DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

# INGINERIE SOCIALĂ

- ☑ Ce este ingineria socială
- ☑ Cum funcționează
- ☑ Tehnici de manipulare
- ☑ Tipuri de atacuri
- ☑ Cum să recunoaștem un atac
- ☑ Grupuri vulnerabile
- ☑ Aspecte legale
- ☑ Impactul noilor tehnologii


TLP:CLEAR

## Publicul țintă al ghidului

Prin conținutul său accesibil și practic, ghidul servește ca instrument educațional pentru publicul larg ajutând utilizatorii de internet să devină mai conștienți de riscurile de securitate online. În esență, ghidul se adresează oricărei persoane interesate să își protejeze informațiile personale și profesionale de schemele din ce în ce mai sofisticate de inginerie socială.

## Rezumat executiv

Ghidul prezintă strategii și tactici adoptate de infractori în cadrul atacurilor de inginerie socială. Amenințarea este reală și omniprezentă, manifestându-se sub diverse forme, de la emailuri și mesaje text frauduloase (phishing și smishing) la apeluri telefonice false (vishing) și chiar interacțiuni directe.

Ghidul oferă detalii despre tehnicile de manipulare utilizate de atacatori pentru a obține informații sensibile sau a influența victimele, precum și metode de colectare a datelor. Aspectele legale, incluzând Regulamentul general privind protecția datelor (GDPR), Legea comerțului electronic și Codul Penal, sunt analizate în contextul infracțiunilor informatice, fraudei și perturbării sistemelor informatice. Pentru combaterea atacurilor de inginerie socială, ghidul recomandă strategii precum educarea publicului, conștientizarea angajaților, implementarea tehnologiilor de protecție și adoptarea unor bune practici.

Evoluția rapidă a tehnologiei, manifestată prin ascensiunea inteligenței artificiale și popularizarea muncii la distanță, a generat un context propice proliferării atacurilor de inginerie socială. Infractorii cibernetici exploatează constant tendințele actuale și vulnerabilitățile specifice populației pentru a-și atinge obiectivele frauduloase.

## Ce este ingineria socială

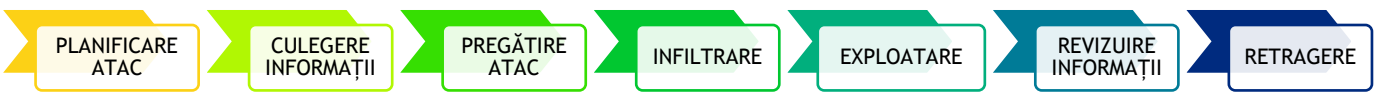
Ingineria socială reprezintă o tactică folosită de indivizi sau grupuri, care folosesc manipularea și înșelarea oamenilor pentru a obține informații sensibile sau pentru a-i determina să întreprindă acțiuni care le compromit securitatea. Aceasta se bazează mai degrabă pe psihologie și pe comportamentul uman decât pe abilitățile tehnice.

În atacurile de inginerie socială, infractorul pretinde adesea că este o persoană de încredere sau un reprezentant legitim al unei instituții cunoscute pentru a câștiga încrederea victimei. Utilizând tactici precum furtul identității, aplicarea de mijloace de convingere sau diverse șiretlicuri, atacatorul poate obține informații sensibile: parole, detalii financiare, acces la sisteme și rețele informatice.

## Cum funcționează

Metodele de inginerie socială sunt printre cele mai întâlnite tactici de atac cibernetic deoarece, se consideră că omul reprezintă veriga cea mai slabă din lanțul de securitate al unei companii sau instituții. Un astfel de atac poate fi inițiat într-un timp foarte scurt, printr-un singur email, sau poate dura mai multe luni, implicând conversații pe platforme de socializare sau chiar în persoană.

