AUTORITATEA DE SUPRAVEGHERE FINANCIARĂ

Utilizator frecvent de SOCIAL MEDIA?

Facebook | Instagram | TikTok

Nu ești în social media, nu exiști

Conform statista.com, numărul de profile social media din România în 2022 a fost de 14,7 mil., cele mai populare fiind Facebook (12,5 mil. utilizatori) și Youtube (13 mil. utilizatori). Instagram are peste 5,6 mil. utilizatori. Alte platforme social media utilizate sunt TikTok, LinkedIn, Twitter, Reddit ș.a.

Comunicarea în mediul digital rapid, ușor accesibil, atrăgător şi având costuri reduse a permis dezvoltarea new media – un spaţiu de comunicare publică şi de marketing, scopul fiind acela de a câştiga notorietate, bani sau influenţă.

FINsafe în social media

1. Mediul digital conține riscuri care, odată produse, te pot costa bani. Prin social media poți fi supus acestor riscuri
2. Social media este un canal prin care poți fi abordat de fraudatori sau scameri
3. Afectarea siguranţei tale financiare în social media poate fi şi din cauza unor înşelăciuni. Aici, lucrurile şi persoanele nu sunt neapărat ce par a fi.

Educație financiară pentru social media

Dacă ești utilizator de social media atunci este important să înțelegi că acest spațiu, desi este virtual, are și el riscurile sale și trebuie utilizat rațional. Chiar dacă la o primă vedere prezența în social media nu costă nimic, totuși s-ar putea ca pe termen lung, dacă nu ești atent, să coste. Spațiul larg al internetului (world wide web) are și avantaje dar și permite tuturor conectarea, cu o viteză inimaginabilă și posibilitatea creării unei imagini total diferite de realitate. Nu degeaba se cheamă „avatar" poza pe care o poți avea pe internet – aici te poți transforma în oricine …

Ce este social media?

Social media = tehnologii digitale interactive, canale de comunicare, platforme web care permit crearea și distribuirea către public/comunități de informații, idei, interese, lucrări de autor (în orice formă), știri și alte forme de conținut.

- utilizatorul urmărește interactivitatea și inter-conectivitatea oferită de platforma aleasă
- comerciantul o folosește în scopuri de marketing/publicitate pentru a ajunge la un număr mai mare de posibili consumatori (folosind algoritmii specifici și bazându-se pe tehnici de persuasiune)

- comunități virtuale (persoane cunoscute sau necunoscute de utilizator).
- conținutul este generat și/sau controlat de utilizator.
- sunt facilitate relațiile inter-personale, profesionale și comerciale.
- conectează utilizatorii cu grupuri, postări, furnizori de diferite servicii, idei, știri etc. – agregator de conținut/informații.
- tehnologiile folosesc algoritmi de „împerechere" a informației – cauți o informație pe Google și ți se furnizează ca publicitate pe social media.

Educație financiară digitală?

Nu poți vorbi în ziua de astăzi despre educație financiară fără a avea în discuție și elemente digitale, piața financiară și accesul la instrumente, produse și servicii financiare fiind bazate pe o relație digitală a consumatorului cu banii săi, indiferent de forma efectivă a banilor: carduri, asigurări, investiții bursiere, fonduri de investiții sau de pensii. Fiecare dintre noi suntem consumatori în fiecare zi: folosim cardul, avem o asigurare obligatorie, poate și una facultativă, suntem participanți la pensia administrată privat Pilon II, poate și la cea facultativă Pilon III, ne dorim să fim sau suntem investitori, nevoia de a valorifica pe termen scurt sau lung economiile. Fix în acest moment intervine și nevoia de a cunoaște mai mult despre mediul digital și cum ne protejăm financiar propriul portofel.

Securitatea cibernetică este o sintagmă care poate părea destul de pretențioasă, dar în realitate ea reprezintă modul în care ne protejăm telefoanele și calculatoarele personale de atacuri ale unor sisteme malițioase care au ca intenție furtul de date sau frauda. Educația pentru securitate cibernetică a unei persoane nu se referă doar la utilizarea unui antivirus care este destinat protecției sistemului informatic de pe dispozitivele mobile folosite, sau la un comportament prevăzător care ne învață să nu deschidem atașamente de la emailuri necunoscute și să nu folosim USB-uri neidentificate, ci și la cunoașterea unor practici și pericole digitale, vitală pentru securitatea financiară personală. pericolele cibernetice s-au diversificat odată cu dezvoltarea lumii digitale.

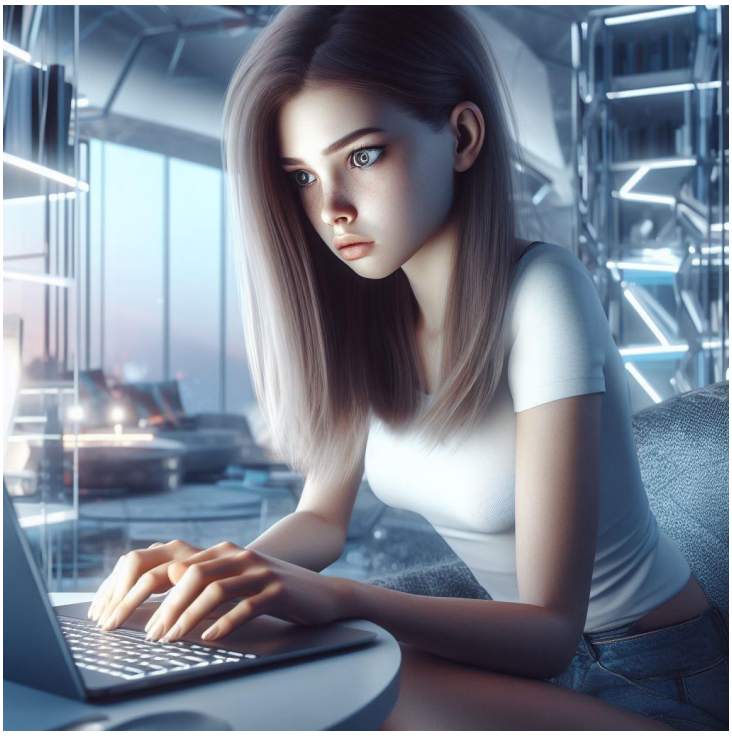
dacă știi,

te poți păzi

Fraudele cibernetice

- cyber-crime (care include persoane care țintesc sistemele informatice pentru a obține un câștig financiar sau pentru a cauza o perturbare a sistemului).
- cyber-attack (implică colectarea de informații cu caracter personal).
- cyber-terrorism (menit să compromită sistemele electronice pentru a cauza panică).

Dar cum obțin atacatorii controlul asupra sistemului unui calculator sau telefon personal?



Malware

Malware-ul este un program maliţios, un software creat cu scopul de a distruge sau strica funcţionarea unui calculator sau telefon. Cel mai adesea, malware-ul este distribuit prin emailuri care au ataşamente sau linkuri sau prin accesarea diferitelor ferestre pop-up apărute în timpul navigării pe internet sau a folosirii unor aplicaţii.

Atacurile malware sunt extrem de diversificate în prezent, afectând zilnic milioane de persoane şi sisteme.

Numărul fraudelor în mediul digital a crescut accelerat în ultimii ani, fiind favorizat de utilizarea tot mai largă a internetului şi aplicaţiilor mobile.

