DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Cum ne protejăm eficient în mediul online?

Directoratul Național de Securitate Cibernetică

18 martie 2025

Cine este DNSC?

Misiune

Supraveghează securitatea cibernetică națională și asigură reziliența spațiului cibernetic civil al României.

Obiective

- Infrastructură sigură și fiabilă pentru spațiul cibernetic național.
- Dezvoltarea strategiilor și politicilor de securitate cibernetică.
- Promovarea colaborării între sectoarele public și privat.

Poți să fii 100% protejat în spațiul cibernetic?

dacă ai suspiciuni, cel mai bine e să eviți să accesezi

verifică dacă sursa care face publică o informație (alarmantă, exagerată) este oficială

folosiți mereu parole cu un nivel de complexitate ridicat

atenție sporită linkurilor pe care le accesezi (de unde provine, de ce am primit?)

schimbă periodic parolele

asigură-te că ai mereu copii de rezervă ale datelor tale

folosește o soluție antivirus eficientă

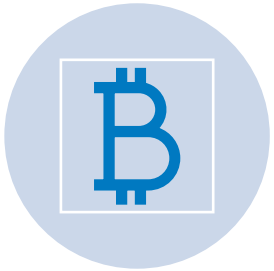
nu folosiți termeni uzuali pentru crearea parolelor

folosește versiuni actualizate ale sistemelor de operare

este important să ne educăm apropiații

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Siguranța în mediul online - riscuri și amenințări



Preluarea controlului asupra contului

(account takeover attack - ATO)

Phishing

Distribuția de malware

Inginerie socială

Siguranța în mediul online – recomandări

- Parole puternice
- Autentificare în doi pași (2FA)
- Actualizări regulate ale parolelor
- Revizuirea setărilor de confidențialitate
- Evită să postezi informații sensibile
- Atenție la încercările de phishing
- Actualizări regulate ale aplicațiilor
- Verificarea sesiunilor active
- Folosirea unui VPN
- Evitarea aplicațiilor neoficiale

Amprenta digitală (digital footprint)

Tot ce postăm, căutăm sau accesăm pe internet lasă urme.

Ce poate fi afectat

- Imaginea personală și profesională, mai ales în procesul de angajare.
- Situații de șantaj sau utilizare abuzivă a informațiilor.

Cum să îți controlezi amprenta digitală

- Gândește-te bine înainte de a publica ceva.
- Asigurați-te că știi sigur cu cine comunici.
- Utilizează setări stricte de confidențialitate.
- Caută-te periodic online și șterge conținutul vechi neadecvat.
- Folosește unelte precum "Google Alerts" pentru a monitoriza mențiunările tale online.

Deepfake - ce înseamnă?

Definiție

- Manipularea digitală a unei înregistrări video, audio sau a unei imagini
- Realizată cu ajutorul inteligenței artificiale (IA) sau a altor programe specializate

Caracteristici cheie

- Realism ridicat: Poate fi foarte greu de distins de conținutul autentic
- Manipulare complexă: Poate schimba fețe, voci și gesturi
- Creat cu IA: Utilizează tehnologii avansate de învățare automată

Domenii de utilizare a Deepfake

Manipularea opiniei publice

- Crearea de conținut fals atribuit liderilor sau personalităților publice
- Răspândirea dezinformărilor și știrilor false

Activități frauduloase

- Înșelătorii financiare prin impersonare
- Șantaj cu materiale compromițătoare fabricate
- Furt de identitate pentru activități ilegale

Abuz și hărțuire

- Crearea și distribuirea de conținut compromițător fals
- Modificarea fără consimțământ a imaginilor cu conținut explicit

Impersonare digitală

- Crearea de conturi false pe rețelele sociale
- Falsificarea identității pentru diverse scopuri ilicite


DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ
Deepfake audio limba chine

Cum identificăm deepfake?

- Imperfecțiuni ale feței (ochii, dinții, trăsăturile faciale)
- Nesincronizarea vorbirii/sunetului și a mișcării buzelor
- Comportament nefiresc
- Probleme de perspectivă
- Detalii biologice inconsistente
- Probleme de rezoluție și claritate
- Lipsa continuității în mișcări sau expresii
- Instrumente de detectare

Cum să nu fii păcălit de deepfake-uri?