Obținerea accesului la conturile personale poate fi surprinzător de simplă pentru un atacator care deține informații minime, precum numele complet, data nașterii sau adresa. De ce? Mulți oameni utilizează date personale ca parole, oferind hackerilor o cale facilă de a le sparge conturile. În general, un atac de inginerie socială este complex, desfășurarea acestuia fiind împărțită în 7 etape:




1. **Planificarea atacului**. Stabilirea clară a obiectivelor de către atacator (fie că este vorba despre acces la informații confidențiale sau la anumite sisteme). Următorul pas este selectarea țintelor vulnerabile care pot facilita atingerea acestor obiective. Țintele sunt supuse unei evaluări amănunțite pentru a identifica posibile vulnerabilități, atât de natură tehnică cât și umană, precum și pentru a analiza infrastructura IT și procedurile de securitate existente.

2. **Culegerea de informații**. Identificarea surselor de unde se pot obține date despre țintă, cum ar fi rețelele sociale sau website-urile profesionale. Informațiile colectate care includ date personale, obiceiuri online sau relații interpersonale, sunt analizate în detaliu pentru a construi un profil complet al țintei și a descoperi vulnerabilități care pot fi exploatate.
3. **Pregătirea atacului**. Conceperea unui plan detaliat de acțiune care include selecția tacticilor și tehnicilor specifice care vor fi utilizate. Sunt pregătite materialele necesare precum email-uri false sau conturi pe rețele sociale. Planul poate fi supus unui proces de simulare și testare pentru a identifica și corecta orice greșeli ulterioare.
4. **Infiltrarea**. Stabilirea unei linii de comunicare cu victima prin diverse mijloace și construirea unei relații de încredere pentru a facilita manipularea. Atacatorul își ajustează apoi tactica în funcție de reacția și personalitatea victimei, asigurându-se că mesajul său este cât mai convingător.
5. **Exploatarea**. După ce a stabilit o relație de încredere cu ținta, atacatorul începe să manipuleze situația pentru a obține informațiile sau accesul dorit. Contează foarte mult cât de bine a fost pregătită infiltrarea și cât de convingător este atacatorul.
6. **Revizuirea informațiilor**. După obținerea tuturor informațiilor necesare, atacatorul va menține contactul pentru o scurtă perioadă de timp, astfel încât victima să nu conștientizeze faptul că a fost atacată și implicit să nu contacteze autoritățile competente în domeniu. Greșelile sunt notate pentru a fi evitate în viitor, iar planul de atac este actualizat în consecință.
7. **Retragerea**. Eliminarea oricăror dovezi ale implicării atacatorului și închiderea tuturor căilor de comunicare cu victima. În această fază finală, poate avea loc și o monitorizare discretă a victimei pentru a se asigura că aceasta nu a detectat atacul.

## Tehnici de manipulare în ingineria socială

Tehnicile de inginerie socială se bazează pe o varietate de metode de persuasiune și manipulare pentru a influența comportamentul victimelor și a le determina să dezvăluie informații sensibile sau să execute acțiuni dorite de atacator.

**Simpatia**. Crearea unei relații de simpatie și conectare cu victima o face mai receptivă la mesajele manipulatorului și mai predispusă să-i acorde încredere.

**Reciprocitatea**. Oamenii sunt mai predispuși să se conformeze solicitărilor, dacă simt că datorează ceva solicitantului.

**Dovada socială**. Prezentarea de dovezi false (ex: mărturii, statistici) care sugerează că o anumită acțiune este acceptată sau recomandată de o majoritate, poate influența decizia victimei.

**Urgența**. Crearea unui sentiment de urgență prin limitarea timpului disponibil pentru luarea unei decizii, poate determina victima să acționeze impulsiv fără a analiza critic situația.

**Frica**. Incitarea fricii de a suferi consecințe negative sau de a fi expusă la riscuri poate determina victima să cedeze solicitărilor manipulatorului.

**Autoritatea**. Afirmarea unei poziții de autoritate, fie reală, fie simulată, poate determina victima să se supună instrucțiunilor fără a le pune la îndoială.