Tipuri de malware:

- viruși – programe care au capacitatea de a se auto-replica pentru a șterge sau infecta fișiere, conducând la blocarea funcționării unor aplicații sau a dispozitivelor; virușii se răspândesc între dispozitive (ex. două dispozitive cuplate sunt telefonul şi calculatorul, dar şi prin ataşamente transmise prin email, social media ș.a.); ei pot afecta dispozitivul până la pierderea completă a datelor sau distrugerea sistemului;
- viermi – nu provoacă daune directe unui sistem, dar scopul lor este de a se multiplica şi a se răspândi în dispozitiv sau în rețea, având ca obiectiv obținerea de informații;
- troiani – pot colecta date din calculator (ex. parole salvate), ei fiind ascunşi în programe care par inofensive; aceste software-uri dau acces hackerilor la sistem pentru furt de date personale, financiare etc.;
- spyware – programe care înregistrează ce face utilizatorul (ex. datele de identificare de la o aplicație financiară); software-ul va spiona ascuns în fundal activitatea dispozitivului (navigare internet, introducerea de parole etc.) şi va colecta informații (parole, detalii financiare, emailuri), transmițând informațiile adunate unui utilizator la distanță; poate instala fără permisiune şi alte malware-uri;
- ransomware – programe care blochează accesul la fişiere şi informații (prin criptare), sub amenințarea ştergerii lor dacă nu este plătită o recompensă; are capacitatea de a se răspândi rapid şi de a provoca daune costisitoare; scopul său este de a aduce profit;
- botnets – rețele de calculatoare infectate cu malware care sunt folosite de atacatori fără permisiunea proprietarilor pentru diferite acțiuni online;

Semne ale infectării malware

Apariţia pe dispozitiv a unor aplicaţii suspecte (fişiere, aplicaţii, extensii), pe care nu le recunoşti sau manifestarea ciudată a unor aplicaţii (se deschid/ închid aleatoriu).

Schimbarea setărilor de securitate ale dispozitivului, browserului sau aplicaţiilor fără a fi solicitate de tine.

Scăderea vitezei dispozitivului sau browserului, blocarea/închiderea frecventă a dispozitivului, supraîncălzirea dispozitivului sau descărcarea rapidă a bateriei.

Apariţia unor mesaje (email, text) neobişnuite care ţi se atribuie ca destinatar (dar nu tu le-ai trimis).

Apariţia unor plăţi solicitări de plată sau a unor plăţi efectuate suspecte, precum facturi nejustificat de mari la utilităţi, magazine etc.

- adware – programe de publicitate care sunt folosite pentru distribuirea de malware; scopul lor nu este neapărat de a produce daune, ci mai ales să obţină bani; software-ul este bazat pe publicitate agresivă, adică afişează reclame de tip banner sau pop-up pe diferite site-uri accesate sau aplicaţii;
- keylogging – procese de urmărire a tastelor apăsate, scopul fiind de a obţine parole sau de a observa comuncaţii private;
- SQL injection – interogări de limbaj structurat (SQL) folosite pentru a lua controlul şi a fura date dintr-o bază de date;
- fileless malware – deşi nu instalează nimic iniţial, sunt programe care aduc schimbări fişierelor native dintr-un sistem de operare; pentru că sistemul de operare recunoaşte fişierele ca fiind legitime, un astfel de atac nu va putea fi identificat de antivirus şi de aceea el este de 10 ori mai primejdios decât un malware tradiţional;
- rootkits – programe care permit hackerilor controlul de la depărtare asupra dispozitivului victimei, cu toate privilegiile administratorului; ele pot fi găsite în aplicaţii, nuclee, hipervizori sau firmware şi se răspândesc prin phishing, ataşamente, downloadări maliţioase sau fişiere compromise primite; mai pot ascunde şi alte tipuri de malware (ex. keylogging);
- wiper malware – un wiper are un sigur scop: de a șterge datele utilizatorului fără ca acestea să mai poată fi recuperate și fără a avea posibilitatea de a observa intruziunea, slăbind capacitatea victimei de a răspunde; de regulă așa sunt atacate rețele publice sau companii;
- mobile malware – infectează dispozitivele mobile (ex. telefoane), fiind la fel de variate ca cele care atacă calculatoarele; sunt distribuite prin phishing, downloadare, accesarea linkurilor ș.a.

Phishing

Phishing-ul este o practică a atacatorilor cibernetici (social engineering) prin care este transmis (de cele mai multe ori) un email care pare a fi de la o sursă oficială, credibilă – o companie, o entitate financiară, o instituție ș.a. – fiind solicitate informații specifice, așa cum sunt parolele aplicațiilor financiare, datele cardurilor sau alte informații personale. Prin phishing ești îndemnat să dai click pe un link, să descarci un atașament sau să introduci credențialele tale într-un site.

Atacurile phishing uzuale nu au o țintă specifică. Dar atacurile spear phishing sunt făcute de hackeri care țintesc o anume persoană sau organizație. Un exemplu de astfel de atacuri sunt mailurile de la o instituție financiară sau clienții ei. Un alt exemplu este whaling, care țintește un profil special (celebritate, manager, persoană publică), cu scopul de a găsi informații sau poze utilizabile apoi în cereri de recompensă. În angler phishing, scammerii pretind că sunt profile de rețele sociale de servicii pentru consumatori și încearcă să te convingă să le transmiți datele tale de conectare.

un mesaj în social media este la fel ca un email

Spam-ul este echivalentul electronic al unui email de tip junk sau a flyerelor publicitare găsite în cutia poștală, adică o corespondență nesolicitată care poate fi încadrată în categoria de marketing agresiv. Dar spam-ul poate fi mai mult decât enervant, el poate fi și periculos când este și phishing.

Diferența dintre cele două nu o poate face victima, deoarece este determinată de calitatea destinatarului: spamer sau cyber-criminal. Acesta din urmă are ca obiectiv banii celor care răspund la mesaj, obținând de la ei parole, numere de carduri, detalii de conturi și multe altele (fie direct, prin răspuns, fie indirect, prin infiltrarea unui cod malițios în calculatoarele sau dispozitivele mobile ale victimelor).

Spam-urile care promit premii sau câștiguri gratuite ar trebui să atragă atenția – nu există nimic gratuit!

Cum poți recunoaște un phishing

- îți cere informații sensibile.
- folosește un alt domeniu.
- conține linkuri care nu se potrivesc cu domeniul.
- include atașamente nesolicitate.
- nu este personalizat.
- folosește un limbaj incorect, cu greșeli de scriere/gramaticale.
- încearcă să inducă panică.
- este de la companii/persoane celebre.

Spoofing

Spoofing-ul este o activitate online frauduloasă prin care este falsificat un email, o identitate telefonică sau un profil de whatsapp, o pagină de internet etc., expeditorul real fiind ascuns sub o identitate falsă, de regulă a unei instituţii sau entităţi de încredere. Astfel sunt distribuite malware-urile sau phishingul, destinatarul încrezându-se în falsa identitate şi devenind victimă.

Baiting

Baiting-ul este un atac în care victimele sunt păcălite să dea informaţii în schimbul promisiunii că vor primi recompense. De exemplu, sunt anunţuri pop-up care oferă jocuri gratuite, muzică, filme şi odată accesat acest link dispozitivul este infectat cu un malware. Similar este şi Scareware, care apare sub forma unui pop-up în browser care anunţă că dispozitivul a fost infectat şi victima trebuie să facă click pe un buton care înlătură virusul sau asigură un antivirus gratuit. Dar aşa nu vei face decât să dai acces la un malware.

