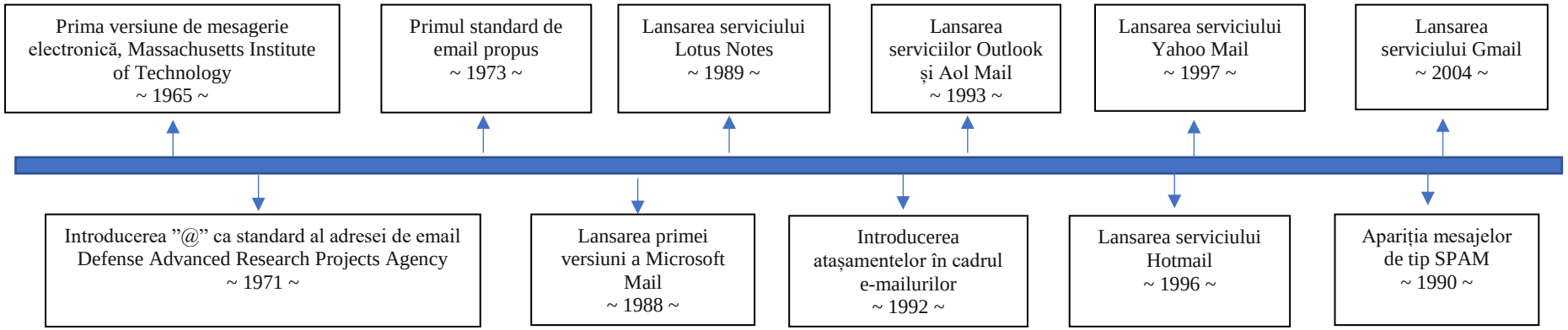

AGENȚIA DE APĂRARE CIBERNETICĂ

Ghid de bune practici pentru utilizarea serviciului de Email

Introducere

Email-ul este un serviciu de comunicare ce permite transmiterea mesajelor în format electronic către unul sau mai mulți destinatari prin intermediul unei rețele de calculatoare. Acesta a fost dezvoltat cu mult timp înainte de apariția Internetului propriu-zis, fiind implementat pentru prima oară în cadrul rețelei ARPANET[1] în anul 1971 de către Ray Tomlinson[2]. În prezent, email-ul este metoda principală utilizată pentru comunicarea la distanță, fiind trimise peste 100 de miliarde de mail-uri zilnic.

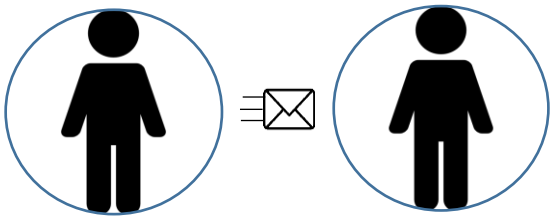


Evoluția serviciului de email

[1] ARPANET - Advanced Research Projects Agency Network

[2] Ray Tomlinson - programator, a implementat primul serviciu de email din lume, fiind și cel care a folosit semnul @ pentru a desemna utilizatorul care urma să primească mesajul

Modul de funcționare al serviciului de email



Pentru a putea primi, trimite sau citi email-uri este necesară utilizarea unui client de email. Unele sisteme de operare, ex. Microsoft, au în mod implicit configurat un astfel de serviciu, ex. Outlook Express. Există și servicii de email gratuite disponibile prin intermediul unui browser obișnuit precum Gmail, Yahoo mail sau Hotmail. În principiu, indiferent de tip, un client de mail ar trebui să îndeplinească următoarele funcții:

- primește mesajele, afișând header[3]-ul acestora;
- permite selectarea unui email și afișează conținutul propriu-zis;
- permite crearea unui mesaj nou și trimiterea către unul sau mai mulți destinatari;

Cum poate fi recunoscut un email malițios ?