- Nu crede tot ce vezi online
- Caută semne de manipulare
- Verifică sursa
- Nu te baza pe o singură sursă
- Folosește instrumente de verificare
- Învață despre Deepfake-uri

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.

Tehnici de manipulare în ingineria socială

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

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.

DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Cum ne apărăm de atacurile tip 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.
- Verifică identitatea apelantului sau expeditorului emailului. Nu te baza pe afișajul ID-ului apelantului sau pe adresa de email aparentă.
- 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.
- Nu reutiliza parolele și nu le partaja cu nimeni.
- Activează autentificarea multi-factor (MFA) ori de câte ori este posibil.
- Fii atent la ce informații personale postezi online.

Fii atent la emailuri și linkuri suspecte

- Nu deschide emailuri de la expeditori necunoscuți.
- Nu faceți clic pe linkuri din emailuri sau mesaje suspecte.
- Verifică adresa URL a site-ului web pe care îl vizitezi înainte de a introduce orice informație personală.

Cum ne apărăm de atacurile tip inginerie socială?

Utilizează software de securitate

- Instalează un antivirus și un anti-malware pe toate dispozitivele tale.
- Instalează actualizările de software imediat ce sunt disponibile.
- Efectuează scanări regulate pentru a detecta programe malware.

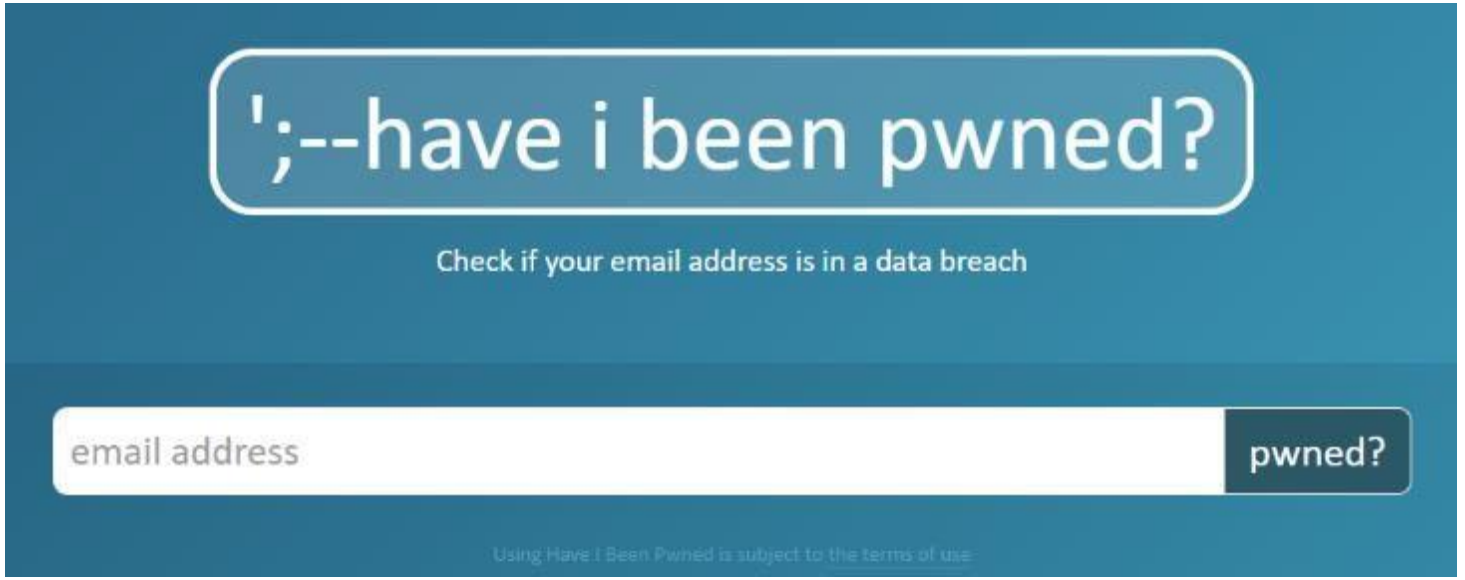
Informează-te

- Citește despre cele mai noi tehnici de inginerie socială.
- Participă la cursuri de securitate cibernetică.
- Discută despre securitatea online cu familia și prietenii.