Smishing

Smishing-ul (adică phishing prin SMS) sunt SMS-urile prin care se primesc facturi false, linkuri care trebuie accesate pentru a revendica un premiu câştigat din „noroc”, linkuri care „trebuie” accesate pentru actualizarea de date la un cont financiar sau la un curier, linkuri în care se solicită actualizarea de date personale (cum ar fi transmiterea pozei cărţii de identitate) pentru o aplicaţie financiară sau a unei instituţii, linkuri care te conduc spre platforme false sau frauduloase de tranzacţionare ş.a.

Vishing-ul este phishing-ul cu voce, adică un atac prin telefon, adresat mai ales companiilor, acestea fiind sunate pentru a da date despre salariaţii săi. Scopul acestor atacuri este de a obţine de la victimă fie datele sale, fie accesul la aplicaţii financiare (evident, pentru a fi sustraşi banii victimei).

Atacurile care interceptează comunicaţii sau transferuri de informaţii (atacuri man-in-the-middle) între 2 persoane au scopul de a fura date şi pot apărea în cazul utilizării unor reţele wi-fi nesecurizate, când un atacator interceptează transmiterea unor informaţii personale care îi dau acces la date financiare.

Atacurile cibernetice denial-of-service (DoS) sunt cele care sunt construite pentru a împiedica conectarea utilizatorului la o reţea sau server, acestea apărând ca fiind afectate de un trafic intens. Ele provoacă instabilitatea unui sistem şi îl împiedică să îşi mai îndeplinească funcţiile.

Watering hole

Atacurile de tip watering hole sunt realizate de hackeri care infectează o pagină web pe care o vizitezi des. Atunci când o accesezi, automat este descărcat în dispozitiv un malware (drive-by-download) sau eşti direcţionat către o versiune clonă (cu scopul de a-ţi fura credenţialele). Pentru a te feri de acest tip de atac este folositor să foloseşti un manager de parole, acesta făcând imposibilă conectarea la un site de acest tip.

Ce te costă?

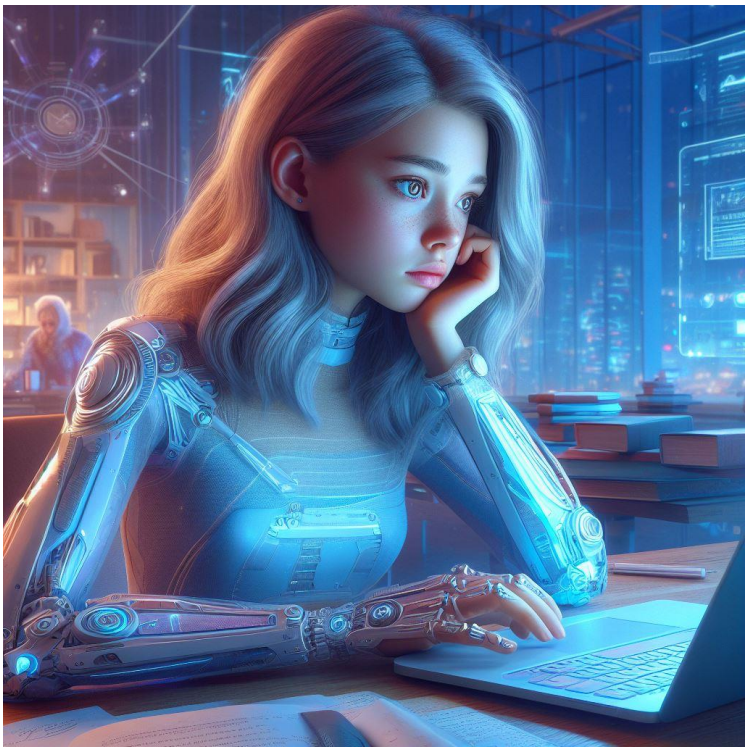
Atacurile cibernetice sunt chiar ele destinate furtului de bani sau înşelăciunii. Dar au şi alte efecte asupra portofelului tău, de exemplu:

- în cazul furtului de identitate, profilul tău din social media nu este singurul afectat; atacatorul nu are ca obiectiv doar să „pozeze" în pielea ta, el urmăreşte să fraudeze pe alţii purtând „faţa" ta, iar efectele acestor fraude te vor costa pe tine.
- în cazul defectării calculatoarelor sau telefoanelor, este evident care va fi costul înlocuirii sau reparării lor; mai mult, dacă sunt afectate fişiere importante, baze de date, agende telefonice ș.a., s-ar putea ca aceste costuri să crească.
- extragerea de date financiare te va conduce la necesitatea schimbării conturilor, cardurilor etc.

dacă nu lași ușa deschisă la casă, nu te lăsa nici online neprotejat

Cyberterorrism sau terorismul electronic se realizează prin utilizarea mijloacelor tehnologice de informare, de comunicare, informatice sau electronice pentru a genera frică, teroare, panică sau intimidare generalizată la o populaţie sau un grup ţintă definit, încălcând voinţa persoanelor, având scopuri economice, financiare, politice sau religioase.

Agresiunea online sau cyberbullying este hărţuirea prin intermediul calculatorului sau telefonului şi are loc pe bloguri, pagini personale, forumuri, email, SMS, şi mai ales chat rooms şi social media. În acest tip de hărţuire sunt distribuite public online poze, video sau texte care încalcă dreptul la viaţa privată al victimei.



Cum ne păzim?

Securitatea cibernetică a fiecăruia dintre noi este în strânsă legătură cu siguranța banilor noștri și de aceea este important să ne formăm câteva obiceiuri sănătoase. Până la urmă, utilizatorul este cel care, accidental și din neglijență, încarcă un malware sau o altă formă de atac cibernetic în dispozitivul său. Iar atacatorul nu urmărește decât să câștige bani. Când suntem victima unui atac cibernetic:

- schimbăm parolele aplicațiilor mobile aferente banilor (bancare, de pensii, de investiții etc.); de preferat ar fi să folosim un alt dispozitiv decât cel care a fost utilizat atunci când am fost victima atacului (alt calculator sau telefon).
- pentru conturi bancare sau de investiții, informăm entitatea financiară și eventual blocăm contul respectiv până la schimbarea accesului.
- raportarea unui atac cibernetic este realizată în UE către Europol, respectiv către Poliția Română.

Și pe calculator și pe telefon:

- să avem instalat un antivirus, să ne asigurăm că este pornit și actualizat permanent; măsurile de securitate se bazează pe criptarea de informații și date, destinate protecției împotriva pierderii sau furtului.

- să folosim diferite adrese de email în funcție de scopul lor; o adresă personală și una de școală/ serviciu trebuie utilizate distinct; spamerii construiesc liste de adrese de email utilizând diferite combinații sau informații; adresa personală este bine să rămână personală, adică nepublicată online sau folosită în social media (grupuri de emailuri, forumuri de discuții etc.), mai ales dacă este utilizată în raport cu entitățile financiare – conturi bancare, conturi de pensii private, conturi de investiții etc.

- parolele folosite la calculator, telefon sau la aplicații (financiare, magazine online etc.) trebuie să fie diferite pentru fiecare în parte, stabilite într-un format „puternic” (care să nu fie ușor de ghicit) și niciodată salvate pe dispozitiv; deși poate părea greu să ținem minte toate aceste parole, este mai sigur să nu le salvăm chiar în locul din care ele pot fi furate.

- nu trebuie deschise atașamente sau accesate linkuri din emailuri transmise de autori necunoscuți, nesolicitate sau care par suspecte; acestea pot fi infectate cu un malware.

- o entitate financiară nu va solicita prin email accesarea paginii sale pentru actualizarea unor date de cont personale; chiar dacă linkul paginii poate conduce la o sursă asemănătoare paginii de internet originale, există atacatori care folosesc astfel de paravane clonate pentru a fura informații financiare și a iniția, în numele și cu banii victimei, diferite tranzacții.