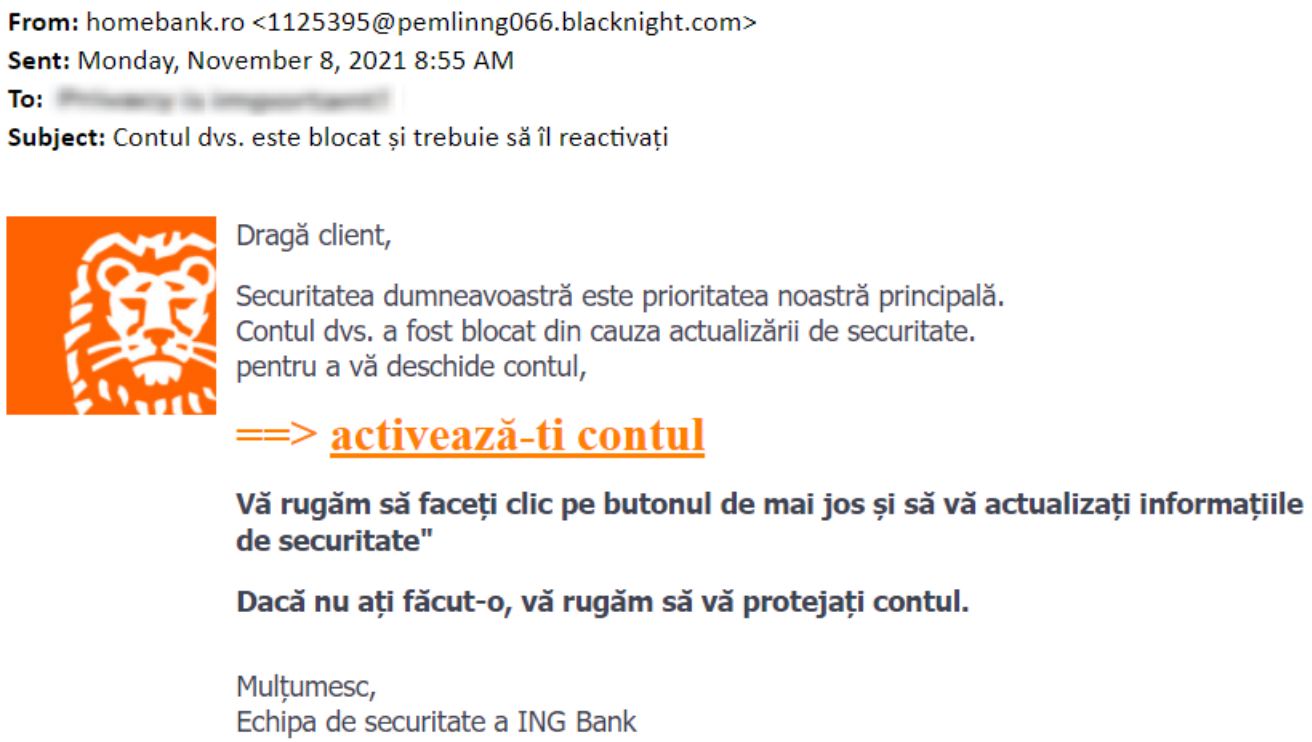
Email-ul reprezintă un standard atunci când vorbim de discuții oficiale între două sau mai multe organizații. Acest lucru a atras atenția atacatorilor, care au conceput diferite metode de atac pentru a exfiltra date sensibile și obține beneficii bănești de pe urma acestora. La primirea unui email nesolicitat, este recomandat ca, înainte de deschiderea mesajului, acesta să fie analizat.

În continuare sunt prezentate câteva sfaturi generale care pot ajuta la identificarea email-urilor rău intenționate.

[3] Header – în cadrul header-ului unui email sunt introduse informații despre dimensiunea mesajului, expeditor, data și ora trimiterii, etc.

- ***Adresa expeditorului nu este corectă***

În cazul în care este primit un email nesolicitat de la o adresă de email necunoscută, înainte de deschiderea mesajului, este recomandată verificarea validității adresei. Dacă este posibil, expeditorul ar trebui contactat prin intermediul unei alte căi de comunicare pentru a verifica dacă acel mesaj este legitim.