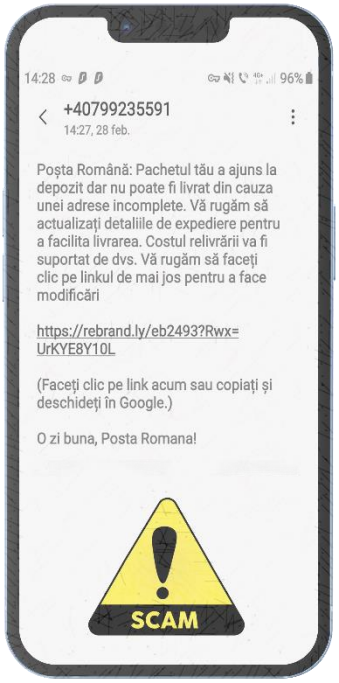
**Lipsa de disponibilitate**. Sugerarea, că o anumită resursă este rară sau limitată, poate intensifica dorința victimei de a o obține făcând-o mai vulnerabilă la manipulare.

## Tipuri de atacuri de inginerie socială

**Phishing**. Atacatorii trimit e-mailuri, mesaje sau linkuri înșelătoare din partea unor site-uri care par legitime, cu scopul de a convinge destinatarii să le acceseze și să dezvăluie informații sensibile, cum ar fi parole, datele cardului bancar sau date cu caracter personal.

**Vishing**. O formă de phishing care are loc prin comunicații vocale, de obicei prin apeluri telefonice. Atacatorii se prefac a fi reprezentanți ai unor companii sau instituții de încredere (bănci, operatori de telefonie, etc.) pentru a convinge victimele să le divulge informații sensibile. Cu ajutorul noilor tehnologii atacatorii pot chiar falsifica ID-ul apelantului să pară că provine de la o sursă legitimă.

**Smishing**. O formă de phishing care utilizează mesaje text manipulative pentru a fura informațiile personale și corporative confidențiale, similar e-mailurilor de tip phishing.




**Spear-phishing**. Similar cu phishingul, dar foarte bine direcționat. Pentru a părea și mai convingători, atacatorii adaptează mesajele pe baza unor informații specifice despre victimă.

**Angler phishing**. O tactică specifică platformelor de comunicare socială, unde atacatorii aruncă "momeli" atractive pentru a captura victime. Ei exploatează subiecte populare sau de actualitate pentru a crea mesaje convingătoare, făcându-le să pară relevante și de încredere.

**Baiting**. Atacatorii ademenesc victimele cu promisiuni irezistibile, cum ar fi acces gratuit la software, reduceri semnificative sau premii exclusive, menite să stârnească curiozitatea sau lăcomia. Oferta tentantă poate include linkuri sau fișiere infectate, care, odată accesate, pot infecta dispozitivul victimei cu malware sau pot duce la furtul de date sensibile.

**Pretexting**. Tactică de fraudă prin care atacatorii creează un pretext fals, o poveste inventată, pentru a obține informații sensibile de la victimă. Scenariul inventat implică adesea uzurparea identității unei persoane de încredere, cum ar fi un coleg sau un reprezentant al unei bănci.

**Impersonation**. Atacatorii pretind a fi altcineva, fie online, fie în persoană, pentru a câștiga încrederea victimelor. Scopul lor este de a manipula victimele să divulge informații confidențiale sau să le determine să realizeze anumite acțiuni dorite de atacatori.

**Extortion**. Atacatorii amenință victimele cu dezvăluirea de informații sensibile dacă nu primesc o răscumpărare. Ei folosesc frica și intimidarea pentru a-și constrânge victimele să le satisfacă cererile.

## Tehnici de colectare a datelor

**Open Source Intelligence** (OSINT). Căutarea informațiilor din surse deschise este un proces de colectare, analiză și diseminare a informațiilor obținute din surse disponibile publicului.

**Typosquatting**. Exploatează greșelile de scriere sau asemănările dintre caractere pentru a redirecționa utilizatorii către site-uri web frauduloase. Atacatorul înregistrează nume de domenii care conțin greșeli comune de scriere sau caractere similare cu cele ale numelor de domenii populare (de exemplu, "facebok.com" în loc de "facebook.com").

