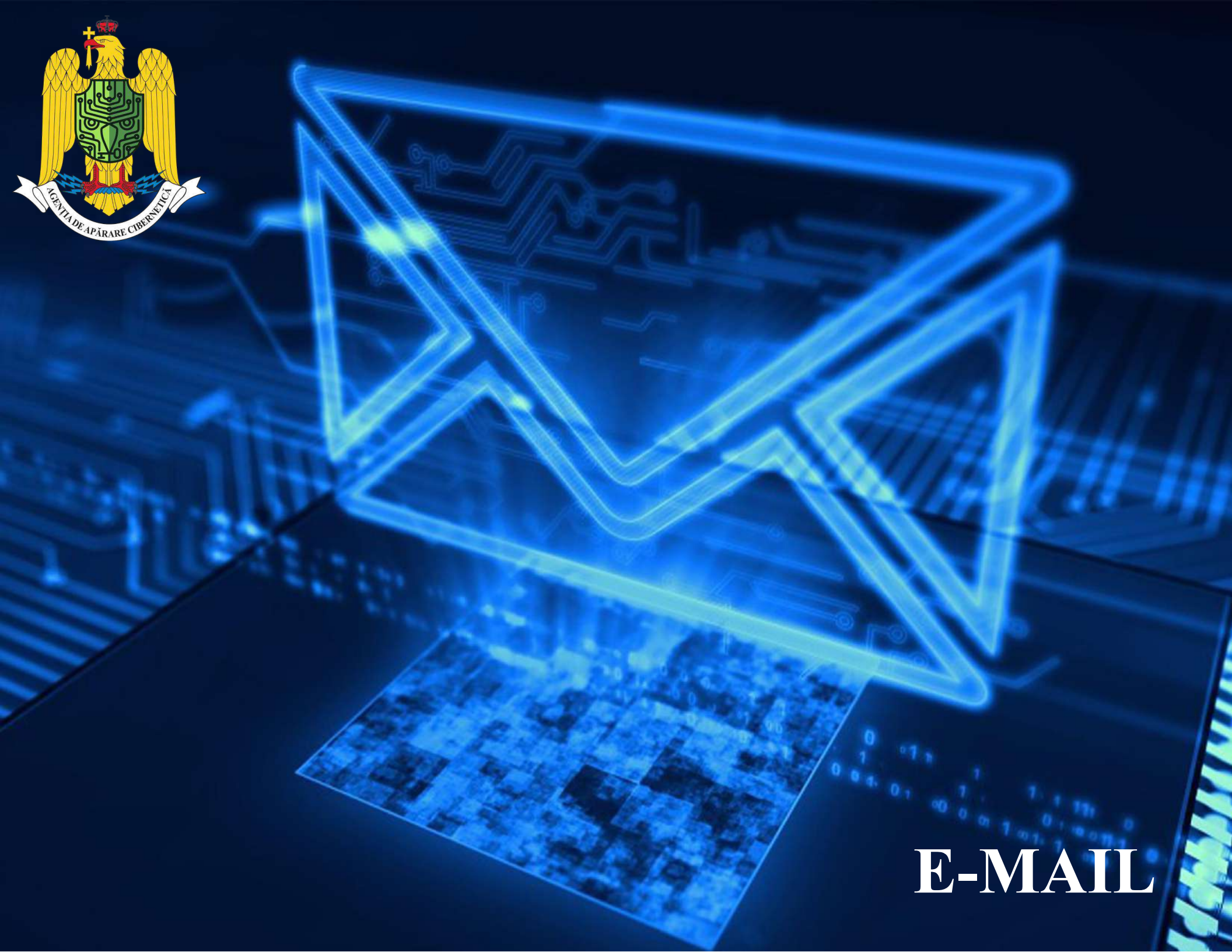

AGENȚIA DE APĂRARE CIBERNETICĂ
E-MAIL

GHID DE BUNE PRACTICI PENTRU UTILIZAREA SERVICIULUI DE E-MAIL

CUPRINS

INTRODUCERE

Serviciul de e-mail este un sistem electronic complex și versatil care facilitează schimbul de mesaje electronice între utilizatori prin intermediul rețelelor locale și al internetului. Acest sistem oferă posibilitatea de a trimite, primi și gestiona mesaje electronice, cunoscute și sub denumirea de e-mailuri, utilizând adrese de e-mail unice și valide.

Utilizatorii pot compune și trimite mesaje către o anumită persoană sau entitate, aceasta din urmă primind mesajul într-un timp foarte scurt, indiferent de poziția geografică. De asemenea, utilizatorii pot organiza și gestiona mesajele primite în diverse moduri, inclusiv prin crearea de foldere sau etichete pentru marcarea mesajelor importante sau eliminarea mesajelor nesolicitate. Totodată, utilizatorii au posibilitatea de a atașa fișiere sau documente la mesajele trimise, facilitând astfel partajarea de informații și protejând totodată mediul înconjurător.

Un mare avantaj al e-mailului este că utilizatorii își pot accesa căsuța de e-mail și mesajele primite/trimise de pe diverse dispozitive, precum calculatoare, smartphone-uri sau tablete, și pot sincroniza modificările făcute pe un dispozitiv pe toate celelalte dispozitive conectate.

Serviciul de e-mail este un instrument important în comunicarea modernă, utilizat atât în mediul personal, pentru a menține legătura cu familia și prietenii, cât și în mediul profesional, pentru a facilita colaborarea și schimbul de informații între colegi și parteneri de afaceri. Exemple de servicii populare de e-mail includ Gmail, Yahoo Mail, Outlook, etc.

În prezent, e-mailul este una dintre cele mai frecvente metode de înșelătorie și furt de informații. Multe mesaje pot arăta perfect legitime și pot părea trimise de colegi sau persoane cu funcții de conducere. Respectarea regulilor de siguranță este esențială pentru protejarea informațiilor și a sistemelor.

