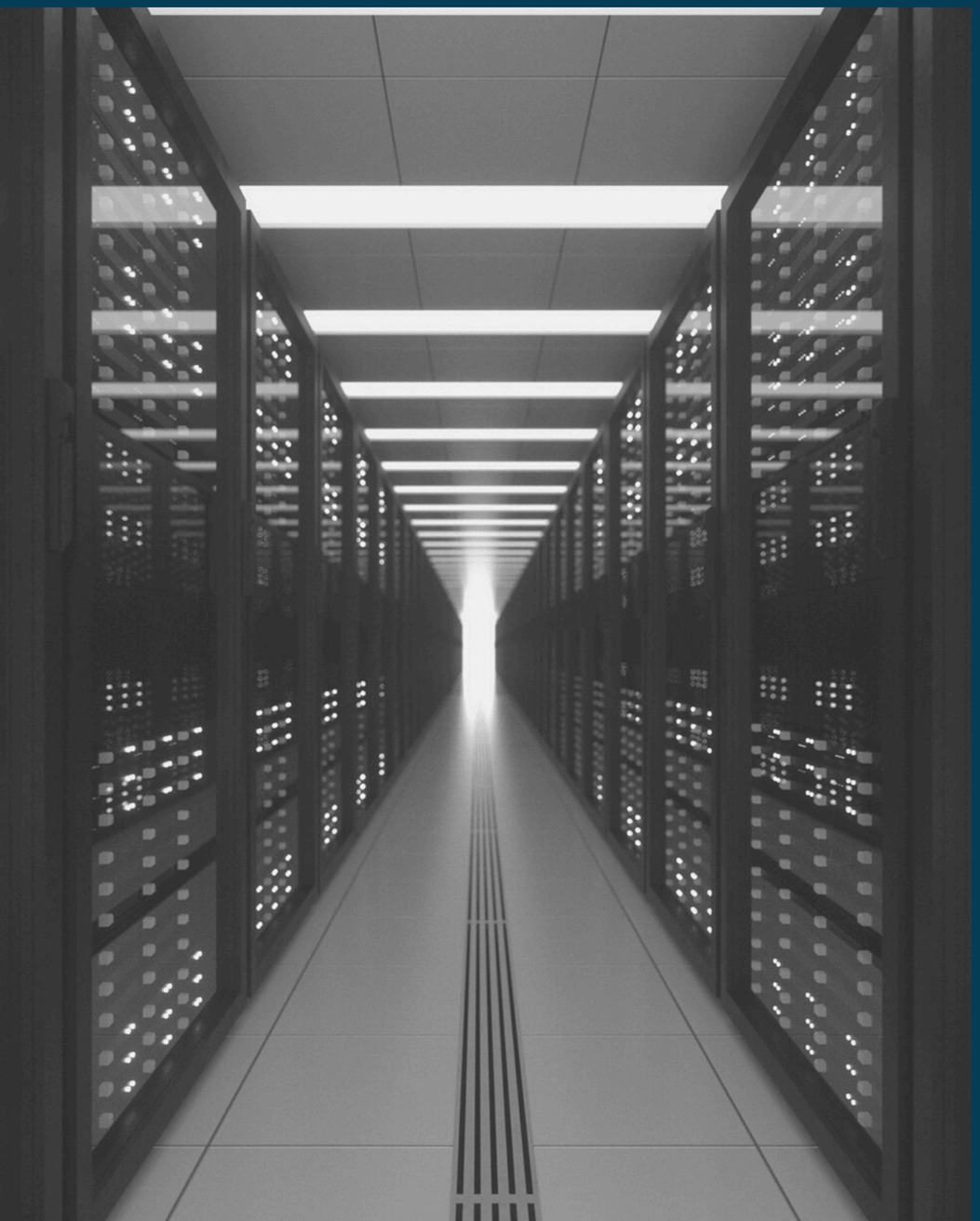
CERINȚE MINIME DE SECURITATE CIBERNETICĂ CONFORM HG.NR. 201/2017

Persoana(subdiviziunea) responsabilă de Sistem de management, conform legislației are următoarele atribuții:

1) organizează sistemul de management al securității cibernetice în instituție conform sistemului de management al securității cibernetice;

2) participă, cel puțin o dată pe an, la cursurile de formare organizate de Ministerul Tehnologiei Informației și Comunicațiilor privind securitatea cibernetică și, respectiv, organizează cursuri pentru angajații instituției;

3) asigură elaborarea, implementarea și respectarea prevederilor următoarelor documente: planul de acțiuni pentru asigurarea securității cibernetice al instituției, politica de securitate cibernetică a instituției, planul de instruire și responsabilizare în securitatea cibernetică a personalului, regulamentele interne de securitate cibernetică, procedurile de recuperare.



Sistemul de management al securității cibernetice asigură:

1) disponibilitatea informației (accesul la informație pentru o anumită perioadă de timp specificată, conform specificațiilor tehnice);

2) integritatea informației (păstrarea informației cu toate atributele sale inițiale și modificarea ei doar de către persoanele autorizate);

3) confidențialitatea informației (acces la informație doar al persoanelor autorizate și doar la datele prestabilite pentru acces);

4) protecția echipamentelor și produselor program (calculatoare, software, sisteme de stocare a datelor, echipamente de rețea și alte echipamente tehnice);

5) identificarea și remedierea vulnerabilităților;

6) efectuarea copiilor de rezervă și stabilirea procedurilor de recuperare.

Politica de securitate cibernetica include

Scopul și obiectivele Declarația managementului instituției de susținere a scopului și principiilor securității cibernetice în instituție.

Principiile de organizare internă a managementului de securitate cibernetică;

Analiza situației și vulnerabilităților (disponibilitate, integritate și confidențialitate a datelor, precum și analiza riscurilor și căilor de remediere);

Atât pentru nivelul 1 (utilizarea TIC în activitatea instituției) cât și nivelul 2 (utilizarea TIC în activitatea instituției și prestarea serviciilor bazate pe TIC) cadrul legal stabilește:

- Descrierea măsurilor de control al accesului;
- Definirea și descrierea măsurilor de securitate fizică;
- Stabilirea securității operaționale;
- Descrierea schimbului securizat de date și de comunicări;
- Cerințele la inițierea achizițiilor de SIA noi sau actualizarea celor existente, ca cerințe nonfuncționale obligatorii;
- Definește condițiile contractuale minime obligatorii la externalizarea/ mentenanța sistemelor;
- Definește prevederile generale aferent răspunsului la incidente, continuitatea proceselor și recuperare

Ciclu de viață SMSC

- Menținerea rezistenței și recuperarea capacităților după incident cibernetică

- Identificați activele primare
- Managementul riscurilor
- Dezvoltați politici formale cibernetice

- Threat intelligence
- Stabilire plan de remediere a situațiilor de urgență

- Protejați activele în funcție de risc
- Consolidați cultura securității cibernetice
- Construiți un sistem stratificat

- Monitorizare cibernetică
- Crearea canale securizate pentru partajarea informației, pentru a prezice potențiale amenințări

Riscuri și amenințări cibernetice conform resurselor informaționale utilizate

Riscuri asociate stațiilor de lucru

Programele malițioase - (malware) reprezintă o aplicație sau script conceput cu scopul de a provoca modificarea sau ștergerea datelor informatice, deteriorarea sau restricționarea accesului la dispozitive de calcul sau rețele.