From: homebank.ro <1125395@pemlinng066.blacknight.com>
Sent: Monday, November 8, 2021 8:55 AM
To: [redacted]
Subject: Contul dvs. este blocat și trebuie să îl reactivați

Dragă client,

Securitatea dumneavoastră este prioritatea noastră principală.
Contul dvs. a fost blocat din cauza actualizării de securitate.
pentru a vă deschide contul,

==> activează-ti contul

Vă rugăm să faceți clic pe butonul de mai jos și să vă actualizați informațiile de securitate"

Dacă nu ați făcut-o, vă rugăm să vă protejați contul.

Mulțumesc,
Echipa de securitate a ING Bank

- ***Expeditorul pare să nu cunoască destinatarul***

Pentru identificarea unor posibile nereguli se recomandă analizarea cu atenție a subiectului și mesajului. Dacă mesajul pare suspect, iar expeditorul se adresează de parcă nu ar cunoaște destinatarul, se recomandă ignorarea mesajului.

- **Link-urile încorporate au adrese URL ciudate**

Fiecare link primit ar trebui analizat înainte de a fi accesat. Pentru a verifica dacă link-ul va redirecționa către pagina dorită, este suficientă trecerea cursorului pe deasupra acestuia, iar în colțul stânga jos al ferestrei de email va fi afișată adresa reală către care acesta va redirecționa.

- **Limba, ortografia și gramatica sunt greșite**

Dacă mesajul primit prezintă greșeli de exprimare și ortografie, este posibil ca acesta să nu fie un mesaj legitim și să fie transmis de o persoană rău intenționată care a folosit un program de traducere online.

- **Mesajul primit este de necrezut**

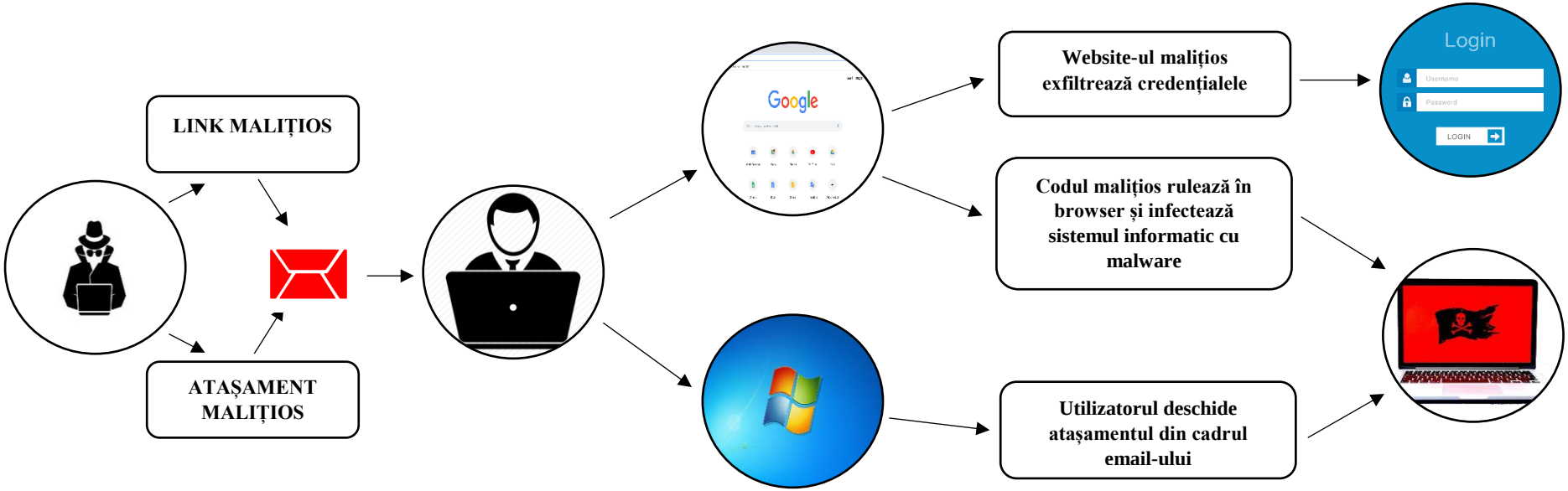
Dacă un lucru pare prea bun ca să fie adevărat, atunci probabil că nici nu este. Multe înșelătorii se bazează pe promisiunea unui câștig mare în schimbul unei investiții mici sau pe primirea unei moșteniri din partea unei rude necunoscute. De cele mai multe ori, aceste mesaje sunt încercări ale atacatorilor de a obține informații sensibile sau bani din partea victimelor.