STRUCTURA UNUI E-MAIL

Formatul standard al mesajului e-mail este definit în RFC 5322, care stabilește, printre altele, că mesajul este compus din două părți:

- **Antetul (Header)** – conține informații despre mesaj, precum expeditorul, destinatarul, subiectul și data trimiterii; (1)
- **Corpul (Body)** – reprezintă conținutul propriu-zis al mesajului. (2)

Antetul conține cel puțin următoarele câmpuri:

- **From (Expeditor)** – adresa de e-mail a expeditorului; (3)
- **To (Destinatar)** – adresa de e-mail a destinatarului; (4)
- **Subject (Subiect)** – un rezumat al conținutului mesajului; (5)
- **Date (Data)** – data și ora trimiterii mesajului. (6)

Alte câmpuri utilizate frecvent în antet sunt:

- **Cc (Carbon Copy)** – o copie a mesajului este trimisă și la adresa sau adresele din acest câmp, vizibile pentru toți destinatarii;
- **Bcc (Blind Carbon Copy)** – similar cu Cc, însă adresele din acest câmp nu sunt vizibile pentru ceilalți destinatari.


Plata acceptata - comanda 140397182
Mesaje primite ×
ING_pentru_Digi@ing.ro
către eu
13:42 (acum 49 de minute)
Confirmare plata
DIGI
Conectați #Nelimitat
Salut!
Iti multumim pentru plata efectuata prin ING WebPay in valoare de 40.00 RON.
Acest email este o confirmare a platii si te rugam sa il pastrezi o perioada.
1
2
3
4
5
6

AVANTAJELE SERVICIULUI DE E-MAIL

- **Securitatea comunicației** – serviciile moderne de e-mail pot utiliza standarde și mecanisme de protecție care ajută la verificarea sursei mesajelor și la protejarea transmiterii acestora. Nivelul real de securitate depinde de configurarea sistemelor și de atenția utilizatorilor;

- **Rapiditate** – mesajele de e-mail pot fi trimise și recepționate aproape instantaneu, permițând comunicarea rapidă între utilizatori, indiferent de distanța fizică dintre aceștia;

- **Accesibilitate și mobilitate** – serviciile de e-mail sunt disponibile pe mai multe platforme, inclusiv pe computere, smartphone-uri și tablete, permițând accesul la căsuța de e-mail ori de câte ori există conexiune la internet;

- **Organizare și gestionare** – e-mailurile pot fi organizate prin foldere, etichete sau categorii, facilitând căutarea și regăsirea mesajelor. De asemenea, serviciul păstrează istoricul conversațiilor, permițând revizuirea mesajelor anterioare;

- **Asincronism** – e-mailul permite destinatarilor să răspundă atunci când au timpul și disponibilitatea necesară, fără a fi nevoie de comunicare în timp real;

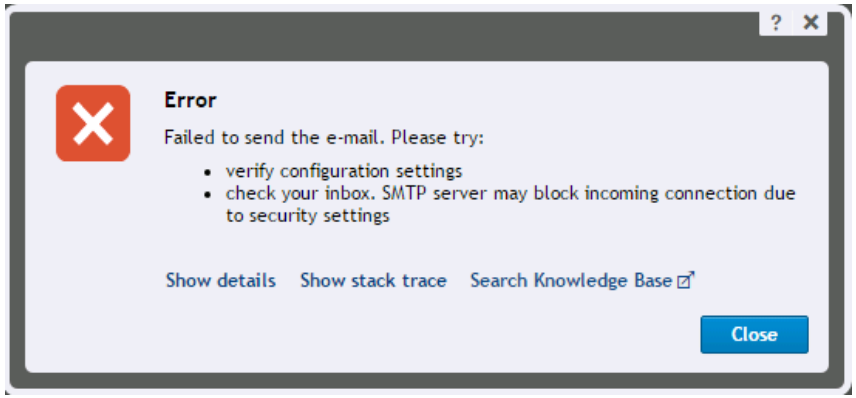
- **Globalitate** – e-mailul poate fi utilizat pentru a comunica cu persoane din întreaga lume, fără limitări geografice sau de fus orar;

- **Fișiere atașate** – posibilitatea de a atașa fișiere facilitează partajarea informațiilor și colaborarea între utilizatori;

- **Ecologie** – utilizarea e-mailului reduce necesitatea tipăririi și transportului documentelor, contribuind la diminuarea impactului asupra mediului.