**Pharming**. Vizează manipularea serverului DNS (Domain Name System) pentru a redirecționa traficul de internet către site-uri web frauduloase. Spre deosebire de phishing, unde atacatorul trimite email-uri sau mesaje pentru a induce în eroare utilizatorul, pharmingul atacă infrastructura internetului în sine.

**Dumpster Diving**. Metodă ce constă în colectarea de date din coșul de gunoi al unei persoane/companii. De foarte multe ori informațiile cuprinse în documentele aruncate pot crea atacatorilor o cale de intrare (nume de utilizator și parole, indicii privind structura organizațională și sistemele informatice, informații financiare, contracte, documente personale).

**Shoulder Surfing**. Cunoscut sub denumirea de spionaj peste umăr, se realizează prin observarea directă a ecranului dispozitivului victimei de la o distanță apropiată sau prin intermediul unor tehnici de zoom. Informațiile vizate pot include parole, coduri pin, date financiare sau alte detalii confidențiale.

**Tailgating**. Tactică de atac cibernetic care se bazează pe lipsa de atenție a utilizatorilor pentru a obține acces neautorizat la sisteme sau rețele informatice. Atacatorul se "lipește" de un utilizator autorizat pentru a pătrunde într-o zonă restricționată sau pentru a obține acces la resurse protejate.

## Cum să recunoaștem un atac de inginerie socială

**Presiunea**. Atacatorul te grăbește să iei o decizie rapidă, creând un sentiment de urgență care te poate împiedica să gândești limpede.

**Manipularea emoțiilor**. Te poate face să te simți speriat, panicat, vinovat sau plin de compasiune pentru a te manipula.

**Informații sensibile**. Instituțiile sau chiar departamentele dintr-o companie nu solicită prin email/telefon parole sau coduri PIN/token-uri din aplicații, date financiare sau alte informații sensibile.


**Oferte tentante**. Fii atent la cadouri neașteptate pe rețelele sociale sau la "oportunități de afaceri" incredibile, dar limitate în timp.

**Informații incomplete**. Oferă detalii insuficiente sau vagi pentru a ascunde adevăratele sale intenții.

**Email suspect**. Adresa expeditorului conține numere și caractere aleatorii, sau elemente în plus față de domeniul oficial.

Atacatorii de tip inginerie socială utilizează diverse tactici de manipulare pentru a obține informații sensibile sau a induce victimele să execute acțiuni dorite. Suspectează orice solicitare care pare prea bună ca să fie adevărată, verifică identitatea expeditorului și nu oferi niciodată informații sensibile.

## Profilul atacatorului din ingineria socială

| Caracteristici generale | Motivație | Tipuri de atacatori |
|---|---|---|
| • **Inteligență**. Atacatorii de social engineering sunt adesea inteligenți și abili în manipularea oamenilor.<br>• **Carismă**. Carismatici și convingători, câștigă cu ușurință încrederea victimelor.<br>• **Abilități de comunicare**. Au abilități excelente de comunicare, atât verbală, cât și scrisă.<br>• **Cunoștințe psihologice**. O bună înțelegere a psihologiei umane și a modului de a manipula emoțiile oamenilor.<br>• **Răbdare**. Pot fi răbdători și pot aștepta oportunitatea potrivită pentru a-și ataca victimele. | • **Câștig financiar.** Mulți atacatori de social engineering sunt motivați de câștigul financiar. Ei pot fura bani sau informații financiare de la victime.<br>• **Spionaj**. Alții pot fi motivați de spionaj, încercând să obțină informații confidențiale de la companii sau guverne.<br>• **Activism**. Unii atacatori pot fi motivați de activism, dorind să promoveze o cauză politică sau socială. | • **Escroci**: Obținerea de bani sau bunuri materiale prin înșelăciune.<br>• **Hackeri**: Obținerea accesului neautorizat la sisteme informatice sau rețele computerizate.<br>• **Actori statali/Grupări afiliate statelor, Agenții guvernamentale**: implicate în operațiuni de culegere de informații și spionaj cibernetic.<br>• **Activiști**: Promovarea unei cauze specifice prin accesarea sau perturbarea sistemelor. |

Cunoașterea profilului atacatorilor în social engineering este importantă pentru a reduce riscul de a deveni victimă. Implementarea măsurilor de protecție și menținerea vigilenței sunt necesare pentru a contracara amenințarea tot mai complexă a atacurilor de social engineering.