Cum putem deveni victima unui atac lansat prin intermediul email-ului ?

Sunt multe metode prin care putem deveni victime ale atacurilor lansate prin intermediul email-ului. Fie că vorbim de campanii de phishing sau de infectarea dispozitivului cu malware, toate aceste acțiuni au ca scop exfiltrarea de date pentru a provoca de cele mai multe ori daune financiare.

- **Accesarea unui link sau atașament malițios**

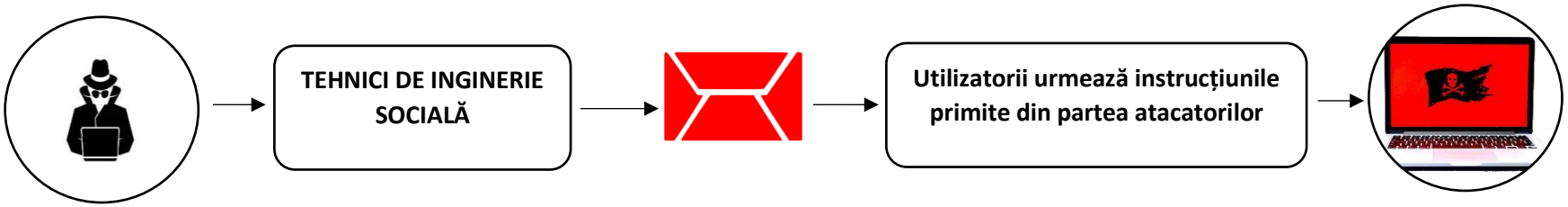
Accesarea atașamentelor sau link-urilor primite prin email fără a le verifica în prealabil, poate rezulta în exfiltrarea datelor sensibile, precum credențialele conturilor, sau infectarea dispozitivelor cu malware.



- **Tehnici de inginerie socială**

Atacatorii caută în permanență potențiale victime prin utilizarea tehnicilor de inginerie socială. Acestea au ca scop exploatarea slăbiciunilor umane, precum lăcomia sau frica. Spre exemplu, aceștia transmit email-uri prin care pretind că sunt un vechi prieten sau o rudă îndepărtată și au nevoie de un mic ajutor financiar pentru rezolvarea unei probleme extrem de urgente, sau că sunt o anumită persoană cu care ați interacționat în trecut și este interesată de crearea unei relații cu dumneavoastră.

De asemenea, atacatorii pot trimite mesaje de tip phishing sau spear phishing prin care vă notifică o problemă extrem de gravă ce solicită remediere urgentă, iar pentru a remedia problema vi se solicită accesarea link-ului primit de la aceștia. Un astfel de link redirecționează de obicei către copia perfectă a unui website legitim, acolo unde, pentru a continua, vi se vor solicita credențialele de acces.

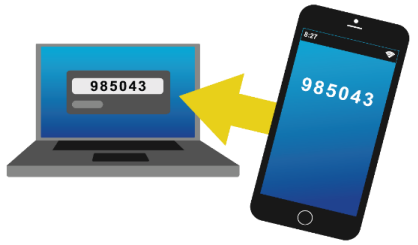


Bune practici de securitate în cadrul serviciului de email

- **Configurarea unei parole complexe**

Pentru o bună securitate a contului de email, dar și a celorlalte conturi din mediul online, este recomandată configurarea unei parole unice și complexe. Este indicat ca aceasta să fie compusă din litere mari, litere mici și caractere alfanumerice precum și caractere speciale. De asemenea, nu este recomandată utilizarea informațiilor personale în conținutul parolelor.