DEZAVANTAJELE SERVICIULUI DE E-MAIL

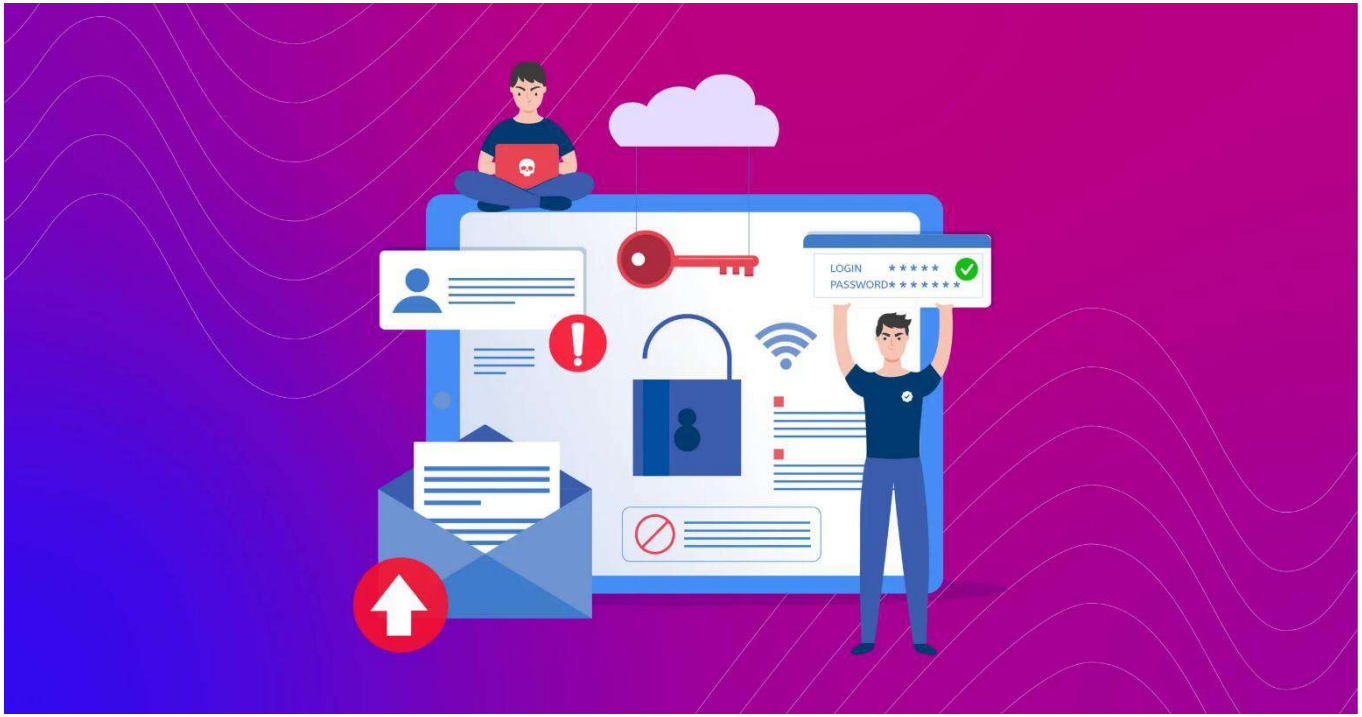
- **Erori de comunicare** – e-mailurile pot duce la confuzie sau neînțelegeri, deoarece este uneori dificil de înțeles tonul sau contextul mesajului;
- **Spam** – utilizatorii pot primi mesaje nedorite, unele dintre acestea putând conține linkuri sau fișiere atașate periculoase;
- **Suprasolicitare** – primirea unui volum mare de mesaje poate îngreuna identificarea și gestionarea celor importante;
- **Lipsa feedback-ului imediat** – e-mailul nu oferă comunicare în timp real, ceea ce poate fi o problemă atunci când este necesar un răspuns rapid;
- **Erori tehnice** – pot apărea probleme de sistem care să întârzie trimiterea sau primirea mesajelor;
- **Ineficiență pentru discuții complexe** – e-mailul nu este cea mai bună opțiune pentru discuții care necesită feedback rapid de la mai multe persoane;
- **Mesaje false foarte convingătoare** – unele e-mailuri pot părea trimise de persoane cunoscute și pot determina utilizatorii să divulge informații fără verificare;
- **Presiune prin urgență falsă** – mesaje care creează grabă și forțează luarea unor decizii greșite.



SECURITATEA SERVICIULUI DE E-MAIL

Securitatea serviciului de e-mail se referă la ansamblul de măsuri și reguli aplicate pentru protejarea confidențialității, integrității și disponibilității informațiilor transmise și stocate prin e-mail, asigurând o comunicare sigură și fiabilă.

Aceste măsuri urmăresc prevenirea accesului neautorizat, interceptării mesajelor, atacurilor de tip phishing, distribuirii de programe malițioase și altor amenințări care pot afecta utilizatorii și sistemele.



TIPURI DE ATACURI CIBERNETICE CE POT FI LANSATE PRIN INTERMEDIUL SERVICIULUI DE E-MAIL

- **Fraudă** – frauda prin intermediul e-mailului poate lua o varietate de forme, de la înșelătoriile clasice care vizează utilizatorii, precum solicitarea unor sume de bani în avans pentru o presupusă moștenire sau un beneficiu, până la mesaje adresate instituțiilor sau companiilor, în care atacatorii încearcă să păcălească personalul financiar pentru a obține transferuri de bani sau informații sensibile. De regulă, mesajele sunt create astfel încât să pară că provin dintr-o sursă legitimă;

- **Phishing** – scopul acestui tip de atac este determinarea utilizatorului să furnizeze informații sensibile, precum date personale, credențiale de acces sau informații bancare. Atacurile redirecționează frecvent utilizatorii către pagini web false care colectează datele introduse sau încearcă să convingă victima să trimită aceste informații la o adresă de e-mail controlată de persoane rău intenționate. Falsificarea domeniilor și a adreselor de expediere este o practică des întâlnită;

- **Malware** – tipurile de programe malițioase livrate prin e-mail includ, printre altele, spyware, adware și ransomware. Codul periculos poate fi transmis prin fișiere atașate infectate sau prin linkuri care duc către fișiere găzduite pe servicii online aparent legitime;

- **Mesaje „din interior" (impersonare)** – atacatorii se dau drept colegi, superiori sau persoane cunoscute și solicită documente, informații sau acțiuni urgente. Aceste mesaje nu conțin întotdeauna linkuri sau fișiere periculoase, ci se bazează pe încredere și presiune psihologică;