Viruși - se replică modificând alte programe de calculator prin introducerea propriului cod.

Troieni - dau impresia că efectuează operațiuni legitime, când încearcă de fapt să exploreze vulnerabilitățile sistemului și să permită infractorilor cibernetici să acceseze sistemul în mod ilegal.

Viermi - aplicații cu efecte distructive care infectează sistemul informatic și se propagă prin internet.

Ransomware - criptează sau blochează accesul la fișiere și solicită o răscumpărare pentru a elimina restricțiile.

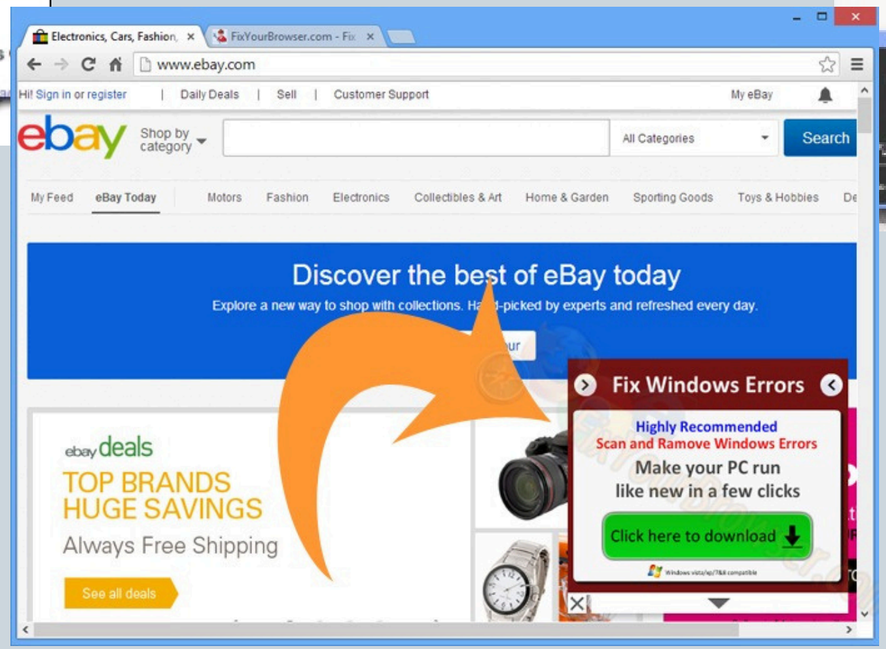
Adware- programe care transmit în mod agresiv reclame utilizatorilor pe Internet.

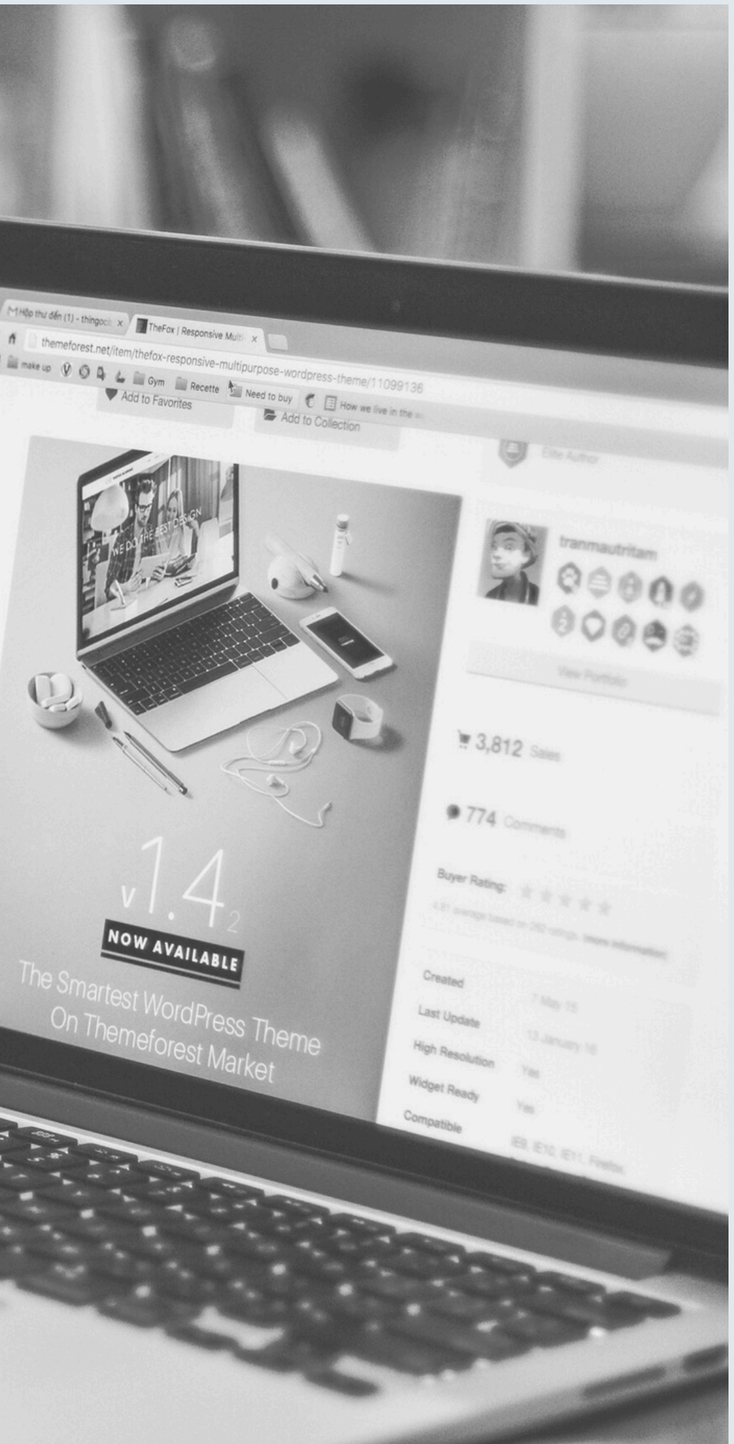
Criptomineri - aplicații care utilizează resursele informatice pentru a mina criptomonedele pentru infractorii cibernetici.