- **Utilizarea autentificării multi-factor**

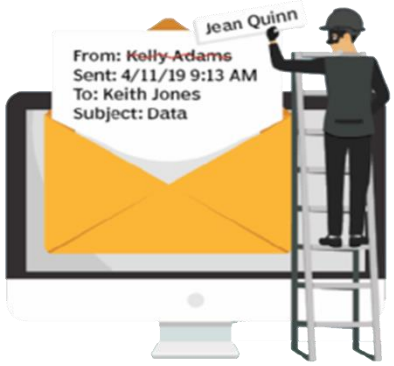


Această metodă de autentificare reprezintă o metodă de protecție suplimentară. Totodată, utilizarea autentificării multi-factor sporește substanțial protecția împotriva atacurilor de phishing și spear-phishing, deoarece este oferită siguranța că informațiile de conectare sunt utilizate pentru autentificarea pe website-ul dorit și nu pe o pagină falsă.

- **Atenție la email-urile de tip spam**

Atunci când este primit un mesaj nesolicitat de tip spam, este recomandată raportarea și ștergerea acestuia.

- **Atenție la email-urile de tip spoof**



În cazul primirii unui email nesolicitat, pentru verificarea veridicității emailului, este recomandată trecerea cursorului peste numele afișat în câmpul ”from”. Dacă adresa este validă, pe lângă numele expeditorului va fi afișată și adresa de email a acestuia. Mesajele de tip *spoof* sunt parte a unui atac prin care atacatorii trimit către victime mesaje ce par a veni din partea unor persoane de încredere.

- **Atenție la email-urile de tip phishing**

Email-urile de tip phishing reprezintă unul dintre principalele moduri prin care atacatorii reușesc să fure informații sensibile. Scopul acestor mesaje este de a atrage atenția victimelor și de a le convinge să se ”conecteze” pe site-urile false ale atacatorilor. Cele mai frecvente mesaje vin de obicei din partea instituțiilor bancare sau din partea furnizorilor de servicii. Înainte de accesarea link-urilor din cadrul mesajului, este recomandată contactarea instituției respective pentru confirmarea legalității și expedierii acelui mesaj.

- **Atenție la link-urile din mesaje**

De multe ori atacurile cibernetice sunt inițiate prin accesarea unui atașament sau link malițios. Înainte de accesarea unui link primit prin intermediul serviciului de mail, este recomandată trecerea cursorului peste link, astfel încât, în partea stânga-jos a ferestrei va fi afișată adresa URL către care se va face redirecționarea în momentul accesării.

- **Evitarea utilizării emailului de serviciu în scop personal**

Adresele de email organizaționale trebuie utilizate doar în interes de serviciu. Publicarea acestor adrese pe platformele de social media sau utilizarea pentru cumpărături online pot avea ca rezultat primirea de email-uri nesolicitate, unele dintre ele posibil malițioase.

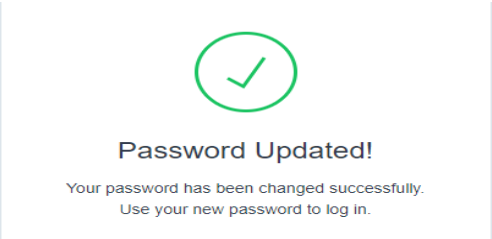
- **Scanarea atașamentelor primite**

Înainte de a fi deschise, este recomandată examinarea cu atenție și scanarea anti-malware a tuturor atașamentelor primite, chiar dacă acestea provin din partea unui cunoscut. În prezent există mai multe instrumente de analiză care permit scanarea atașamentelor. Dacă rezultatul analizei indică faptul că un atașament are conținut malițios este recomandată ștergerea cât mai rapidă a acelui mesaj.

Atenție la atașamentele cu dublă extensie, ex. *”list.txt.exe”.* Nu este recomandată rularea fișierelor primite pe email care au extensii de tipul .exe, .scr, .bat, .com sau alte fișiere executabile.