Ponturi de securitate online

Când suntem prezenţi în social media, conturile noastre sunt publice.

O „amprentă” mai mică online este mai sănătoasă.

Nu te lăsa păcălit de cereri de „prietenie” de la celebrităţi. În spatele unor astfel de profile se află diferite malware-uri.

Nu fii „prieten” cu persoane pe care nu le cunoşti şi nu le poţi verifica identitatea reală.

Vezi dacă poţi bifa opţiunea de a nu fi inclus în afişarea/primirea de publicitate.

- dacă dorim să mergem pe pagina web a unei entităţi financiare sau a unui magazin online, este indicat să introducem adresa URL manual în loc să o accesăm dintr-un link; accesarea unui astfel de link primit într-un email, într-un mesaj postat în social media, într-un mesaj dintr-o aplicaţie chat, dintr-un anunţ publicitar de pe un alt site sau dintr-o aplicaţie, sau dintr-un mesaj primit de la o persoană necunoscută – toate aceste comportamente ne pot pune în primejdie nu numai securitatea cibernetică a dispozitivului folosit, dar şi securitatea financiară.
- să dăm atenţie adresei web (URL-ului), mai ales când accesăm pagini de internet prin intermediul cărora cumpărăm ceva (adică introducem date financiare); dacă URL-ul este compus dintr-o secvenţă de litere şi cifre aleatorii sau care par ciudate, este indicat să nu introducem date sensibile sau private; dacă conexiunea este sigură, atunci URL-ul va începe cu „https” şi bara browserului va afişa o mică pictogramă a unui lacăt; dacă se apasă pe această pictogramă, se pot citi informaţii despre certificatul de autentificare SSL al paginii de internet respective.
- evitarea utilizării unor reţele wi-fi publice nesecurizate ne lasă vulnerabili în cazul unor atacuri cibernetice; dacă nu este absolut vital, mai bine evităm transmiterea de date prin astfel de reţele – în conversaţii cu familia şi prietenii nu transmitem parole ale conturilor sau alte date personale, nu accesăm aplicaţii financiare ş.a.
- în timpul utilizării unor aplicaţii, în special a jocurilor pe telefon, apare posibilitatea vizionării unor reclame în schimbul unor recompense în joc; evitaţi astfel de accesări şi recompense, costul lor poate apărea mai târziu sub formă de malware.

Ești atent digital la bani?

Este extrem de important ce informații personale (inclusiv financiare) punem la dispoziția tuturor. Limitează persoanele care îți pot accesa postările și informațiile din social media. Toate platformele colectează informații despre tine din aceste rețele.

Șterge conturile și profilurile pe care nu le mai folosești.

Este de preferat să nu accesezi linkuri primite prin mesaje sau comentarii în social media sau diferite aplicații (inclusiv sondaje, quizuri, concursuri sau câștiguri de premii, ori de tipul care îți „spun" cum vei arăta peste 10 ani sau ce tip de personalitate ești). Acestea pot fi malware care urmăresc obținerea de informații despre tine sau care au ca țintă furtul de identitate sau de bani.

Dacă primești un mesaj de la un prieten prin care ți se cer bani sau îți prezintă o oportunitate de neratat, dă-i un telefon. Contul lui ar putea fi folosit de altcineva, în special dacă ți se prezintă ca metodă de plată criptomonedele.

Înainte de a cumpăra ceva, verifică compania, magazinul sau persoana. Poți verifica printr-o căutare online, alăturând numele vânzătorului cu „scam", „păcăleală", „plângere", „complaint" sau alte cuvinte similare (ai prins ideea!). În social media, verifică profilele cu care interacționezi – dacă au o istorie de postări, ce alți prieteni (pe care chiar îi cunoști) sunt comuni ș.a.

nu crede un profil Facebook, toți părem frumoși online

Mai mult, dacă constatăm un posibil furt de identitate, chiar dacă el este online, este important să comunicăm acest lucru pe propriul profil. Hackerii obțin accesul la profilul din social media fie păcălindu-te să le dai acces, folosind un atac de tip phishing pentru a fura parola, găsind informațiile tale de acces pe dark web ș.a.

Odată ce au preluat controlul profilului, hackerii vor posta în numele tău diferite oprtunități false de investiții, vor distribui linkuri către site-uri phishing sau magazine false, vor aduna date despre prietenii și familia ta, vor avea acces la alte conturi de ale tale în care ai acces cu credențialele tale din profil (de exemplu, „sign in with Facebook").

Cum pot criptomonedele să ducă la atacuri cibernetice

În trecut, hackerii își monetizau eforturile prin: spargerea calculatoarelor pentru a fura date ale cardurilor și cumpărând bunuri sau prin spargerea aplicațiilor și cumpărând bunuri în numele și pe creditul tău. Astăzi, lucrurile au devenit mai complexe și hackerii mai inteligenți, mai ambițioși și mai sofisticați. Ei nu mai urmăresc doar câștigul pe termen scurt, ci o „pradă" mult mai mare. Monedele digitale și FinTechurile le-au facilitate aceste ambiții.

O platformă sau o aplicație care îți gestionează banii și pe care o poți deschide cu o poză a actului de identitate are din start o problemă de securitate. Contrapartea ta la orice tranzacție în această platformă poate fi oricine (deschizându-și contul cu orice poză).

Hackerii pot intra în platformele de criptomonede pentru a face tranzacții anonime, pentru a fura bani sau pentru a spăla bani. Tranzacțiile cripto nu cer nume reale, contrapartea ta la o tranzacție rămânând anonimă.

Crypto-jacking: hackerii folosesc browserul victimei pentru a mina fraudulos noi unități.

Formulare de înregistrare compromise: furtul informației victimei din platformele de tranzacționare și vânzarea ei pe Dark Web.

Atacuri malware: furtul de resurse de mining pentru cripto din portofele (wallet).

Atacuri crypto phishing: mailuri sofisticate care redirecționează victima către o versiune falsă a site-ului de criptomonedă, pentru ca apoi să le fure credențialele și banii.

O monedă digitală (criptomonedă) este o formă de bani disponibilă doar digital și tranzacțiile cu ea se realizează pe dispozitive (calculator, telefon) utilizând un portofel electronic. Monedele digitale există într-o rețea descentralizată, independentă, portabilă și divizibilă. Ele se bazează pe criptografiere pentru a securiza și verifica tranzacțiile, a administra crearea de noi unități și a preveni falsificarea. Până aici, totul este bine. Ceea ce nu este atât de bine: criptomonedele crează și o anonimizare care, la rândul ei, aduce riscuri mai ales în zona de cybercrime. O astfel de monedă este format din mai multe componente (adrese, chei private și publice, tranzacții care se pot citi în linii de text – ele nu conduc la identitatea cuiva, asigurând anonimizarea tranzacțiilor financiare). Sistemele sunt descentralizate și, prin urmare, nesupravegheate de vreo entitate sau autoritate.

când este vorba de banii tăi, verifică și asigură-te

Mesaje private

În social media poţi primi şi mesaje private, un fel de SMS-uri utilizate acum pe scară largă. Toate platformele permit astfel de mesagerie şi ea este folosită de multe ori de scameri pentru a atrage posibile victime financiare. Prevederea legală care interzice contactarea prin telefon pentru a „vinde” servicii de investiţii, dar mai ales uşurinţa cu care găseşti fără costuri şi fără efort o masa de persoane cărora să le transmiţi mesaje au făcut din social media „mediul” ideal pentru această abordare frauduloasă. Scamerii transmit mesaje (sau postează, fac comentarii pe diferite profiluri/grupuri) prin care invită la accesarea unor platforme de tranzacţionare (de investiţii), menţionând poveşti de success cu profituri nerealist de mari.

ofertă prea bună – este oare reală?