Portaluri web ce au conținut malițios

Semne de identificare

- **Link-uri suspicioase**
- **Solicitare urgentă de instalare suplimentară de plug-in sau alte programe**
- **Mesaje tip pop-up urgente ce nu permit utilizarea site-ului pînă nu sunt accesate**
- **Mesaje de cîștiguri sau promoții neașteptate ce solicită click sau oferirea de date personale**





Portaluri web ce au conținut malițios

Măsuri de prevenție

Actualizați aplicațiile - Mențineți actualizate sistemele de operare, browserele internet, plugin-uri, add-on-uri și aplicați patch-uri.

Activați funcții avansate Endpoint - Utilizați sistemul de prevenire a intruziunii și a prevenirii heuristice a fișierelor pentru monitorizare comportamentului fișierelor din sistem.

Acționați proactiv - Controlați periodic versiunea scripturilor de conținut, precum și scanarea fișierelor și a scripturilor găzduite local.

Lista albă a aplicațiilor- Izolați aplicațiile și creați un sandbox pentru a reduce riscul de atacuri de tipul drive-by.

Restricționați conținutul pe web - Utilizați instrumente precum ad-blockers pentru a limita posibilitatea de a executa coduri rău intenționate în timp ce vizitați anumite site-uri web.

Monitorizați și filtrați - Utilizați instrumente de monitorizare și filtrare a conținutului web și al e-mailurilor pentru detectarea și prevenirea livrării de adrese URL și fișiere dăunătoare.

Ransomware

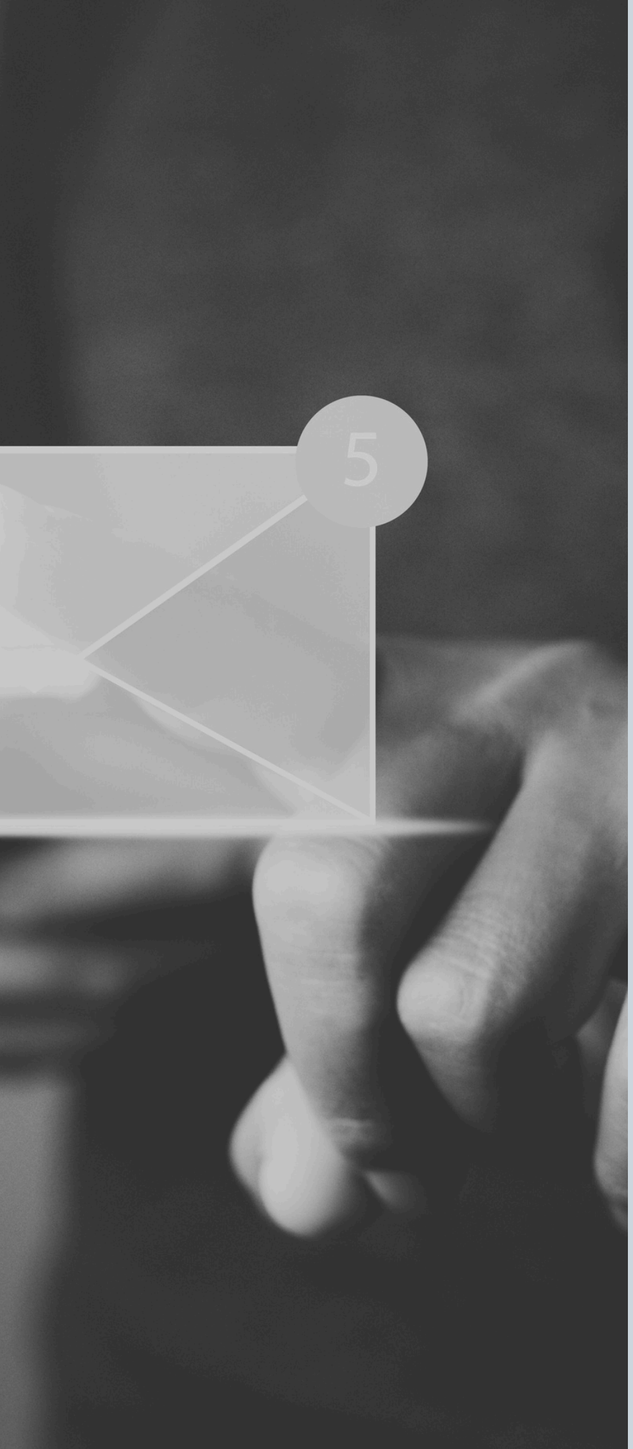
Ransomware este un software rău intenționat care, după ce seinstalează pedispozitivul victimei (calculator, smartphone), criptează datele victimei ținându-le „ostatice” sau șantajează victima, pe care o amenință că îi va publica datele dacă aceasta nu plătește o „răscumpărare” (în engleză ransom). În cele mai multe cazuri, când victima a plătit suma solicitată, victima nu a scăpat de ransomware.

Caracteristici cryptolocker

- Criminalii cibernetici dețin date Dvs până la plata unei „recompense”;
- Datele calculatorului infectat sunt criptate folosind criptarea puternică;
- Plata solicitată pentru decriptarea;
- Decriptarea nu este posibilă fără cheia private. Calculatorul este rar deblocat după plată.

Măsuri de prevenție

- Faceți copii de rezervă periodice a tuturor datelor importante
- Nu deschideți atașamente primite din resurse necunoscute sau neverificate.
- Asigurați-vă că Sistemul de operare al calculatorului Dvs. și baza de date a antivirusului este actualizată;
- Dacă există posibilitate, deschideți fișierele suspecte într-un mediu virtual (de exemplu VMware Player);
- Dacă vă aflați în situația în care vi s-au criptate fișierele și vi se cere să plătiți răscumpărarea, nu faceți asta!



Riscuri asociate utilizării de poștă electronică

E-mailul este un instrument indispensabil de comunicare, utilizat zilnic în procesul de lucru. Din păcate, multe atacuri își au originea în e- mailuri fiind variate ca formă, conținut și scop: de la mesaje de publicitate până la scheme frauduloase complexe.

Securitatea cibernetică folosește mai multe nivele de apărare (protecție) a informațiilor. Dacă un nivel este învins, următorul ar trebui să-l oprească. Un utilizator vigilent, instruit și conștient este un nivel critic de apărare împotriva amenințărilor, atât interne, cât și externe.

Pentru a evalua corect un e-mail legitim de unul fraudulos, trebuie pentru început să cunoaștem și să distingem tipurile principale de atac prin e-mail.

Spam și spam-phishing

Spam- deseoriscopul acestormesaje nu este întotdeauna clar și variază începînd cu promovare de servicii/produse, și mai nou distribuirea unor fișiere sau link-uri malițioase în rețea aleator la un număr cât mai mare de conturi.

O metoda de spam este phishing-ul prin care se încearcă obținerea, de la clienții unei organizații – indiferent de aria sa de activitate – a credențialelor de acces, parolelor, informațiilor personale și/sau importante, având scop prioritar sustragerea de bani.