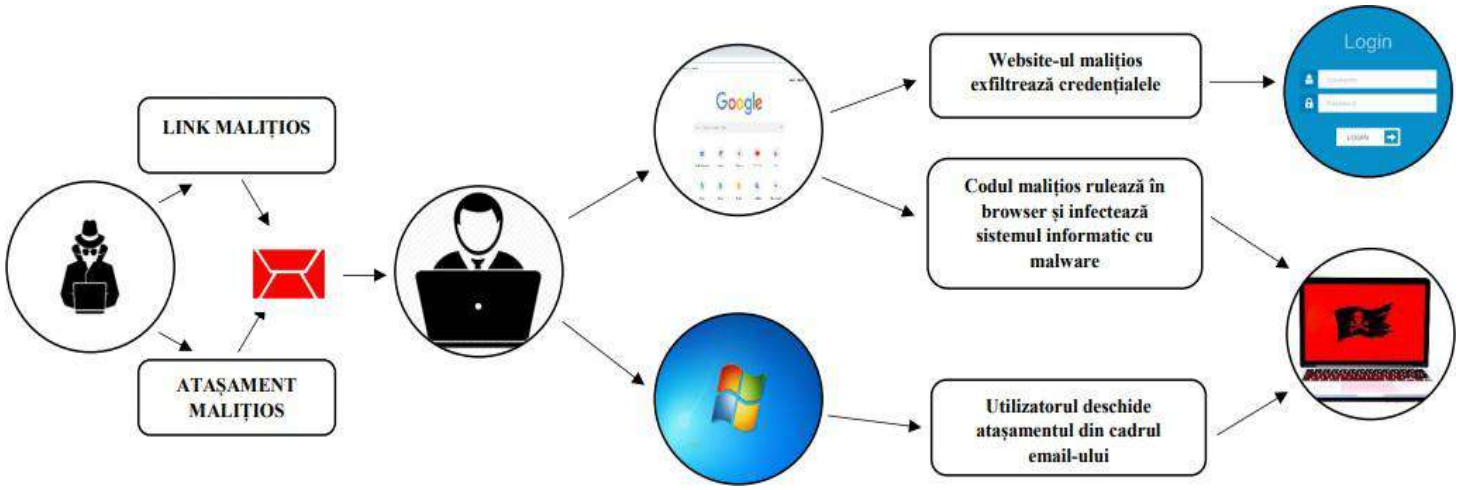
- **Linkuri către servicii cunoscute** – mesajele conțin linkuri care duc către platforme aparent legitime, precum servicii de stocare online, unde sunt găzduite fișiere sau pagini false ce solicită parole sau alte date sensibile;

- **Mesaje cu cod QR** – mesajele includ un cod care, scanat cu telefonul, redirecționează utilizatorul către un site fals, ocolind uneori filtrele de securitate ale sistemelor de e-mail;

- **Mesaje automate și personalizate** – atacatorii folosesc sisteme automate pentru a crea mesaje bine redactate, adaptate numelui, funcției sau activității utilizatorului, crescând șansele ca mesajul să fie considerat legitim;

CUM POATE FI COMPROMISĂ CĂSUȚA DE E-MAIL?

- **Accesarea unui link sau a unui fișier atașat periculos**, primit prin e-mail fără verificare prealabilă, poate duce la furtul de date sensibile, precum credențialele de acces, sau la infectarea dispozitivului cu programe malițioase;



- **Liste de credențiale compromise anterior** – în ultimii ani au avut loc numeroase scurgeri de date, iar listele cu adrese de e-mail și parole sunt vândute sau distribuite ilegal. O persoană rău intenționată poate folosi aceste informații pentru a încerca să preia controlul conturilor utilizatorilor;

- **Tehnici de inginerie socială** – atacatorii folosesc mesaje create pentru a exploata reacții umane precum frica, graba sau dorința de a ajuta. De exemplu, pot pretinde că sunt o persoană cunoscută sau o rudă și solicită ajutor financiar pentru o situație „urgentă”. În alte cazuri, trimit mesaje care anunță probleme grave cu un cont sau un serviciu și cer accesarea unui link pentru „rezolvare”. Aceste linkuri duc, de regulă, către pagini false care imită site-uri legitime, unde utilizatorii sunt determinați să își introducă datele de acces.

- **Brute-force** – compromiterea căsuței de e-mail poate avea loc și fără implicarea directă a utilizatorului, prin încercarea repetată de parole până la găsirea celei corecte. După preluarea controlului asupra unei căsuțe legitime, atacatorii pot citi mesajele, sustrage informații și pot folosi adresa compromisă pentru a trimite mesaje periculoase sau spam către alte persoane.

- **Spyware** – sistemul utilizatorului poate fi infectat cu un program de tip spyware care înregistrează activitatea, inclusiv ce este tastat, și transmite aceste informații către atacator. Astfel pot fi furate numele de utilizator și parolele, inclusiv cele pentru e-mail.

- **Aplicații sau servicii conectate la e-mail** – unele aplicații externe pot primi acces la căsuța de e-mail pentru citire sau trimitere de mesaje. Dacă aceste aplicații sunt nesigure sau compromise, atacatorii pot obține acces indirect la cont;

- **Confirmarea involuntară a adresei de e-mail** – răspunsul la mesaje suspecte sau apăsarea butoanelor de „dezabonare” din surse necunoscute poate confirma atacatorilor că adresa este activă, crescând volumul de atacuri;

- **Rețele nesigure** – conectarea la e-mail prin rețele Wi-Fi publice sau nesigure poate permite interceptarea datelor sau redirecționarea către pagini false;

Majoritatea compromiterilor au loc prin neatenție sau grabă. Verificarea atentă a mesajelor și respectarea regulilor de siguranță reduc semnificativ riscul de pierdere a informațiilor.