În primul rând ar trebui verificată legalitatea platformei de investiţii. Aceasta se face gratuit accesând registrul ASF. De multe ori, platformele permit tranzacţionarea, şi chiar îţi vezi contul crescând precum Făt Frumos, dar când vrei să îţi retragi banii platformele (sau brokerii) nu mai sunt de găsit. „Consultantul financiar binevoitor” nu este un profesionist autorizat şi nu vei cui să soliciţi banii.

Sau există şi cazul în care autorizarea este făcută în altă ţară. În acest caz, recomandăm o informare mai atentă cu privire la entitate şi ţara de origine.

În caz de înşelăciune, plângerea se adresează autorităţilor cu atribuţii de cercetare penală şi autorităţilor financiare din ţara de origine a respectivei entităţi financiare. Dacă vă aflaţi, totuşi, într-o astfel de situaţie nefericită, dacă mai puteţi, încercaţi să solicitaţi băncii (dacă aţi folosit un card şi nu un FinTech) blocarea operaţiunilor şi anularea lor.

Dacă aţi pierdut bani din cauza unui scam şi aţi vorbit despre acest lucru pe social media, există posibilitatea să fiţi în atenţia altor scameri – aceştia vă vor contacta tot prin social media pentru a se oferi să vă recupereze banii. Cel ma bun sfat – nu acceptaţi astfel de oferte!

De asemenea, aveţi grijă că monedele virtuale nu sunt considerate instrumente financiare şi că există state unde nu există obligaţia de autorizare pentru entităţile de servicii financiare, aşadar nu au nici o obligaţie legală de protecţie a investitorilor.

În România este interzisă promovarea şi oferirea de servicii de investiţii prin call center, iar social media poate fi un astfel de canal.

Un mesaj în social media este un tip de comunicare (publicitate) agresivă, deci nu vă grăbiţi să luaţi o decizie şi verificaţi atent.

Stai safe

Prezența în social media este deja o parte a vieții noastre, creează și păstrează legături într-o lume digitală, cumperi sau vinzi rapid, ai parte de distracție sau de informare și educație. Doar că social media a atras și persoane mai puțin bine intenționate (scameri). O statistică din 2021 a Federal Trade Commission din SUA arată că 1 din 4 persoane care au raportat că au pierdut bani fiind fraudați a afirmat că totul a început din social media cu o postare, un mesaj sau un anunț. Același studiu arată că social media a crescut în profitabilitate pentru fraudatori, mai mult decât orice altă metodă de abordare, înregistrându-se (față de 2020) o creștere de peste 100% a numărului de persoane și de aproape 300% a sumelor fraudate. Pentru cei care urmăresc să înșele în social media, acest spațiu este extrem de ofertant – costă foarte puțin pentru a ajunge la miliarde de oameni din întreaga lume. Este extrem de ușor să creezi o identitate falsă sau să preiei fraudulos un profil pentru a păcăli „prieteni". Poți afla o multitudine de detalii personale și financiare despre o persoană – unde locuiește, unde călătorește, ce își cumpără, ce interese are, care este statutul familial ș.a., putând fi realizate profiluri extrem de complexe fără măcar să te miști din fața dispozitivului.

doar pentru că îți scrie nu înseamnă că trebuie să răspunzi

Pot exista cazuri de entități „clonă", care copiază entități autorizate (site, date de identificare ș.a.). Verificarea se face comparând datele de identificare ale entității cu cele din registrul ASF.

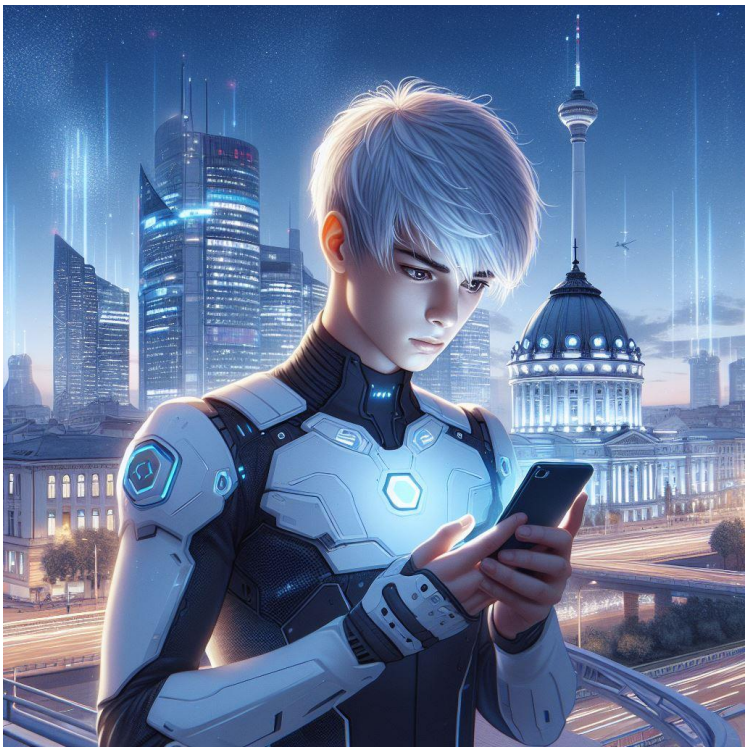
Unii scameri folosesc fotografii sau declarații false ale unor celebrități pentru a atrage victimele, de cele mai multe ori sub forma unor reclama. Clickul redirecționează spre o platformă de investiții sau o pagină web care implică introducerea unor date de contact, pentru ca apoi să fiți contactat. Nu cădeți în această capcană!

Mai sunt utile, în acest context, și verificările pe care le puteți face pe web cu privire la părearile altor persoane – în forumuri, social media, grupuri etc. – dacă este o înșelăciune, atunci vor exista atenționări.

Nu accesa aplicații care îți oferă o distracție de 3 secunde

Ceea ce poate părea o distracție nevinovată în social media poate fi o cale prin care permiți unui malware să preia din dispozitivul tău sau unui scamer să aibă acces la informațiile tale, ambele cu intenții care au ca obiectiv bani ... banii tăi. Aplicațiile (de tip quiz și gratuite) care îți „ghicesc" cine ai fost în antichitate, ce tip de animal sau floare ești, câți ani vei trăi, sunt mici distracții în plasa cărora cad tot mai mulți.

Cel mai sigur este să reziști tentației de a accesa aceste aplicații care circulă în social media și, dacă nu ai făcut-o până acum, să îți ștergi datele personale precum numărul de telefon și emailul din profil.



Scopul influencerilor este de a obține profit din activitatea lor în social media sau în afara ei. Unii influenceri sunt profesioniști în domeniile lor și conținutul pe care îl fac public în socal media este etic, original. Ei folosesc aceste platforme strict pentru o comunicare profesională și această comunicare respectă regulile profesiei, respectivele persoane fiind avizate.

Alții își construiesc mai întâi imaginea de influencer ca apoi aceasta să atragă comunitatea necesară. Construcția de imagine este bazată pe fake followeri, fake news sau fake image pentru a arăta că există numere mari de urmăritori și a crea mai mult engagement. Cu cât mai mare impactul, cu atât mai mare câștigul financiar al influencerului.