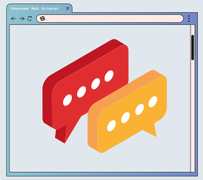
E-mailurile sau site-urile de tip **phishing** pot să îți ceară:

- nume de utilizator și parole, inclusiv modificări de parolă;
- codul numeric personal;
- numărul contului bancar;
- codurile PIN (numere de identificare personală);
- numărul cardului de credit;
- numele dinainte de căsătorie al mamei dvs.;
- data nașterii.

Semnele unui mesaj phishing

Arată identic cu e-mail-urile pe care le primiți de la intituții autorizate

Solicită să descarci un atașament sau să deschizi un link



Imită logo-ul și designul mesajelor reale

Utilizează un limbaj care sugerează urgență

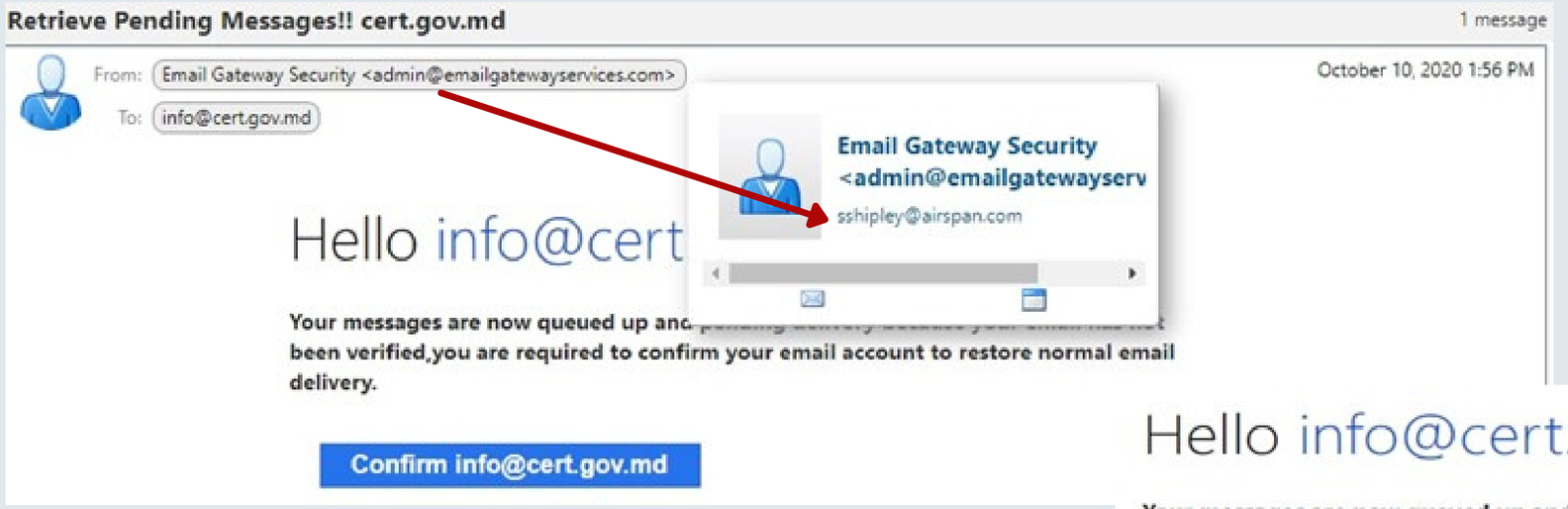
Tehnici și metode de evaluare și identificare e-mailuri frauduloase

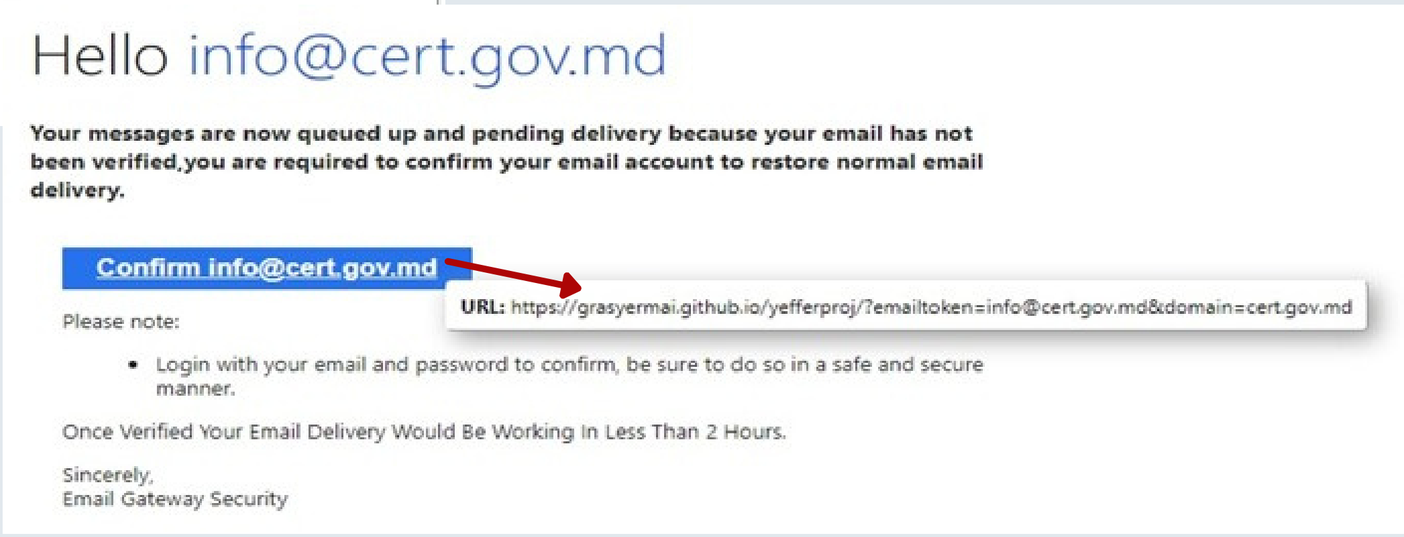
Cea mai buna metodă de tratare a e-mailurilor frauduloase este cea pro-activă. Vă sugerăm o serie de exemple a elementelor trigger, ce ar trebui să vă atragă atenția și crea suspiciuni: 1.Antetul e-mail-ului; 2.Adresarea generică; 3.Solicitarea deschisă a datelor sensibile, confidențiale sau a unor acțiuni precum accesare link-uri și chestionare; 4.Caracterul general al mesajului.

În cele ce urmează vom analiza un e-mail sub toate cele aspecte menționate anterior, utilizând tehnici și tehnologii de identificare a potențialului risc cibernetic.