CUM POATE FI INFECTAT SISTEMUL INFORMATIC PRIN INTERMEDIUL FIȘIERELOR ATAȘATE MALIȚIOASE

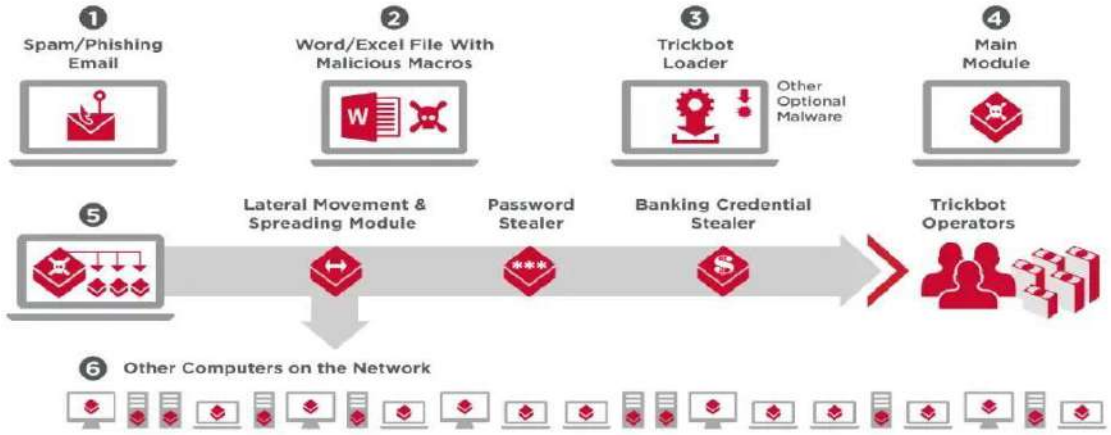
O metodă comună este trimiterea unui fișier executabil, precum un fișier cu extensia **.exe**, și păcălirea destinatarului să îl deschidă. O altă abordare este ascunderea codului periculos într-un document aparent „inofensiv", cum ar fi un fișier **Word** sau **Excel**, care poate conține **macrocomenzi**. Unele fișiere **PDF** pot include, de asemenea, scripturi. Odată deschise, aceste fișiere pot executa acțiuni periculoase pe sistemul utilizatorului, precum instalarea de programe malițioase sau permiterea accesului de la distanță.

Multe atacuri de tip ransomware din ultimii ani au început printr-un fișier atașat sau un link primit prin e-mail, care a instalat un program periculos pe sistemul utilizatorului. De regulă, acest program oferă atacatorilor acces inițial, care este apoi folosit pentru lansarea ransomware-ului.

De exemplu:

- **QakBot, IcedID și Pikabot** – programe malițioase răspândite prin e-mail, folosite pentru a obține acces inițial în sistemele utilizatorului;

- **LockBit și BlackCat (ALPHV)** – exemple de ransomware modern care este lansat după compromiterea inițială, adesea pornind de la fișiere sau linkuri primite prin e-mail.



CUM POATE FI RECUNOSCUT UN E-MAIL MALIȚIOS?

Identificarea unui e-mail malițios poate fi dificilă, deoarece atacatorii folosesc adesea metode complexe pentru a păcăli utilizatorii să acceseze linkuri periculoase sau să întreprindă acțiuni necorespunzătoare. Cu toate acestea, există indicii care pot ajuta la diferențierea unui e-mail legitim de unul malițios. Mai jos sunt prezentate câteva semne importante:

1. **Adresa expeditorului este suspectă sau necunoscută** – uneori, atacatorii folosesc nume de expeditor false sau adrese care imită domenii reale pentru a-și păcăli victimele (de exemplu, prin modificarea unor litere, adăugarea de puncte sau cratime). Atunci când primiți un mesaj de la o persoană sau organizație necunoscută, ori care pare suspectă, verificați cu atenție adresa completă a expeditorului și comparați-o cu cele ale persoanelor sau instituțiilor pe care le cunoașteți. Dacă mesajul pare să provină de la un cunoscut, dar conținutul este neobișnuit sau suspect, este recomandat să contactați expeditorul printr-un alt canal de comunicare pentru a confirma veridicitatea mesajului.

2. **Expeditorul pare să nu cunoască destinatarul** – citiți cu atenție mesajul și analizați modul de exprimare al expeditorului. Dacă mesajul pare suspect și expeditorul se adresează ca și cum nu ar cunoaște destinatarul, acest lucru poate reprezenta un indiciu de tentativă de fraudă.