## Profilul grupurilor vulnerabile la atacurile de inginerie socială

| Caracteristici generale | Motivele vulnerabilității |
|---|---|
| • **Persoane în vârstă**. Pot fi mai credule și mai ușor de manipulat, având o experiență redusă cu tehnologiile digitale și tacticile de inginerie socială.<br>• **Persoane cu dizabilități**. Pot avea dificultăți în a recunoaște indiciile de fraudă sau în a se proteja împotriva manipulării.<br>• **Persoane cu probleme de încredere**. Pot fi mai predispuse la a se conforma solicitărilor insistente sau a fi influențate de emoții.<br>• **Persoane stresate**. Susceptibile la erori de judecată sau la a lua decizii impulsive sub presiune.<br>• **Angajați cu acces la date sensibile**. Pot fi ținta unor atacuri specifice care exploatează vulnerabilitățile din cadrul organizației. | • **Lipsa de conștientizare**. Lipsa cunoștințelor despre tehnicile de social engineering și riscurile asociate.<br>• **Naivitatea**. Tendința de a avea încredere excesivă în alții și de a lua de bune informațiile primite.<br>• **Curiozitatea**. Atracția pentru momeli digitale sau solicitări neobișnuite.<br>• **Presiunea**. Sentimentul de urgență sau obligația de a se conforma solicitărilor insistente.<br>• **Lipsa de resurse**. Acces limitat la instruire, asistență tehnică sau soluții de securitate. |

Identificarea grupurilor vulnerabile la atacurile de social engineering este importantă pentru a le putea oferi protecția și asistența necesară. Implementarea de strategii specifice de educare, sensibilizare și sprijin poate contribui semnificativ la reducerea riscului de victimizare a acestor grupuri.

## Aspecte Legale

**Legea nr. 190/2018** privind GDPR, reglementează modul de colectare, stocare și utilizare a datelor cu caracter personal. Atacurile de social engineering pot încălca această lege prin obținerea frauduloasă a datelor personale.

**Legea nr. 365/2002** privind comerțul electronic, reglementează aspectele juridice ale tranzacțiilor online. Atacurile de phishing pot încălca această lege prin inducerea în eroare a utilizatorilor pentru a dezvălui informații sensibile sau a efectua tranzacții frauduloase.

**Legea 286/2009** (Codul Penal), fraude comise prin sisteme informatice și mijloace de plată electronice: frauda informatică (art. 249), efectuarea de operațiuni financiare în mod fraudulos (art. 250), infracțiuni contra siguranței și integrității sistemelor și datelor informatice: accesul ilegal la un sistem informatic (art. 360), interceptarea ilegală a unei transmisii de date informatice (art. 361), alterarea integrității datelor informatice (art. 362), perturbarea funcționării sistemelor informatice (art. 363), transferul neautorizat de date informatice (art. 364), operațiuni ilegale cu dispozitive sau programe informatice (art.365).

## Strategii de educare și conștientizare a publicului

**Campanii de informare publică**. Difuzarea de materiale informative prin intermediul mass-media, rețelelor sociale și a platformelor online.

**Programe de educație în școli și universități**. Integrarea de module specifice în curriculumul educațional pentru a informa tinerii despre riscurile online și metodele de protecție.

**Seminarii și workshop-uri**. Prezentarea de informații detaliate și interactive pentru diferite categorii de public (persoane în vârstă, persoane cu dizabilități etc.).