Analiza unui e-mail (Studiu de caz)

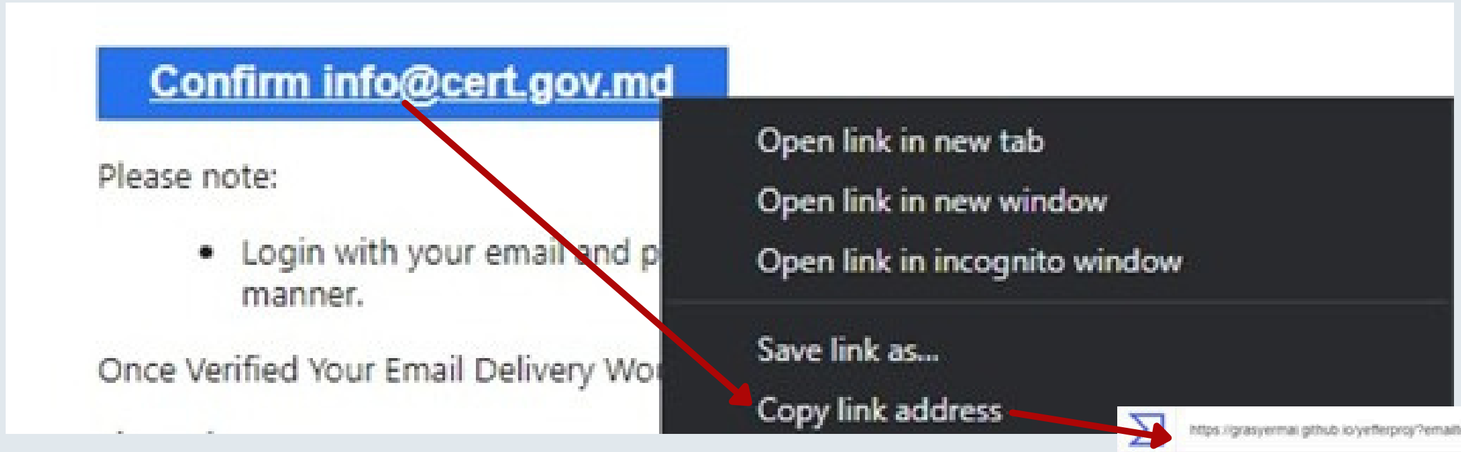
La recepționarea unui e-mail atragem atenția în primul rând la antet. Detalii precum adresa și numele emitentului.
La prima vedere pot părea autentice. Foarte ușor poți testa dacă adresa declarată a emitentului coincide cu cea de facto.
E nevoie doar să îndrepți cursorul mouse-ului fără a face click, în rîndul emitentului scrisorii sau respectiv în rîndul link-ului ce solicită accesare.

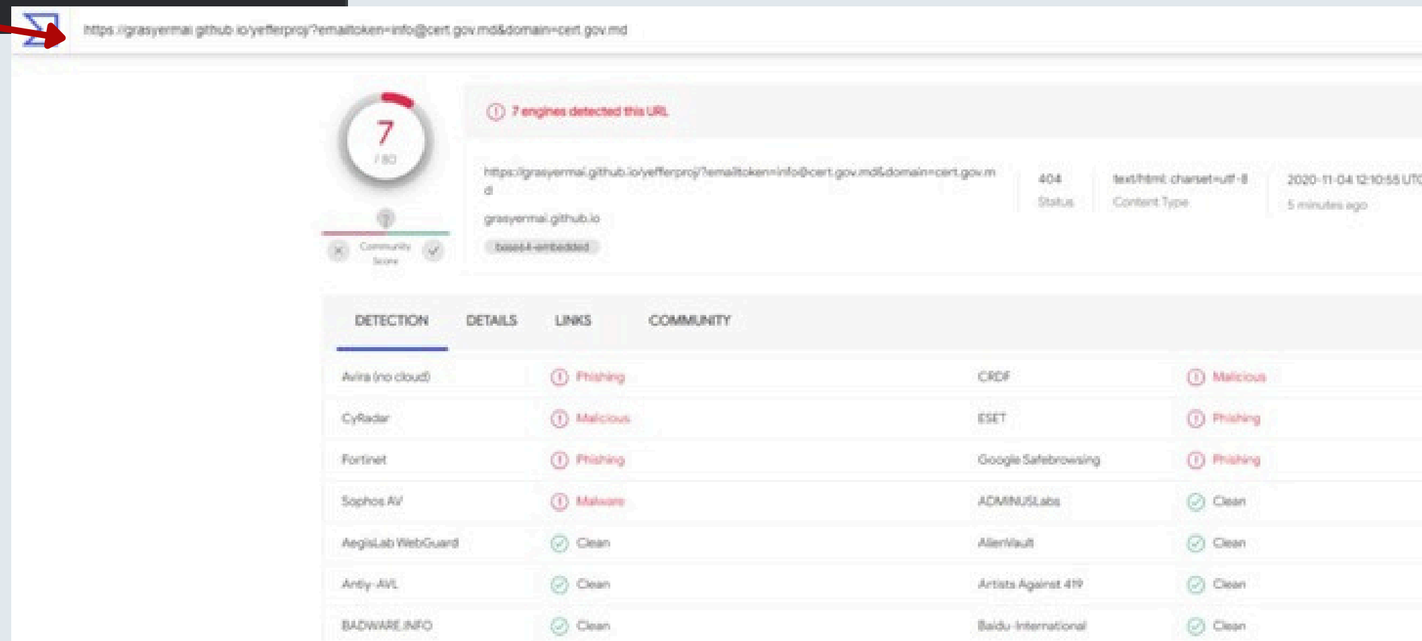




Verificarea adreselor emitente prin platforme specializate de scanare

Încazulîncareadreseletrezescsuspiciuni,este recomandată verificarea lorprincopierelinkșiscanareaprin VIRUSTOTAL, Hybrid Analysis, Cuckoo Sandbox (nu accesăm link, ci copiem adresa).

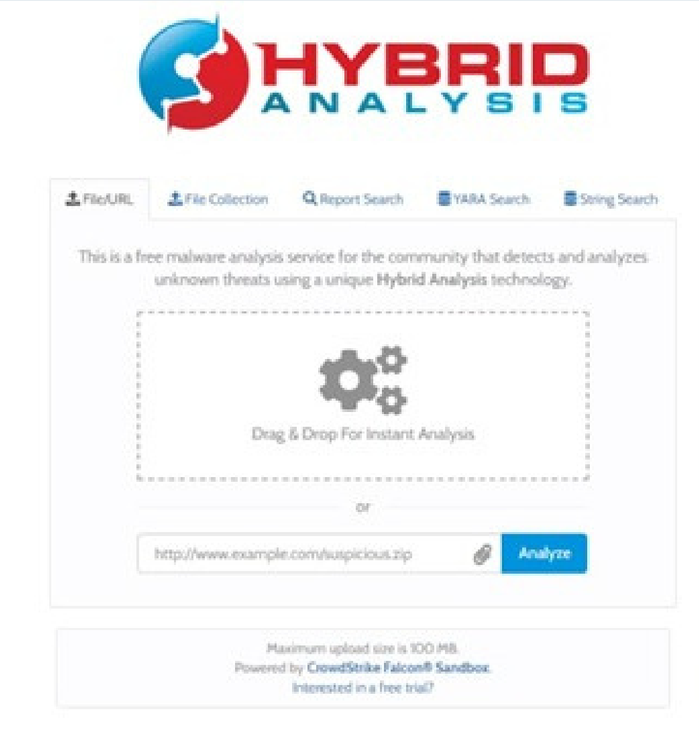




Verificarea atașamentelor și link-urilor

Chiar dacă un mesaj e-mail pare a fi autentic, sau după natură inofensiv, evitați descărcarea sau deschiderea automată a atașamentelor din acestea, precum și accesarea link-urilor de redirecționare, fără a le verifica mai întâi.
Soluții online simple și accesibile pentru a verifica un atașament, URL sau IP sunt:

https://www.hybrid-analysis.com/

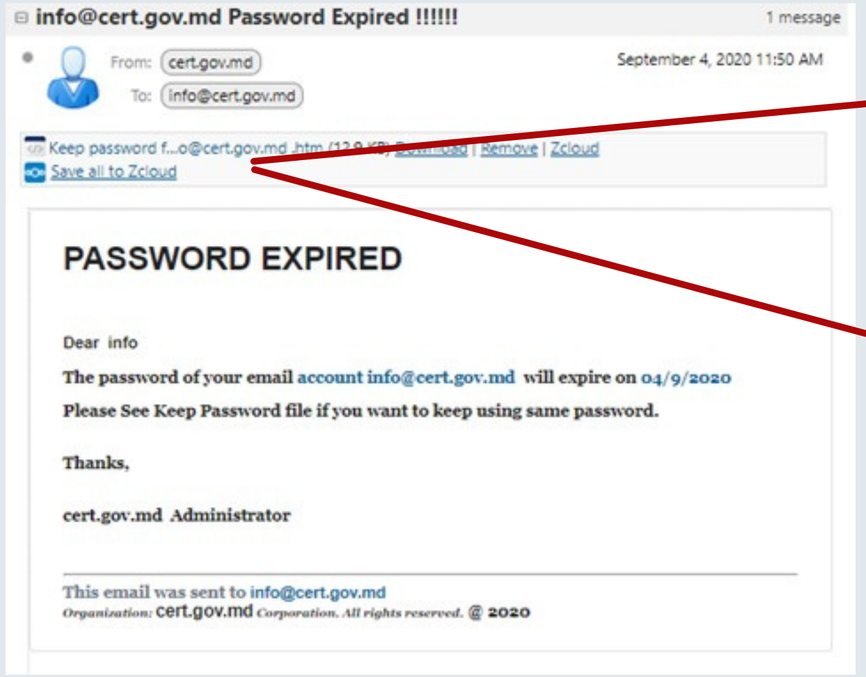


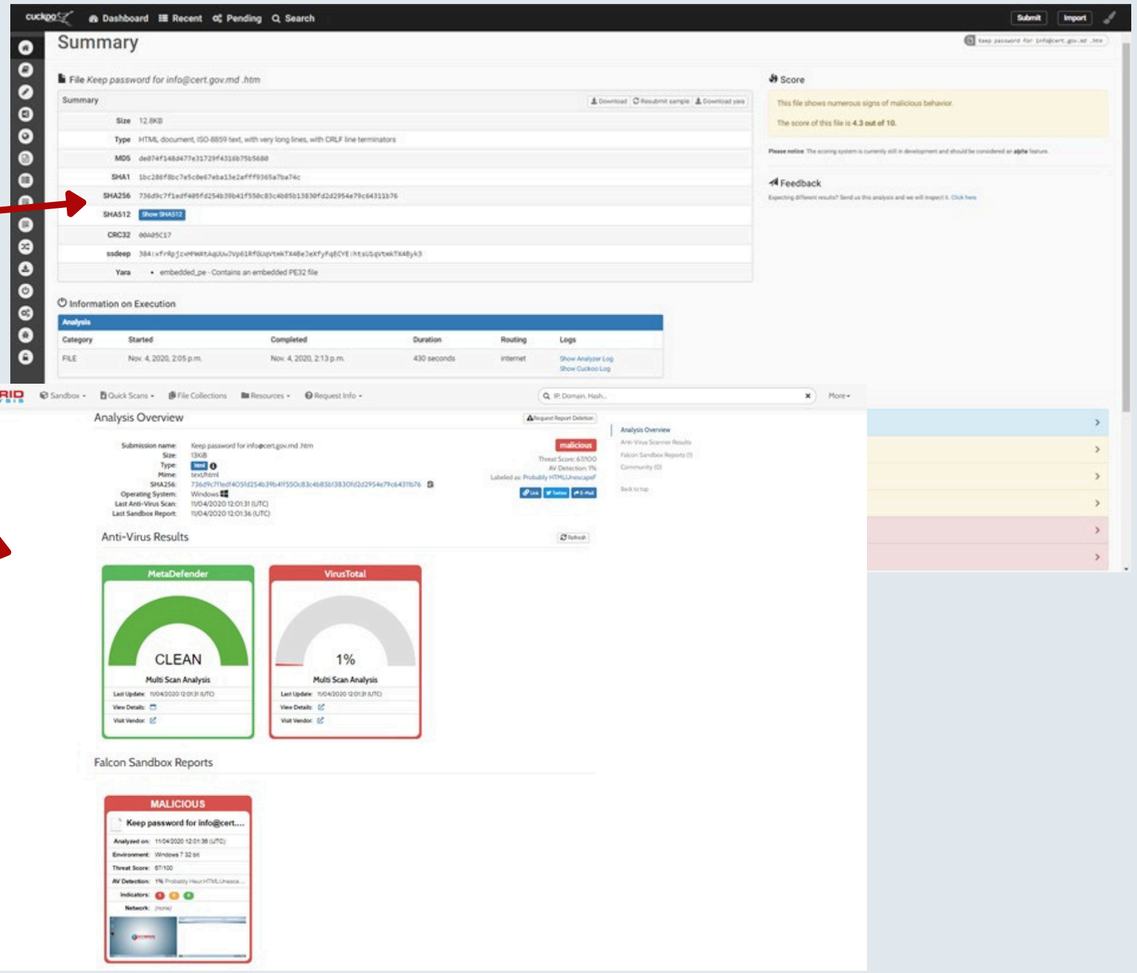
https://www.virustotal.com/gui/

Verificarea atașamentelor și link-urilor

Este recomandată scanarea fișierelor atașate la mesaje suspicioase, evitînd deschiderea sau lansarea lor.

- VIRUSTOTAL (https://www.virustotal.com/gui/)
- Hybrid Analysis (https://www.hybrid-analysis.com/)
- Cuckoo Sandbox, (https://cuckoo.cert.ee/)





Amenințări din interiorul organizațiilor

O amenințare din interior este o amenințare care poate duce la un incident de securitate cibernetică, efectuată de o persoană sau de un grup de persoane afiliate care lucrează pentru organizație.