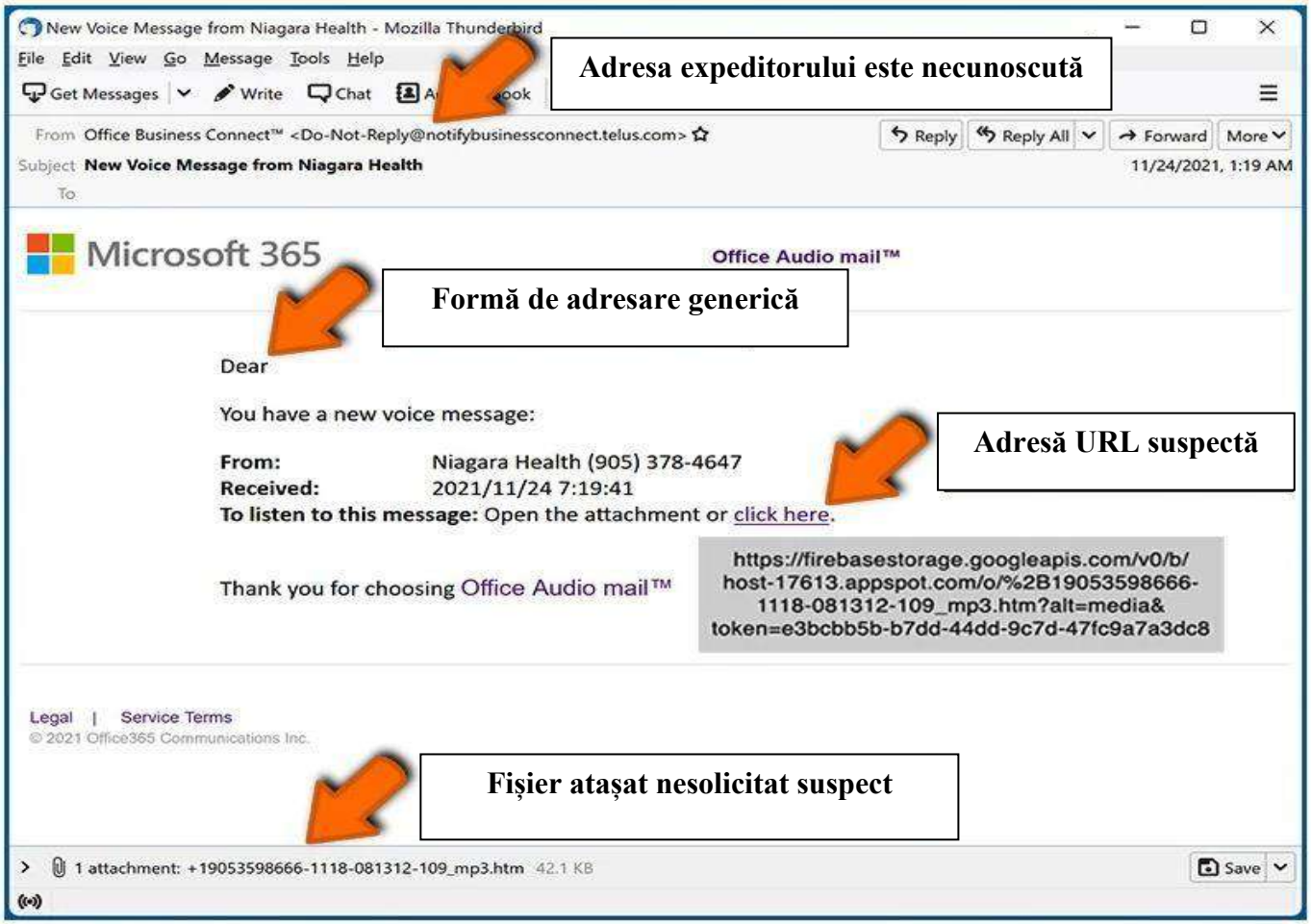
3. **Verificați istoricul discuțiilor** – dacă primiți un e-mail suspect de la o persoană sau instituție cu care ați mai comunicat, comparați mesajul actual cu mesajele anterioare pentru a identifica diferențe de stil, formulare sau conținut neobișnuit.

4. **Greșeli gramaticale sau ortografice** – e-mailurile rău intenționate conțin adesea greșeli gramaticale sau ortografice evidente. Fiți atenți la astfel de indicii, deoarece acestea pot semnala o tentativă de fraudă. Totuși, lipsa greșelilor nu garantează că mesajul este legitim, deoarece unele mesaje malițioase pot fi foarte bine redactate.

5. **Linkuri suspecte** – evitați accesarea linkurilor sau descărcarea fișierelor din e-mailuri suspecte sau din mesaje care provin de la surse necunoscute, deoarece acestea pot conține programe malițioase sau pot redirecționa către pagini de tip phishing. Pentru a verifica destinația unui link, pe calculator este suficientă trecerea cursorului peste acesta, iar adresa reală va fi afișată în partea de jos a ferestrei. Pe telefon sau tabletă, apăsați lung pe link pentru a vedea adresa înainte de a o deschide.

6. **Mesajul prezintă o urgență sau o amenințare** – atacatorii pot încerca să manipuleze utilizatorii prin crearea unui sentiment de grabă sau frică, pentru a determina o reacție rapidă și, de cele mai multe ori, necorespunzătoare. În mod similar, multe înșelătorii se bazează pe promisiunea unui câștig mare în schimbul unei investiții mici sau pe anunțarea unei presupuse moșteniri din partea unei rude necunoscute. Toate aceste tehnici au ca scop obținerea de informații sensibile sau bani din partea victimelor.

7. **Fișiere atașate suspecte** – dacă mesajul primit conține un fișier atașat nesolicitat, în special cu extensii precum .exe, .bat, .js, .zip, .rar, .doc, .xls sau .pdf, și vi se solicită să îl deschideți sau să activați funcții suplimentare (de exemplu, macrocomenzi), există un risc ridicat ca fișierul să fie malițios. De asemenea, dacă deschideți din greșeală un fișier, iar conținutul este gol sau diferit față de ceea ce vă așteptați, acest lucru poate indica o posibilă infectare. În cazul în care observați semne clare de compromitere a stației de lucru, deconectați imediat dispozitivul de la rețea și solicitați cât mai rapid suport tehnic din partea echipei responsabile.



BUNE PRACTICI DE SECURITATE

- **Configurarea unei parole complexe**

Pentru protejarea contului de e-mail și a celorlalte conturi din mediul online, este recomandată utilizarea unei parole unice și greu de ghicit pentru fiecare dintre acestea. Parola ar trebui să aibă o lungime suficientă (de preferat minimum 12-14 caractere) și să conțină o combinație de litere mari, litere mici, cifre și caractere speciale.

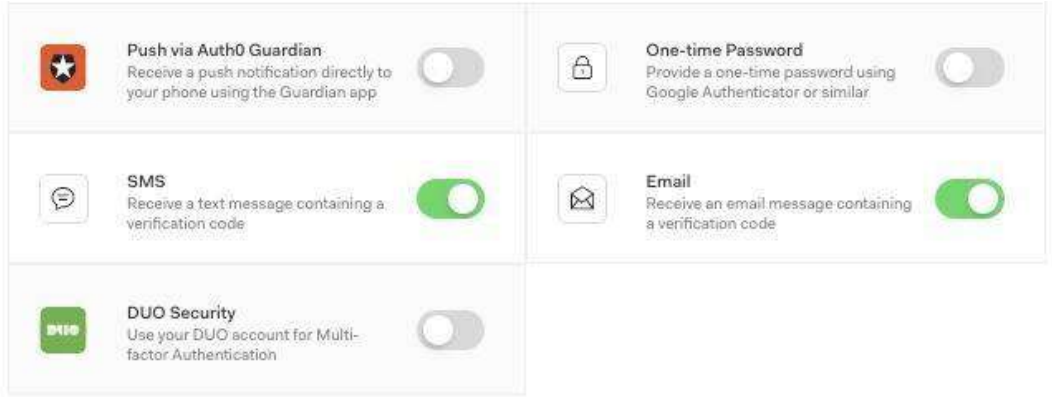
La crearea parolei, evitați folosirea informațiilor personale precum numele, anul nașterii sau date ușor de asociat cu utilizatorul. De asemenea, evitați tiparele ușor de ghicit, cum ar fi cuvinte urmate de ani sau secvențe repetate.