Influencer

Influencerul este acea persoană care prin comunicarea sa realizată în social media a creat un conținut pe care îl urmăresc foarte multe persoane și care, așa cum îi spune și numele, influențează decizii ale urmăritorilor săi. Este creator de opinii și de trenduri, determină cumpărări sau investiții, influențează opțiuni de vot ș.a. Dar cum ajung aceste persoane în poziția de a avea un impact atât de mare asupra mentalului colectiv?

influencerii nu sunt ONG-uri

Și cum social media este o industrie, așa poți utiliza aici instrumente clasice de marketing cum ar fi: cumpărarea de comentarii sau like-uri (ambele asigurând creșterea impactului postării) și de vizualizări de story-uri, o distribuire a postărilor (sponsorizare) după anumiți algoritmi de diseminare stabiliți în funcție de grupul țintă care este dorit să fie atras, cumpărarea de urmăritori (bots), utilizarea unor aplicații care permit automatizarea follow/unfollow pentru generarea de reacții, alăturarea branduri sau nume de marcă cu conținutul pentru a se crea „tracțiune”, adică a realiza mai mult engagement ș.a. Scopul la întreaga această activitate este de a crea o comunitate cât mai mare (altfel cum să fii influencer?). La această comunitate influencerii se adresează, în mare parte, un fel de comunicatori (nedeclarați) pentru firme și branduri care îi plătesc. Cu cât mai mare „influența”, cu atât mai mare recompensa.

Finfluenceri

Influencerii sunt activi fie în domenii generale (cei care vorbesc în mare parte despre orice sau despre subiecte multiple), fie în domenii specifice. Din acest ultim grup fac parte mai noii finfluenceri, adică influencerii în domeniul financiar, cei care oferă un acces rapid și ușor la „sfaturi financiare" și exprimă opinii și păreri despre bani, investiții, asigurări sau diverse alte produse și servicii financiare. Apariția lor a fost determinată de nivelul scăzut de educație financiară din întreaga lume, de răbdarea cât mai mică de a căuta informații și de dorința accesării unor servicii de „sfătuire" gratuite. Dacă înainte te adresai unui consultant financiar, acum te uiți pe Facebook, Instagram, Youtube sau TikTok. Poți găsi aici conținut avizat, profesionist, sau conținut realizat de multe alte persoane. Din păcate, sunt din ce în ce mai mulți oameni care investesc bani fără a mai face o minimă analiză asupra riscurilor, mecanismelor, produselor și instrumentelor financiare sau măcar o minimă cercetare care să îi ferească de scam-uri și înșelăciuni.

Și pentru lucrurile nu sunt niciodată simple, finfluencerii au dezvoltat noi metode de a obține profituri prin cursuri, școli, academii, programe care sunt sau nu gratuite. Unele dintre acestea sunt consistente, având o valoare educațională reală. În altele, participantul „învață" de la cei „experimentați". Pentru că legislația europeană precizează clar ce condiții trebuie să îndeplinească aceste forme de învățare financiară, deseori cursurile iau denumiri atractive precum mentorat, coaching financiar, educație pentru independență financiară ș.a. Posibilul conflict de interese al organizatorului ar trebui făcut public, pentru ca atunci când alegi un astfel de curs să ai o idee cu privire la organizator.

Ceea ce îi deosebește pe finfluenceri de un profesionist financiar este faptul că, în marea majoritate a cazurilor, nu sunt persoane autorizate sau avizate profesional în acest domeniu, așa cum sunt, de exemplu, consultanții financiari autorizați, instituțiile financiare autorizate și personalul acestora, brokerii etc. și neavând studiile de specialitate necesare, conduita și transparența profesională ș.a.

Finfluencerii sunt, de fapt, persoane fizice care exprimă opinii sau prezintă exemple personale, non-profesioniști care utilizează social media. Doar că, de multe ori, aceste opinii nu sunt neapărat lipsite de riscuri pentru cei care aleg să le copieze și exemplele date de finfluenceri nu sunt neapărat reale.

Dacă în viața reală, ca urmare a sfaturilor unui influencer, ai cumpărat un tricou care este de o calitate îndoielnică sau ai ajuns la un restaurant cu mâncare nu așa de bună, ai o dezamăgire de moment și pierzi o sumă mică de bani. Deși, în cazul tricoului îl poți returna și în cazul restaurantului poți întoarce la bucătărie mâncarea. Dacă însă ai urmat sfatul unui finfluencer, suma de bani pe care o cheltui pentru a cumpăra sau investi în instrumente și produse financiare este considerabil mai mare și efectele asupra propriului buget pot fi multiple: un angajament financiar dezavantajos pe termen lung care te poate îndatora; accesarea unor platforme neautorizate care să te facă victimă; afectarea dispozitivelor față de atacuri cibernetice (malware, phishing etc.) ș.a. Mai mult, nu poți trage la răspundere legal un finfluencer – el „doar" a exprimat o opinie ...

Marketingul de tip multilevel (MLM) este o afacere construită după un model piramidal în care câștigi din comisioanele din vânzările tale și ale persoanelor pe care le recrutezi să facă asta. Social media este din ce în ce mai des folosită pentru astfel de recrutări, dar rareori se și câștigă în mod real bani. Cei care îți fac astfel de prezentări sunt VIP-uri ai mediului online și nu numai. Înainte de a te Aventura într-o astfel de lume, caută pe web numele companiei și situațiile ei financiare, din care poți vedea care este venitul mediu din vânzare și poți calcula comisioanele și cât ar trebui să vinzi pentru a avea un venit mai mare decât taxele necesare pentru înregistrarea ca vânzător. VIP-urile vor încerca să te convingă că un job full-time de la 9 la 5 nu este pentru oameni de succes și că poți avea stilul lor de viață luxos dacă urmezi această rețetă și investești în tine (un curs, un e-book, un mentorat – și gata, ești cel mai bun vânzător sau profesionist). Unde nu este greșit – da, poți fi cel mai tare dacă investești în tine – în educație financiară serioasă!

Unii finfluencerii de astăzi vând povești și sfaturi după tipul unei scheme piramidale, vârful fiind chiar ei, iar mai jos fiind vândută doar **iluzia** (povestea, promisiunea, sfatul) și cu cât vârful atrage mai mulți urmăritori, cu atât mai credibilă devine povestea sa.

Nu te lăsa atras de discuții în grupuri

În social media sunt create diferite grupuri care au ca teme îmbogățirea, educația financiară, investițiile, cum să îți faci o afacere profitabilă sau alte astfel de subiecte. Informațiile postate de membri pot avea diferite intenții, unele oneste și unele nu. Este bine să verifici înainte de a lua o decizie financiară și să încerci să afli cât mai multe despre ce te tentează aceste discuții să faci.

O înșelătorie care este din ce în ce mai popular în social media este cea de tip „pump and dump”, care apare în grupurile unde se discută despre oprtunități de investiții. Ea face referire la investiția într-un active real, existent – acțiuni ale unei companii sau alte instrumente financiare. În special, înșelătoriile se fac când piața financiară este de tip bull market.

O persoană din grup care a avut anterior postări care arată un nivel de cunoaștere al pieței financiare postează despre o incredibilă oportunitate de investiții, de regulă într-o companie mica (dar care „are perspective”) sau pe o piață nereglementată sau din altă țară, unde mai greu ai acces la informații. Nu se precizează însă că ei dețin o cotă-parte din companies au au un alt interes în activele financiare tranzacționate. Oamenii cumpără conform recomandării, crescând (pump) astfel prețul de tranzacționare. Cel care a făcut recomandarea (scamer) își poate vinde (dump) astfel deținerile la un preț pe care alții l-au făcut mare. Dar vânzarea sa, dacă este o deținere mare, va scădea la loc prețul și … restul investitorilor pierd.