**Resurse online**. Dezvoltarea de platforme web, bloguri și materiale informative ușor accesibile publicului.

## Strategii de conștientizare a angajaților din organizații

**Instruiri periodice**. Organizarea de sesiuni de instruire pentru a informa angajații despre tacticile de social engineering și metodele de protecție specifice mediului organizațional.

**Simulări de atacuri**. Realizarea de exerciții practice pentru a testa nivelul de conștientizare al angajaților și a le oferi experiență în gestionarea atacurilor simulate.

**Campanii interne de sensibilizare**. Utilizarea de materiale informative, postere, emailuri și alte canale interne de comunicare pentru a menține un nivel constant de conștientizare.

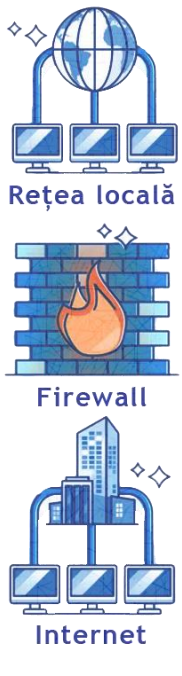
**Implementarea unei culturi a securității**. Promovarea unei culturi organizaționale care pune accent pe securitatea cibernetică și responsabilitatea individuală.

## Metode pentru prevenirea și detectarea atacurilor de inginerie socială

**Tehnologii de protecție a emailului**. Filtre de spam și phishing pentru a bloca emailurile suspecte. Analiza aprofundată a conținutului pentru a identifica tentativele de manipulare. Autentificarea emailului (SPF[1], DKIM[2], DMARC[3]) pentru a verifica identitatea expeditorului.

**Soluții de securitate endpoint.** Antiviruși și anti-malware pentru a detecta/bloca atacurile de social engineering. Monitorizarea comportamentului utilizatorului pentru a detecta activități suspecte. Controlul accesului pentru a restricționa accesul la resursele sensibile.

**Instrumente de analiză a rețelei.** Monitorizarea traficului de rețea pentru a identifica anomalii ce pot indica un atac în curs de desfășurare. Identificarea și oprirea conexiunilor la resursele folosite de agresori. Examinarea modului de utilizare a rețelei de către utilizatori pentru a găsi tipare neobișnuite.




**Inteligența artificială și Machine Learning.** Utilizarea algoritmilor de învățare automată pentru a identifica emailurile de phishing și alte tentative de fraudă. Detectarea anomaliilor în comportamentul utilizatorului care pot indica un atac de social engineering.

**Principiul celui mai mic privilegiu și controlul accesului**. Acordă acces doar la resursele strict necesare pentru a-și îndeplini sarcinile. Monitorizează periodic accesul pentru a preveni abuzurile.

**Planuri de răspuns la incidente și politici de securitate**. Documentează clar procedurile de urmat în caz de incident de securitate. Toți membrii echipei trebuie să cunoască rolul lor și calea de urmat.

**Cele mai bune practici pentru autentificarea utilizatorilor**. Promovează parole complexe, unice, stocate într-un manager de parole. Evită parolele ușor de ghicit.

**Canale de comunicare securizate și criptate**. Protejează datele sensibile prin criptare și utilizează canale de comunicare securizate, cum ar fi VPN-uri și email criptat.

**Gestionarea frecventă a patch-urilor și actualizărilor de software**. Menține software-ul la zi pentru a elimina vulnerabilitățile cunoscute. Implementează un proces automat de actualizare și instruiește personalul să instaleze prompt patch-urile de securitate.

Important de reținut, nici o soluție nu este perfectă, o combinație de metode este necesară pentru a oferi o protecție eficientă împotriva atacurilor de social engineering.

---

[1] **SPF (Sender Policy Framework)**:SPF permite definirea serverelor autorizate să trimită emailuri pentru un domeniu, verificând adresele IP ale expeditorilor împotriva unei liste din DNS.