Atunci când este posibil, se recomandă utilizarea unui manager de parole pentru generarea și stocarea în siguranță a parolelor.

- **Autentificare multifactor (MFA)**

Chiar dacă utilizați o parolă complexă, folosirea autentificării multi-factor sporește semnificativ nivelul de protecție împotriva atacurilor de tip phishing, spear-phishing sau încercărilor repetate de parole.

Această metodă adaugă un pas suplimentar de verificare, cum ar fi un cod temporar sau o confirmare pe telefon, reducând considerabil riscul ca un atacator să poată accesa contul, chiar dacă parola a fost compromisă.



- **Acordați atenție mesajelor nesolicitate**

De fiecare dată când primiți un mesaj nesolicitat de la o persoană necunoscută, este recomandat să verificați adresa completă a expeditorului. Pe calculator, puteți face acest lucru prin trecerea cursorului peste numele afișat în câmpul „From”, iar pe telefon sau tabletă prin apăsare lungă pe numele sau adresa expeditorului.

Dacă mesajul pare să provină de la o persoană cunoscută, dar este formulat neobișnuit sau conține greșeli, se recomandă contactarea acesteia printr-un alt canal de comunicare pentru a confirma veridicitatea mesajului.

În cazul în care considerați că e-mailul primit este periculos, raportați-l conform procedurilor și ștergeți-l din inbox.

- **Acordați atenție linkurilor primite**

Multe atacuri cibernetice sunt inițiate prin accesarea unui link periculos. Atunci când primiți un link prin e-mail, înainte de a-l deschide, verificați destinația acestuia.

Pe calculator, treceți cursorul peste link, iar adresa completă către care se face redirecționarea va fi afișată în partea de jos a ferestrei. Pe telefon sau tabletă, apăsați lung pe link pentru a vedea adresa înainte de a o deschide.

- **Acordați atenție fișierelor atașate primite**

În mod similar linkurilor, fișierele atașate e-mailurilor pot reprezenta un punct inițial de atac. Se recomandă scanarea tuturor fișierelor primite, chiar dacă acestea provin de la persoane cunoscute, utilizând o soluție de protecție anti-malware.

Dacă rezultatul scanării indică faptul că un fișier are conținut potențial periculos, ștergeți imediat mesajul și nu încercați să deschideți sau să rulați fișierul.

De asemenea, fiți atenți și la linkurile care duc către fișiere găzduite pe servicii online, deoarece pot fi la fel de periculoase ca fișierele atașate direct.

- **Atenție la fișierele cu dublă extensie**

Uneori, pentru a părea legitime, atacatorii folosesc fișiere cu două extensii, astfel încât să pară documente normale, de exemplu „raport.pdf.exe” sau „document.docx.js”.

Nu este recomandată deschiderea sau rularea fișierelor primite prin e-mail care au extensii de tip **.exe, .scr, .bat, .js** sau alte fișiere executabile, chiar dacă par a fi documente obișnuite.

- **Modificarea parolelor la un interval de timp**

În mod constant au loc scurgeri de date și breșe de securitate în urma cărora pot fi colectate și distribuite ilegal credențiale de acces.

Pentru a reduce riscul accesului neautorizat, se recomandă utilizarea unei parole unice și puternice și **schimbarea imediată a parolei ori de câte ori există suspiciunea că adresa de e-mail sau un alt cont a fost compromis**.

Schimbarea periodică a parolei poate fi aplicată ca măsură suplimentară, în special în cazul conturilor care nu folosesc autentificare multifactor (MFA).

- **Evitați utilizarea adresei de e-mail de serviciu în scop personal**

Majoritatea persoanelor dețin atât o adresă de e-mail personală, cât și una de serviciu. Este recomandat ca acestea să fie utilizate exclusiv pentru scopurile lor specifice.

Folosirea adresei de e-mail de serviciu pentru activități personale sau a celei personale pentru activități de serviciu poate afecta imaginea instituției și poate crește riscul apariției unor incidente de securitate.

- **Evitați utilizarea e-mailului atunci când sunteți conectat la o rețea Wi-Fi publică**

Rețelele Wi-Fi publice sunt adesea slab securizate, ceea ce le face vulnerabile la interceptarea comunicațiilor. Datele transmise prin intermediul acestor rețele pot fi expuse persoanelor neautorizate.

În astfel de rețele, un atacator poate încerca să redirecționeze utilizatorul către pagini false sau să intercepteze informații, în special dacă conexiunea nu este protejată corespunzător.

Dacă utilizarea e-mailului este necesară, se recomandă folosirea unei conexiuni securizate sau a unui serviciu VPN.

- **Dezabonare**

În cazul mesajelor nesolicitate sau suspecte, nu este recomandată accesarea butonului de „dezabonare”, deoarece unele e-mailuri pot ascunde linkuri periculoase în spatele acestuia.