Măsuri de prevenție

- **Instruiți-vă echipa**- O forță de muncă activă, instruită să recunoască și să raporteze activitatea suspectă sau comportamentul inadecvat, poate ajuta la apărarea împotriva amenințărilor din interior.
- **Reduceți accesul** - Reduceți numărul de utilizatori cu privilegii și acces la informații sensibile.
- **Alocați scoruri de risc -** Aplicațiile cognitive pentru analiza comportamentală pot atribui scoruri de risc pentru a identifica în mod proactiv riscurile potențiale din interior, înainte de a se produce o încălcare.
- **Introduceți un plan de contramăsuri-** Includeți un cadru de gestionare a riscurilor, un plan de continuitate a activității, un program de recuperare în caz de dezastru, o politică de management financiar și contabil și un management legal și de reglementare.
- **Implementați controale tehnice** - Implementați prevenirea pierderii de date (DLP) pentru a proteja activele și pentru a preveni exfiltrarea datelor.
- **Întăriți securitatea cibernetică**- Fiți conștienți de importanța securității rețelei, sistemelor, aplicațiilor, datelor și conturilor.

Bune practici privind resursele informaționale

Managementul Parolelor

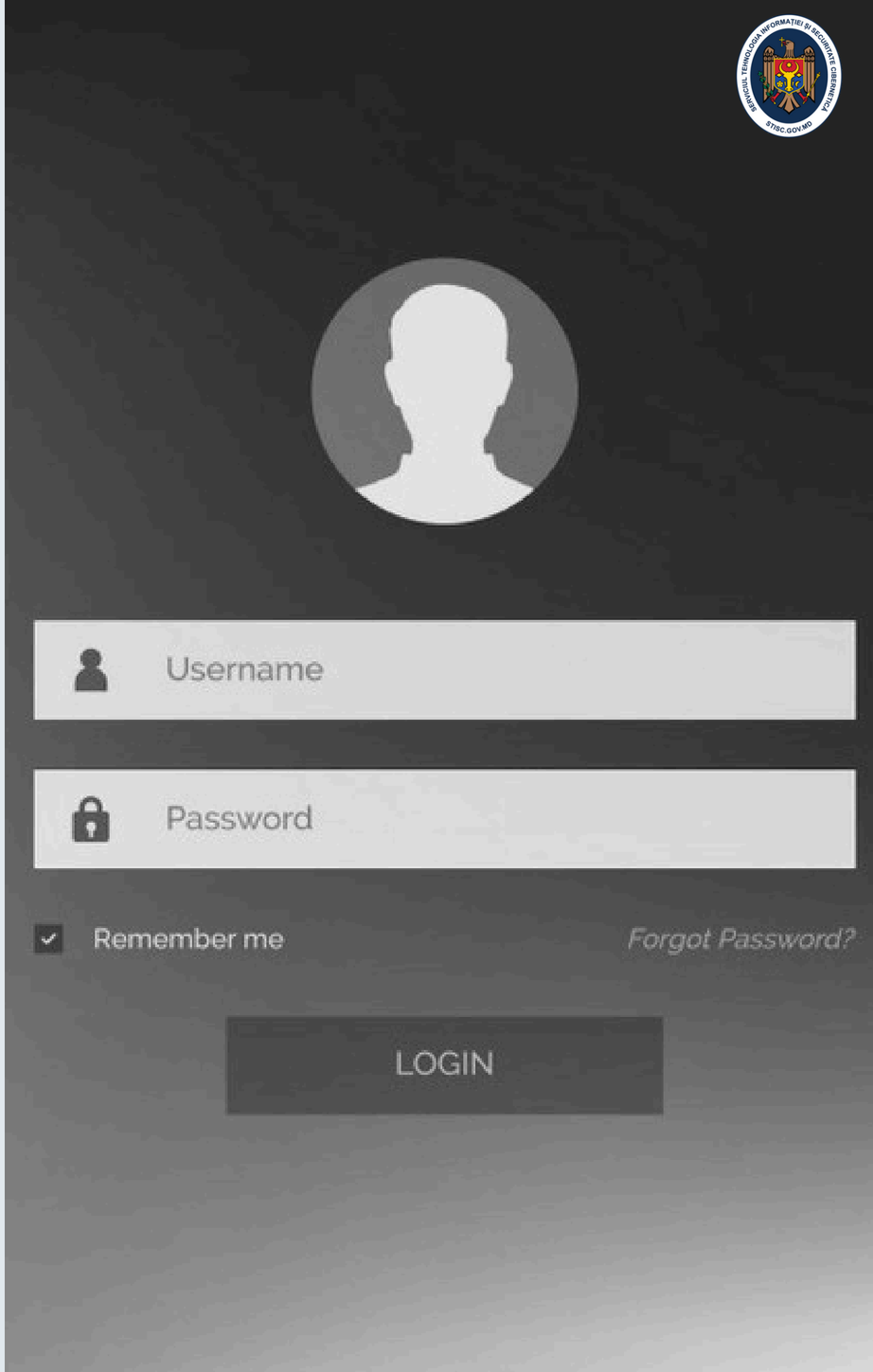
- **Utilizați parole complexe, puternice și unice** - folosiți parole impredicibile și păstrați confidențialitatea acestora.

- O parolă trebuie să îndeplinească condiții precum, să aibă o lungime minimă de **8 caractere pentru conturile de utilizator** și **12 caractere pentru conturile de administrator**, să fie complexă, să includă **combinații de cifre, caractere minuscule și majuscule, simboluri speciale**.

- Aplicați **autentificarea multifactorială** - aceasta reprezintă o metodă foarte eficientă care folosește un dispozitiv suplimentar (de exemplu token de securitate sau smartphone-ul) pentru a confirma într-un pas suplimentar identitatea persoanei care se autentifică.