Răspunsul în caz de atac

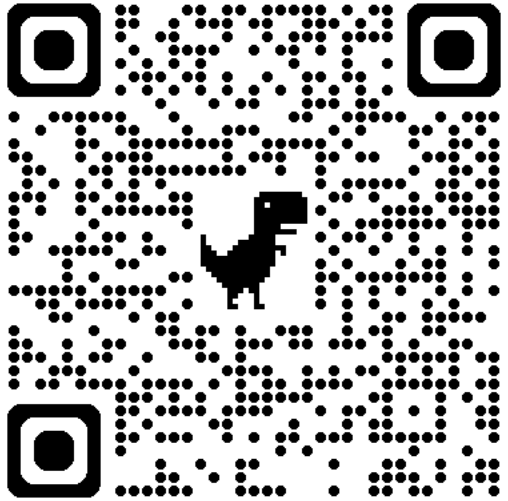
- Dacă suspectezi că ai fost victima unui atac de inginerie socială, schimbă imediat parolele și contactează banca sau instituția financiară.
- Raportează atacul autorităților competente

Instrumente online utile



https://haveibeenpwned.com/

Instrumente online utile

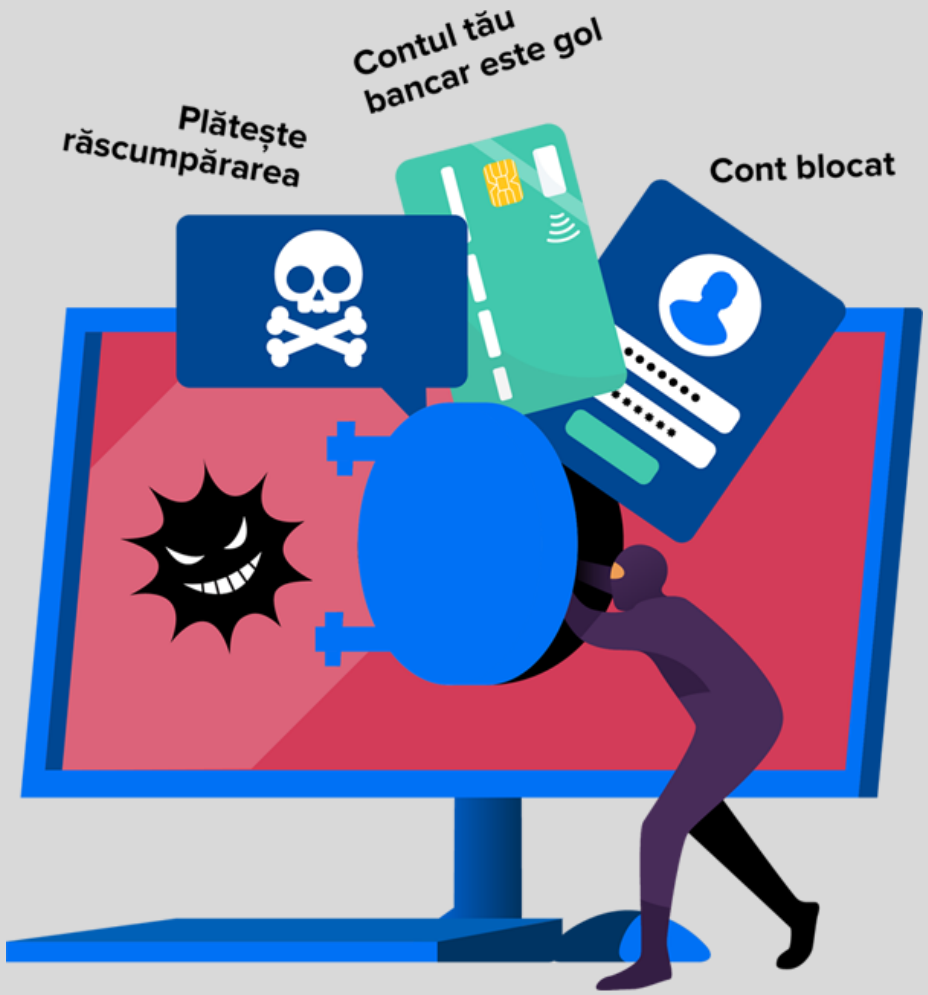


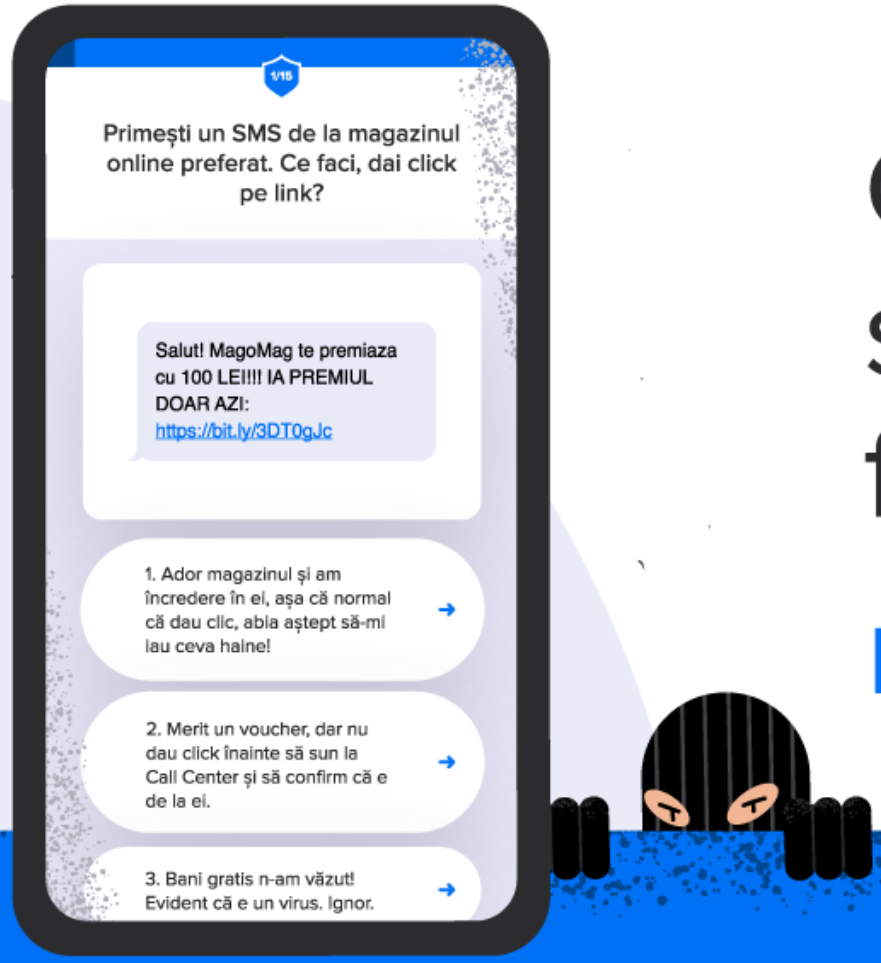
https://www.passwordmonster.com/

SIGURANȚA ONLINE.RO

Proiectul național de conștientizare Siguranța Online

sigurantaonline.ro





Crezi că te pricepi să te ferești de fraudele online?

FĂ-ȚI TESTUL!

SIGURANȚA ONLINE.RO

O campanie inițiată de Poliția Română, DNSC și ARB

POLIȚIA ROMÂNĂ

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Susținută de Dreptul la Banking

#DREPTUL LA BANKING

Mulțumim!

🌐 **Accesați dnsc.ro pentru mai multe informații și resurse utile pentru siguranța digitală:**

✅ Ghiduri practice pentru protecția datelor și a dispozitivelor
✅ Recomandări pentru prevenirea atacurilor cibernetice
✅ Sfaturi pentru navigarea în siguranță online

📢 Urmăriți-ne pe rețelele sociale pentru noutăți și alerte de securitate.
linktr.ee/dnsc.ro

Notă

TLP:CLEAR = Destinatarii pot transmite informația oricui, nu există limitări privind divulgarea. 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.

Sursă: https://www.first.org/tlp/