Şi ce să fac în social media?

Pentru ca banii tăi să fie în siguranţă, tot ceea ce ai citit până acum te-a învăţat să nu urmezi sfatul unor persoane necunoscute şi care nu au o expertiză profesională financiară şi să te protejezi faţă de riscurile cibernetice. Dar educaţia financiară aplicată în social media este mai mult. Ce postezi, rămâne public – gândeşte-te bine ce postezi (drepturi de autor), ce poze cu tine alegi (poate angajatorul tău viitor îşi va forma o altă părere despre tine). O altă chestiune important este ce informaţii laşi publice (chiar vrei să îţi laşi numărul de telefon sau adresa de mail care te identifică cu o firmă, şcoală etc.)?

ce este azi în social media, rămâne mereu online

- Nu posta descrieri sau poze cu casa ta, lucrurile pe care le deţii, cumpărăturile tale cu o anumită valoare sau vacanţele care pot indica sume de bani cheltuite. Profilul tău financiar poate fi observant din astfel de detalii şi poţi ajunge o victimă a hoţilor.

- Nu posta fotografiile din vacanţă atunci când chiar eşti în vacanţă! Nu se întâmplă absolut nimic dacă vei face acest lucru când te întorci şi casa ta este mai bine păzită cu tine acolo.

- Marketplace-ul poate să nu fie exact ceea ce vezi/crezi (pot fi foarte multe informaţii cu potenţial înşelător. Ai grijă când faci donaţii, cumperi obiecte în Marketplace, de la cine cumperi (şi întâlneşte-te în locuri publice) ş.a. – statistic, pe Facebook Marketplace, 1 din 6 sunt subiecţi ai unui scam.

- Nu plăti în avans şi nu trimite obiecte prin curier fără a fi plătite în avans (apropos, PayPal nu restituie/rambursează fonduri).

Stabileşte-ţi obiectivele social media pe care ţi le doreşti de la profilul tău

Like < Comment < Share

- Lumea te urmăreşte doar dacă ai ceva care place.

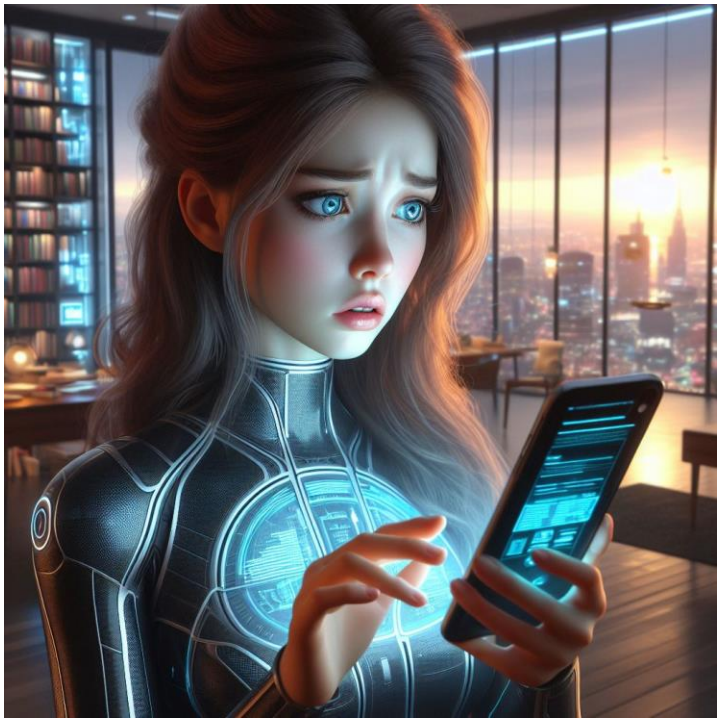
- Lumea intră în conversaţie dacă ai ceva de spus.

- Lumea îţi distribuie postarea dacă ai făcut o impresie.

- Gândeşte-te ce vor prietenii tăi să vadă, ce vrei tu să vadă, ce atrage ş ice vrei să transmiţi.

Marketing și vânzare

- Utilizarea social media în scop de marketing poate fi făcută organic (gratis) sau sponsorizat.
- Social media oferă în vânzări posibilitatea de utilizare a unui format modern (diferit de media tradițională) și costuri scăzute de marketing/comunicare (o proporție eficientă cost-beneficiu).
- Oferă accesul la o gamă largă de informații despre posibilii cumpărători.
- Algoritmii îți pot împinge în față conținut nesolicitat (poate chiar agresiv) – este nevoie de răbdare pentru a-l înlătura.
- Abordarea comunicării în social media trebuie să țină seama de faptul că acesta nu este un canal oficial de comunicare – în cazul în care se solicită informații de la autorități – sau în funcție de politica instituțională; Facebook este, de exemplu, considerat spațiu public, inclusiv din punct de vedere juridic (în România – Decizia ÎCCJ 4546/2016).



Interactivitatea și inter-conectivitatea

- Prin algoritmi specifici de cunoaștere îți sunt afișate în feed știri, clipuri publicitare, postări cu caracter comercial apropiate de interesele utilizatorului.
- Ești influențat să cumperi/investești în anumite produse sau servicii (inclusiv financiare) sau să ai o anumită atitudine față de un comerciant (inclusiv din zona financiară).
- Se realizează o comunicare rapidă sau extragerea rapidă de informații.
- Utilizatorul este direcționat inclusiv către comunități (grupuri) sau influenceri din zona financiară (utilizatorul nu poate mereu să valideze sau nu conținutul) – pericol de informații eronate.

Inter-conectivitatea web înseamnă influențarea atitudinii sau a comportamentului.

Există conturi fake – ai grijă când interacționezi cu ele, ce informații să crezi, nu te angaja în tranzacții și nu face cumpărături etc. Chiar dacă interlocutorul îți răspunde, uită-te la profil – dacă nu este activ (plin de informație) poate fi fake.

Există multe scam-uri în social media, chiar și cu furnizare de ID-uri false – nu da datele personale.

Când ți se dau date de carduri (mai ales emise de non-bănci) – nu te încrede în contraparte – poate fi un scam.

Există controverse privind respectarea vieții private a utilizatorilor – se utilizează informațiile personale ale utilizatorilor cu scopul de a introduce anunțuri publicitare adaptate profilului fiecărui utilizator în parte și chiar de a vinde aceste informații unor companii private. Orice informație introdusă (chiar și ca schiță) este păstrată în permanență pe serverele social media (chiar dacă îți ștergi contul).

Dă-ți seama când ești manipulat

Companiile și blogger-ii se folosesc de social media pentru publicitate. Mulți dintre cei prezenți în mediul online pot să nu fie oameni, ci roboți – orice conținut poate fi postat, nimeni nu garantează veridicitatea unui anunț sau nu blochează o încercare de înșelare. În plus, există profiluri false sau profiluri ale unor persoane decedate (și trolling). Este important să știi că social media furnizează conținut care este realizat astfel încât să stimuleze emoții, utilizarea unei conexiuni emoționale intense conducând la controlarea comportamentului. Există o abordare pozitivă (stimularea emoțiilor pozitive – bucurie, plăcere ș.a.) sau o abordare negativă (insecuritate, frică, furie ș.a.). mai mult, în social media există hiperbolizarea și generalizarea unor fapte, acte, stări, precum și mult deep fake – imagini/video false, prelucrate cu AI și distribuite pe social media.