[2] **DKIM (DomainKeys Identified Mail)**:DKIM asociază un domeniu cu un email printr-o semnătură digitală, verificată cu o cheie publică din DNS, asigurând că mesajul nu a fost alterat

[3] **DMARC (Domain-based Message Authentication, Reporting, and Conformance)**:DMARC utilizează SPF și DKIM pentru a evalua autenticitatea emailurilor, oferind indicații despre cum să se procedeze cu mesajele suspecte și rapoarte despre livrarea acestora.

## Impactul tehnologiilor noi asupra ingineriei sociale

Tehnologiile și societatea se transformă continuu. Odată cu acestea sunt adaptate și tacticile de social engineering. Atacatorii exploatează noile tendințe pentru a manipula și exploata victimele, făcând imperativă adaptarea strategiilor de protecție.

**Rețelele sociale ca armă**. Platformele sociale oferă o sursă bogată de informații personale pentru atacatori. Cu o simplă navigare pe profiluri, poți construi relații false de încredere și poți personaliza mesaje de tip "spear phishing" pentru a maximiza eficacitatea atacurilor.

**Inteligența artificială aliatul întunecat al atacatorilor**. Deepfake-urile video și audio generate de Inteligența Artificială (AI) devin tot mai sofisticate oferind manipulatorilor o armă nouă și extrem de convingătoare. Automatizarea anumitor etape ale atacurilor de tip "inginerie socială" le face mai eficiente și mai ușor de scalat, sporind semnificativ riscurile pentru organizații și alte persoane.

**Munca de la distanță, oportunitate pentru atacatori.** Angajații care lucrează de la distanță pot fi mai vulnerabili la atacuri, neavând protecția unei rețele de birou. Atacurile se pot adapta la specificul muncii de la distanță, simulând emailuri legate de livrări, probleme IT sau alte aspecte relevante.

**Schimbări demografice**. Populația globală este în curs de îmbătrânire, iar persoanele în vârstă pot fi mai vulnerabile la atacurile de social engineering din cauza lipsei de familiaritate cu tehnologiile digitale. Atacurile se pot adapta la specificul acestei categorii, exploatând temerile legate de probleme medicale, financiare sau alte aspecte sensibile.

## Cum te aperi de atacurile de inginerie socială

| | |
|---|---|
| **Fii vigilent și suspicios** | • Fii atent la semnele de alarmă, cum ar fi solicitări urgente, oferte prea bune pentru a fi adevărate sau presiunea de a acționa rapid.<br>• Verifică identitatea apelantului sau expeditorului emailului. Nu te baza pe afișajul ID-ului apelantului sau pe adresa de email aparentă.<br>• Nu da niciodată informații personale sau financiare prin telefon, email sau pe internet, cu excepția cazului în care ești sigur de identitatea destinatarului. |
| **Protejează-ți datele și parolele** | • Folosește parole unice și complexe pentru fiecare cont online.<br>• Nu reutiliza parolele și nu le partaja cu nimeni.<br>• Activează autentificarea multi-factor (MFA ) ori de câte ori este posibil.<br>• Fii atent la ce informații personale postezi online. |
| **Fii atent la emailuri și linkuri suspecte** | • Nu deschide emailuri de la expeditori necunoscuți.<br>• Nu faceți clic pe linkuri din emailuri sau mesaje suspecte.<br>• Verifică adresa URL a site-ului web pe care îl vizitezi înainte de a introduce orice informație personală. |
| **Utilizează software de securitate** | • Instalează un antivirus și un anti-malware pe toate dispozitivele tale.<br>• Instalează actualizările de software imediat ce sunt disponibile.<br>• Efectuează scanări regulate pentru a detecta programe malware. |
| **Informează-te** | • Citește despre cele mai noi tehnici de inginerie socială.<br>• Participă la cursuri de securitate cibernetică.<br>• Discută despre securitatea online cu familia și prietenii. |
| **Răspunsul în caz de atac** | • Dacă suspectezi că ai fost victima unui atac de inginerie socială, schimbă imediat parolele și contactează banca sau instituția financiară.<br>• Raportează atacul autorităților competente. |