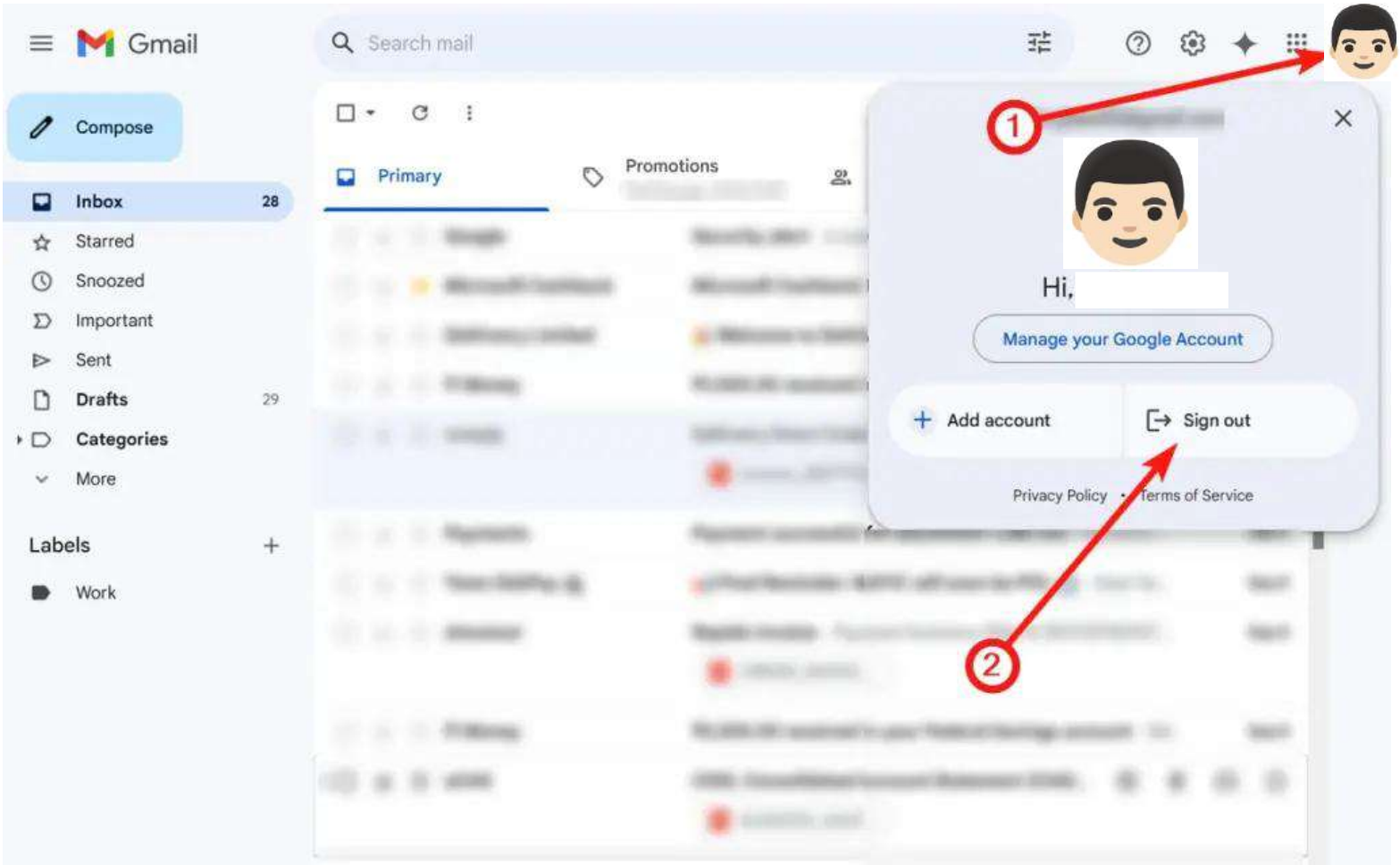
De asemenea, accesarea acestui buton poate confirma atacatorului că adresa de e-mail este validă și activă, ceea ce poate duce la creșterea volumului de mesaje nedorite.

Pentru a gestiona aceste situații, mesajele suspecte trebuie marcate ca spam și șterse din inbox. Butoanele de „dezabonare” pot fi folosite în siguranță doar în cazul mesajelor provenite din surse cunoscute și legitime.

- **Deconectare (Log out)**

Se recomandă deconectarea contului de e-mail de fiecare dată când utilizarea acestuia nu mai este necesară, chiar și atunci când dispozitivul utilizat este personal.

Această măsură reduce riscul compromiterii contului în cazul în care dispozitivul este pierdut, împrumutat sau compromis.



REFERINȚE

- https://ro.wikipedia.org/wiki/E-mail
- https://ro.wikipedia.org/wiki/SMTP
- https://en.wikipedia.org/wiki/Compatible_Time-Sharing_System
- https://en.wikipedia.org/wiki/Ray_Tomlinson
- https://datatracker.ietf.org/doc/html/rfc561
- https://en.wikipedia.org/wiki/Microsoft_Mail
- https://en.wikipedia.org/wiki/HCL_Notes
- https://www.quora.com/What-is-the-history-of-email-attachments
- https://en.wikipedia.org/wiki/AOL_Mail
- https://www.theguardian.com/technology/2016/mar/07/email-ray-tomlinson-history
- https://en.wikipedia.org/wiki/History_of_email_spam
- https://medium.com/building-mailmodo/how-does-email-work-a-dummies-guide-bd1ef894797e
- https://www.educba.com/advantages-and-disadvantages-of-email/
- https://www.egr.msu.edu/decs/security/how-recognize-malware-email
- https://www.titanfile.com/blog/10-best-practices-for-email-security-2/
- https://www.cloudflare.com/learning/email-security/what-is-email-security/
- https://certmil.ro/wp-content/uploads/2022/02/20220117_N_Ghid-de-securitate-email.pdf
- https://blog.comodo.com/email-security/what-is-email-spam/
- https://mailmeteor.com/blog/how-to-write-email-with-attachment
- https://www.pcrisk.com/removal-guides/23868-the-list-of-the-problem-email-virus
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/trickbot-botnet-ransomware-disruption
- https://wallpapers.com/email

AGENȚIA DE APĂRARE CIBERNETICĂ