Tehnici folosite în campanii (pe lângă cele clasice):

- suprimarea/limitarea altor idei/produse (concurența),
- discreditarea (prezentarea în opoziție astfel încât al tău să fie bun),
- epuizarea (suprapopularea cu postări a unei platforme astfel încât utilizatorii să nu mai facă diferența real-fake, bun-rău).

Dezvoltă un control al emoțiilor

Social media este un mediu care poate fi dificil (likes/hates, insulte, replici negative ș.a.).

- Nu intra în conversații jignitoare sau contradictorii.
- Nu posta trăiri interioare care trebuie să rămână interioare.
- Nu distribui (share) conținut pe care nu îl stăpânești bine.
- Nu face recomandări legate de bani sau produse financiare.
- Nu posta poze stânjenitoare cu tine sau cu alții, nu posta poze cu copii (ai tăi sau ai altora).
- Ai grijă în ce grupuri și ce prieteni îți alegi. Nu face plângeri despre școală, locul de muncă ș.a. Nu face comentarii financiare, politice, economice dacă nu stăpânești subiectul și nu cunoști contextul sau dacă profesia ta implică o anumită conduită care nu îți permite să te expui.
- Nu te identifica cu bârfe, atacuri la persoană, jigniri și nu te angaja în răspunsuri. Nu răspunde la provocări, mai ales financiare.
- Ai grijă când renunți la anonimitate. Dacă nu vrei să construiești o reputație profesională, anonimizarea datelor personale este importantă pentru securitatea ta financiară. Exprimarea unor anumite păreri personale poate fi și ea dăunătoare – te poate vedea un angajator, imaginea îți poate fi schimbată și chiar deteriorată etc.
- Există peste 600.000 de încercări de hacking în fiecare zi, deci datele tale nu sunt protejate.

Consumul critic (5c)

Context – cine a scris postarea, de unde vine, când a fost făcută, dacă există informații noi care ți-ar schimba decizia de consum ș.a.

Credibilitate – verifică credibilitatea sursei, reputația ș.a.

Construcția – analizează subiectivismul, dacă există omisiuni în prezentare, cum sunt realizate imaginile care însoțesc postarea, comment/recenzie pot face diferența între fapte și opinii ș.a.

Coroborarea – coroborează informația din social media cu informații din alte surse credibile, asigură-te că nu există o singură referire

Compară – compară produse, prețuri, știri, surse, recenzii ș.a.

- Ai grijă la **CAPCANE DE SUBSCRIERE**: utilizatorul este direcționat spre înscrierea pentru un produs/serviciu pe care nu îl va primi niciodată și se generează credit continuu în cont.
- Nu răspunde la provocările care vin de la „sediul central" al facebook, Instgram etc. și care îți spun că ți se va bloca contul dacă ... dacă știi că nu ai făcut nimic împotriva regulilor, nu se întâmplă nimic. Și dacă își doreau să îți închidă contul – o făceau, fără să îți trimită avertizări sau solicitări sau să îți ceară bani.

gândește-te de două ori înainte de a da click o dată

- Social media reprezintă un canal de comunicare care supraîncarcă utilizatorul cu informații, ceea ce conduce la o stare de paralizie în analiză (Powers)
- Raționalitate mărginită (Simon; Thaler și Mullainathan), limită a sumei de informații care pot fi prelucrate de indivizi, nu este fezabilă evaluarea în profunzime a tuturor alternativelor de alegere (Karimi).
- 81% din deciziile de cumpărare ale consumatorilor sunt influențate de postările prietenilor lor de în social media (Forbes).
- Facebook reprezintă 50% din totalul recomandărilor sociale și 64% din totalul veniturilor sociale (Business Insider).

Fraude (scams) în social media

E-commerce – cei care fraudează pretind a fi vânzători online reali (ex: anumite anunţuri din Facebook Marketplace), consumatorii plătesc pentru bunuri care apoi se dovedesc a fi contrafăcute, de calitate proastă, sau nu sunt livrate.

Fraude de investiţii – cei care fraudează fac publicitate la o oportunitate de investiţii „prea bună pentru a fi adevărată", folosind câteodată poveşti care par a fi din surse reale, iar consumatorii pot pierde banii investiți.

Impostura – cei care fraudează pretind a fi mărci veritabile, prieteni reali sau familie (frauda de identitate), pentru a câştiga încrederea consumatorului şi a-l determina să cumpere bunuri, transfere bani sau să acceseze link-uri (de site-uri, de câştig al unui premiu ș.a.) de pe care se „obține" şi un malware pe dispozitiv.

- CATFISH: fraudatorii creează profiluri false pentru a intra în contact şi a dezvolta o relaţie online, clădesc încredere apoi cer să li se trimită bani sau date personale.
- CRYPTOCURRENCY: publicitate falsă, articole noi sau mesaje care tentează consumatorii să investească în crypto, iar consumatorii pierd bani, au datele personale furate sau ambele.
- FRAUDE CLICKBAIT: postări social media cu „ştiri senzaţionale cu celebrităţi" care încurajează click-ul pe link sau pe un URL ascuns, ceea ce conduce la un site extern de unde se downloadează un malware pe dispozitivul victimei.

nu instala direct din social media, folosește magazinul de aplicații

- CASH GRABS: fraudatorii intră în contul de social media al victimei şi transmit mesaje prietenilor solicitând ajutorul şi bani
- COMPETIŢII FALSE SAU CADOURI: fraudatorii pozează ca având afaceri legale, solicitând „like" şi „share" sau click pe linkuri pentru a câştiga premii (neexistente). „Like-farming" permite fraudatorilor să construiască o reţea de followers, pe care apoi îi au în vedere pentru spam sau fraudă (click-urile conduc şi la malware).
- FRAUDE CU CALITATEA DE MEMBRU: participarea într-un grup fals sau fan page şi cererea de date personale pentru a primi premiul sau pentru a plăti o cotizaţie.

Social media nu duce lipsă de persoane care își doresc să te separe de banii tăi

Nu transmite sau posta date ale conturilor tale – bancare, de investiții, de pensii etc. Comunicarea financiară profesională nu se face niciodată prin social media.

Social media te face prieten cu oricine din lume, dar oare oricine este prieten cu tine? Nu acorda încredere oricui și nu te lăsa păcălit de vorbe frumoase.

Nu posta poze care să arate când lipsești de acasă. Poți să îți arăți vacanța și după ce te întorci.

Setările private (nume, vârstă, data nașterii, reședința, școala, emailul, telefonul ș.a) trebuie alese atent – toate pot face obiectul furtului de identitate.

Alege ca ceea ce postezi în social media (setări private) să fie vizualizat doar de cine alegi tu.

Statistici

Raportul din 2022 al Poliției Române și al Institutului de cercetare și prevenire a criminalității arată că 70% din fraudele online au loc prin intermediul dispozitivelor mobile, atrăgând atenția asupra utilizării telefoanelor, deseori securitatea sistemului lor fiind neglijată de utilizator. O altă statistică este cea a hackout.ro, care arată că cele mai multe atacuri cibernetice din România sunt de tipul phishing, un număr mare dintre acestea fiind în legătură cu platforme web de vânzare-cumpărare de produse. Urmează însă scam-urile care au ca subiect crypto și apoi smishing-ul cu oferte de muncă. Majoritatea raportărilor de incidente cibernetice primite prin intermediul acestei platforme fac referire la pagini web, email și telefon.

Când ai doar jumătate de imagine, nu pretinde că știi tot adevărul. Așa este și în viață ...