- **Modificarea parolei**

În fiecare an au loc scurgeri de informații și breșe de securitate din care atacatorii își construiesc baze de date cu parolele furate. Pentru a evita riscul accesării neautorizate a contului de email printr-un atac de tip ”bruteforce”, una dintre cele mai simple și utile practici de securitate constă în modificarea cât mai frecventă a parolei.



- **Date cu caracter personal**

La primirea unui email care solicită date personale, este recomandat ca acesta să fie ignorat și șters cât mai rapid. Orice entitate cu care utilizatorul relaționează prin intermediul aplicațiilor web ar trebui să cunoască deja aceste informații.

- **Protocoale**

De fiecare dată când se dorește accesarea serviciului de email, aceasta ar trebui să fie realizată doar prin intermediul protocoalelor securizate precum IMAPS, POP3S și HTTPS. Utilizarea acestor protocoale previne interceptarea email-urilor.

- **Criptarea mesajelor**

Pentru o bună securitate este recomandată utilizarea unei metode de criptare. Acest lucru poate fi realizat prin instalarea unui certificat digital precum PGP.

- **Dezabonare**

Deși pare ilogic, nu este recomandată accesarea butonului de dezabonare din cadrul mesajelor nesolicitate deoarece mulți atacatori ascund link-urile malițioase în spatele acestora. Pentru a aborda această problemă, email-urile nesolicitate trebuie marcate ca spam și șterse cât mai rapid posibil.

Ce se întâmplă atunci când este accesat butonul de dezabonare ?

Accesarea acestui buton va confirma atacatorului că adresa de email este valabilă și activă iar de cele mai multe ori, volumul de email-uri nesolicitate va crește. Este posibil ca uneori, pentru a finaliza procesul de dezabonare, să se deschidă automat o pagină web, din cadrul căreia să fie instalat automat malware sau să fie solicitate și mai multe informații personale.

- **Log out**

Este recomandată deconectarea contului de fiecare dată când utilizarea acestuia nu mai este necesară, chiar dacă dispozitivul utilizat este unul personal. Acest lucru reduce riscul compromiterii contului de email în cazul în care dispozitivul este compromis.

Termeni specifici

- **Malware -** software malițios, creat pentru a provoca pagube în cadrul unui computer, server sau rețea;
- **Virus -** tip de cod malițios, care atunci când este executat, se răspândește și infectează sistemul informatic;
- **Rootkit -** software malițios ce are rolul de a obține acces neautorizat pe sisteme informatice simultan cu mascarea prezenței pe dispozitivul infectat;

- **Spam** - de obicei, un email de tip spam nu reprezintă un pericol real, însă poate distrage atenția și afecta productivitatea;
- **Scam -** tip de înșelăciune, bazat pe trimiterea unor oferte *”tentante, greu de refuzat”.*
- **Phishing -** reprezintă o infracțiune cibernetică în care o țintă sau mai multe ținte sunt contactate prin e-mail, telefon sau mesaj text de către o persoană care se prezintă ca fiind reprezentantul unei instituții legitime pentru a convinge victimele să furnizeze date sensibile, cum ar fi informații personale, detalii bancare sau credențiale de acces la diferite sisteme sau servicii;
- **Spear-phishing -** catalogată drept cea mai mare amenințare din mediul online din prezent, aceasta este similară ca principiu atacului de phishing, diferența constând în faptul că spear-phishing-ul este conceput special pentru a viza o anumită țintă, spre exemplu doar personalul unei anumite organizații;
- **Ransomware** - tip de atac ce criptează complet fișierele victimei, solicitând o răscumpărare în schimbul cheii de decriptare;

Referințe

https://certmil.ro/wp-content/uploads/2021/03/Ghid-utilizare-mail-v.1.0.pdf

https://www.titanfile.com/blog/10-best-practices-for-email-security-in-2021/

https://www.insightcdct.com/getattachment/f72847b9-cd86-4cf7-b10b-469c610affe3/Mastering-Email-Security.aspx

Agenția de Apărare Cibernetică