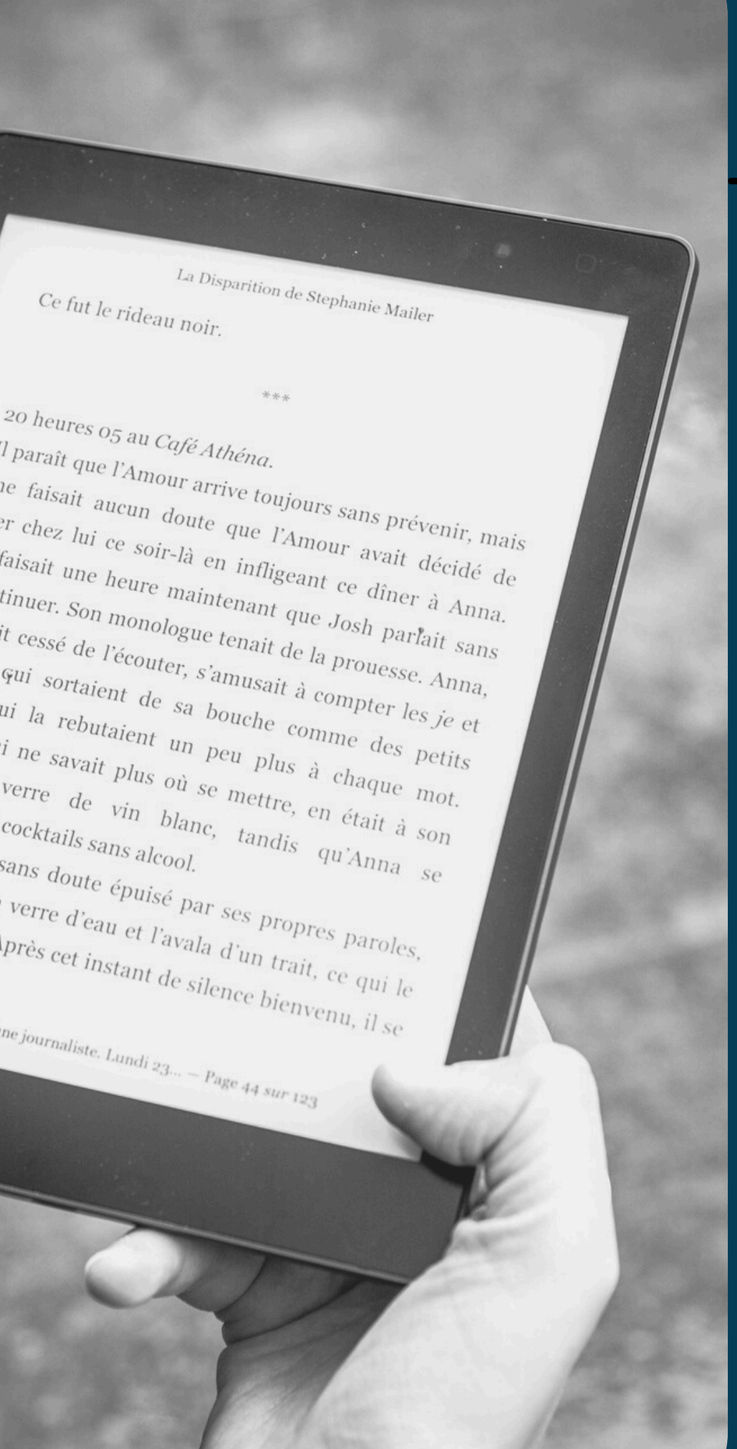
- Schimbați periodic parolele la intervale de **1-3 luni**.

- Nu reutilizați aceeași parolă pentru mai multe servicii.



Securizarea stației de lucru (PC/Laptop)

- **Blocarea ecranului de lucru -** în mod obligatoriu la părăsirea stației de lucru (prin apăsarea combinațiilor de taste Windows+L).
- **Instalarea și actualizarea permanentă a aplicațiilor antivirus** și a programelor de securitate complexe pentru detecția și protecția față de cele mai noi forme de amenințări.
- **Gestionarea parolelor** - utilizarea, la necesitate, a unui manager de parole pentru a stoca parole complexe, unice, generate de calculator.
- **Criptarea datelor sensibile** la nivel de fișier individual, folder sau întreg drive logic.
- **Securizarea sistemului de operare** - prin repararea periodică a erorilor software și/ sau breșelor de securitate și controlul utilizatorilor.
- **Actualizarea aplicațiilor** – este necesară activarea actualizărilor automate a tuturor aplicațiilor esențiale (la nivel de sistem de operare, ativirus, firewall sau IDPS).
- **Copii de rezervă a datelor** -datele trebuie periodic salvate (backup) și stocate pe suporturi magneto-optice de încredere, depozitate în locuri sigure și eventual criptate pentru a evita accesul neautorizat.
- **Utilizați conturi cu drepturi limitate** – utilizarea unor conturi limitate î va bloca accesul la zone sensibile ale sistemului de operare și va bloca implicit atacurile ce vizează serviciile sistemului de operare, fișierele sau bibliotecile sale.



Securizarea echipamentelor mobile

- **Activați facilităților de protecție antifurt** – recunoașterea facială sau a amprentelor, deblocarea dispozitivului pe baza unor modele sau prin PIN, localizarea dispozitivului, blocarea accesului sau ștergerea datelor de la distanță.
- **Sincronizați datele** – sincronizarea datelor cu alte echipamente sau utilizarea serviciilor în cloud permite ca informații importante (documente, contacte, fișiere) să fie disponibile atunci când dispozitivul este pierdut, s-a defectat sau a fost furat.
- **Actualizați aplicațiile** – sistemul de operare și aplicațiile trebuie să fie actualizat constant pentru a fixa breșele de securitate și a utiliza cele mei noi funcționalități.
- **Dezactivați conexiunile neutilizate** – se recomandă dezactivarea conexiunilor infraroșu, bluetooth sau wi-fi dacă nu sunt utilizate, pentru a bloca accesul neautorizat.
- **Utilizați aplicații sigure** – descărcați aplicații numai din surse oficiale.
- **Utilizați medii de stocare verificate** – înainte de conectare, mediul de stocare
- detașabil trebuie scanat cu instrumente antimalware.
- **Verificați drepturile de acces ale aplicațiilor** – utilizați permission manager pentru a seta accesul fiecărei aplicații la resurse (cameră, microfon, locație, stocare) și informații.
- **Conexiuni securizate de date** – se recomandă evitarea hotspot-urilor Wi-Fi publice și utilizarea datelor mobile ori de câte ori este posibil.
- **Utilizați cu precauție a codurilor QR (quick response)** – codurile QR pot conține link-uri către pagini web malițioase.

Securizarea contului de e-mail

- **Nu da-ți click pe link-uri și nu descărcați fișiere atașate** – dacă nu sunteți siguri de sursa e-mailului. **Utilizați comunicarea securizată prin e-mail**, cu semnături digitale sau criptare – când transmiteți date și informații sensibile.
- **Evitați stocarea informațiilor sensibile** în conturile personale de e-mail sau din alte rețele din afara companiei.
- **Folosiți autentificarea în doi pași** – pentru a vă proteja conturile.
- **Folosiți parole** complexe, puternice și unice**.**
- **Verificați** din cel puțin 2 surse informațiile prestatorului băncii prin canale diferite – atunci când transferați bani.
- **Folosiți soluții de securitate pentru e-mail,** actualizați-le cu regularitate
- **Nu utilizați adresele de e-mail corporative pentru mesajele private**
- **Nu accesați e-mail-urile folosind** rețele de hotspot-uri și Wi-Fi public. Utilizați, în asemenea circumstanțe, rețeua mobilă sau rețele virtuale private (VPN).