din cel puțin 10 caractere și să cuprindă litere mari, litere mici și caractere alfa-numerice. Totodată, nu este recomandată includerea informațiilor personale, precum numele părinților, data nașterii sau numele animalului de companie.

De asemenea parola ar trebui schimbată periodic și, acolo unde este posibil, introducerea autentificării multi-factor. Dacă utilizați un dispozitiv partajat cu alte persoane pentru a accesa platformele de social media, se recomandă să vă deconectați de fiecare dată când nu mai utilizați sistemul, utilizând funcția Sign out.

Aplicații third-party vulnerabile

Chiar și atunci când conturile de social media sunt securizate corespunzător, acestea pot fi compromise prin intermediul unor aplicații third-party nesigure instalate pe dispozitiv. Se recomandă descărcarea și instalarea aplicațiilor doar din surse sigure, precum și actualizarea în mod constant a sistemului de operare și a aplicațiilor instalate.

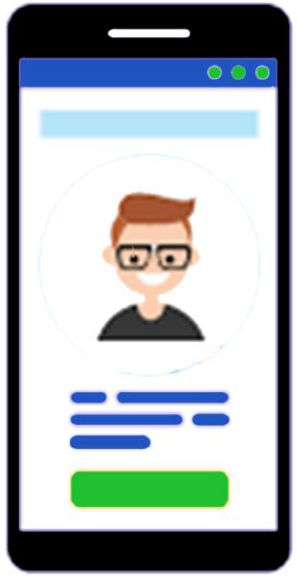
Atacuri malware, scam și phishing

Înșelătoriile și atacurile malware sunt foarte frecvente în cadrul platformelor și rețelelor de social media. Fie că vorbim de campanii de phishing sau de infectarea dispozitivului prin simpla accesare a unui site web, toate aceste acțiuni au de cele mai multe ori același scop și anume furtul credențialelor de autentificare, a datelor bancare ale utilizatorilor sau alte informații private.

Geotagging

Funcția de geotagging este o caracteristică implementată pe majoritatea dispozitivelor mobile. Aceasta constă în adăugarea datelor de identificare geografică în cadrul tuturor fotografiilor, videoclipurilor sau mesajelor text realizate. Menținerea activă a acestei funcții poate duce la încălcarea confidențialității, deoarece poate dezvălui locația utilizatorilor în timp real, oferind astfel informații precum adresa exactă a locuinței sau a locului de muncă.

Conștientizarea riscurilor de imagine din spațiul social media



Este ușor ca postările din cadrul platformelor de social media să devină virale. Audiența, sau oamenii care urmăresc aceste postări, analizează atent conținutul. Cu toate acestea, dacă nu ești atent la conținutul încărcat, poți ajunge să te faci de rușine și să fii pus într-o situație mai puțin plăcută.

Un alt lucru important este capacitatea de a identifica rapid mesajele de tip spam, atacurile de tip phishing sau alte amenințări de securitate și raportarea acestora autorităților competente. Limitați grupul de audiență la un cerc de cunoscuți. Acceptați sau trimiteți cereri de conectare / prietenie doar persoanelor pe care le cunoașteți.

Analizați cu atenție informațiile pe care doriți să le încărcați în mediul online deoarece ulterior acestea nu vor mai putea fi șterse. Chiar dacă site-ul sau platforma utilizată oferă opțiunea de a șterge datele încărcate, copiile de rezervă generate automat vor păstra aceste informații, utilizatorul nemaiavând acces la gestionarea acestora.

Securizarea conturilor create în cadrul platformelor de social media

Fiecare dintre noi este responsabil pentru securizarea conturilor personale sau pentru postările din mediul online. Totuși pentru o mai bună securitate se recomandă securizarea conturilor urmând specificațiile fiecărei platforme:

Facebook - https://www.facebook.com/help/213481848684090

Instagram - https://help.instagram.com/369001149843369

TikTok - https://www.tiktok.com/safety/en-us/privacy-and-security-on-tiktok/

Pinterest - https://help.pinterest.com/en/article/protect-your-account

Twitter - https://help.twitter.com/en/safety-and-security/account-security-tips

Snapchat - https://support.snapchat.com/en-US/a/safety-tips-resources

Youtube - https://support.google.com/youtube/answer/9701986?hl=en

LinkedIn - https://www.linkedin.com/help/linkedin/answer/66/managing-your-account-and-privacy-settings-overview?lang=en

Referințe

https://www.investopedia.com/terms/s/social-media.asp

https://www.webroot.com/us/en/resources/tips-articles/online-activities-internet-security

https://blog.loomly.com/social-media-risks/

https://www.doads.ro/cele-mai-utilizate-retele-sociale-in-romania-2020/

https://datareportal.com/reports/digital-2022-romania?rq=social%20media%20in%20romania

https://www.financierworldwide.com/risks-associated-with-use-of-social-media#.Yqwa7HZBxPY

https://businessdegrees.uab.edu/blog/social-media-risks/

https://www.webfx.com/social-media/learn/social-media-marketing-advantages-and-disadvantages/

https://www.webwise.ie/teachers/what-is-fake-news/

Agenția de Apărare Cibernetică