## Concluzii

O populație informată și conștientă este mai puțin vulnerabilă la atacurile de tip "inginerie socială". Implementarea de strategii specifice de educare și conștientizare poate îmbunătăți semnificativ securitatea cibernetică a organizațiilor și reduce costurile financiare și reputaționale asociate cu victimizarea. Investiția în programe adaptate nevoilor specifice publicului este necesară pentru a combate acest fenomen și a crea un mediu online mai sigur pentru toți. Organizațiile și indivizii trebuie să fie conștienți de noile tendințe și să adapteze strategiile de protecție la noile realități sociale și tehnologice.

Acest ghid a fost realizat de următorii experți ai Directoratului Național de Securitate Cibernetică (DNSC): **Daniel Abotezătoaei, Irina Nemoianu, Mihaela Dan, Alex Leoreanu**

## Bibliografie


Amrut Kajave, S. A. (2022, 12). *How Cyber criminal Use Social Engineering To Target Organizations*. Preluat de pe https://www.researchgate.net/publication/366237883_How_Cyber_criminal_Use_Social_Engineering_To_Target_Organizations

Asad, A. (2024). *Social Engineering Attacks: Techniques, Impacts, and Mitigation Strategies*. Preluat de pe https://www.researchgate.net/publication/377382644_Social_Engineering_Attacks_Techniques_Impacts_and_Mitigation_Strategies

CISCO. (fără an). *https://skillsforall.com/course/ethical-hacker?courseLang=en-US*. Preluat de pe https://skillsforall.com/course/ethical-hacker?courseLang=en-US

CISCO. (fără an). *https://www.cisco.com/*. Preluat de pe https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html

Consiliul European. (2024, 0 24). *Cybersecurity: social engineering*. Preluat de pe https://www.consilium.europa.eu/en/policies/cybersecurity/cybersecurity-social-engineering/

Dragomir, A. M. (2018, 04 02). Amenințări de tip social engineering, prin intermediul rețelelor de socializare. *Buletinul Universității Naționale de Apărare „Carol I”, 5*(1), 63-67. Preluat de pe https://revista.unap.ro/index.php/revista/article/view/400/376

E.Frumento, R. F. (2016). *The role of Social Engineering in evolution of attacks*. Preluat de pe https://www.researchgate.net/publication/341642102_The_role_of_Social_Engineering_in_evolution_of_attacks

ENISA. (2023, 07). *Artificial Intelligence and Cybersecurity Research*. Preluat de pe https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research/@@download/fullReport

ENISA. (2024, 01 26). *Engineering Personal Data Protection in EU Data Spaces*. Preluat de pe https://www.enisa.europa.eu/publications/engineering-personal-data-protection-in-eu-data-spaces

Mitnick, K. (fără an). *The History of Social Engineering & How to Stay Safe Today*. Preluat de pe https://www.mitnicksecurity.com/the-history-of-social-engineering

Nina Klimburg-Witjes, A. W. (2021). Hacking Humans? Social Engineering and the Construction of the “Deficient User” in Cybersecurity Discourses. *Science, Technology, & Human Values, 46*(6), 1316-1339. Preluat de pe https://journals.sagepub.com/doi/epub/10.1177/0162243921992844

Stoica, A. (2021). Ingineria socială – noul joc al înșelăciunii. *Revista Română de Informatică și Automatică, 31*(3), 57-68. Preluat de pe https://rria.ici.ro/documents/106/art._Stoica.pdf

Wang, Z. Z. (2021). *Social engineering in cybersecurity: a domain ontology and knowledge graph application examples*. Preluat de pe https://doi.org/10.1186/s42400-021-00094-6




**TLP:CLEAR** se poate folosi atunci când informațiile prezintă un risc minim de utilizare abuzivă, în conformitate cu normele și procedurile aplicabile pentru publicare. Sub rezerva regulilor standard ale drepturilor de autor, informațiile TLP:CLEAR pot fi partajate fără restricții.