Co-funded by the Erasmus+ Programme of the European Union

Module de instruire InCyT

Securitatea informațiilor pentru manageri **Unitatea 2 Săptămâna 3** **Denumirea unității: Managementul securității informațiilor-1**	
Activități de învățare	❑ **Webinar** ❑ **Exerciții** ❑ **Workshop** ❑ **Prezentare** ❑ **Alte** Streaming webinar, text, exerciții de autoevaluare, exerciții cu răspunsuri pe forumuri de discuții și să fie discutate cu trainerul/mentorul
Responsabil de învățare	• Fatma Gökdemir • Ali Gökdemir
Obiectivele activității de învățare	1. Securitatea informațiilor 2. Politici de securitate a informațiilor 3. Roluri de securitate a informațiilor
Abilități de dobândit	• IS 1 • IS 3 • MS 3
Durata activității de învățare	2 săptămâni
Cerințe de învățare	***Ce e necesar?*** • Cunoștințe medii de calculator

Co-funded by the
Erasmus+ Programme
of the European Union

Informații scurte despre modul

Descriere
Securitatea informației este de mare importanță în asigurarea continuității fiecărei organizații și asigură protecția informațiilor critice ale organizației și a altor active informaționale în diverse medii, în special în cele electronice. Nu numai companiile mari, holdingurile, ci și IMM-urile, agențiile guvernamentale, orice organizație non-profit, școala sau persoanele singure se confruntă în mod constant cu probleme și riscuri de securitate a informațiilor, deși la diferite niveluri. În investițiile pentru a face față acestor riscuri, soluția cea mai scumpă și cea mai complexă nu este întotdeauna cea mai sigură soluție. Fiecare persoană sau organizație trebuie să aleagă și să implementeze soluția cea mai potrivită și corectă. Nu trebuie uitat că, deși o soluție de securitate simplă și ieftină poate fi insuficientă pentru unele instituții, aceeași soluție poate fi suficientă și eficientă pentru o altă instituție. Cu toate acestea, securitatea informațiilor nu este o lucrare care trebuie începută și terminată. Managementul securității informațiilor este un ciclu de viață care trebuie gestionat și auditat în mod constant atâta timp cât instituțiile și informațiile există. În acest modul va fi explicat conceptul de securitate a informațiilor, importanța acestuia și ce ar trebui făcut pentru securitatea informațiilor. Subiectul a fost susținut de un exemplu practic

Conținutul materialului de învățare

1. Securitatea informațiilor

Securitatea informațiilor este aceea de a preveni accesul neautorizat sau neautorizat, utilizarea, modificarea, dezvăluirea, distrugerea, înlocuirea și deteriorarea informațiilor. Este format din trei elemente de bază numite Confidențialitate, Integritate și Accesibilitate (Figura 1). Dacă oricare dintre aceste trei elemente de securitate de bază este deteriorat, apare o vulnerabilitate de securitate.

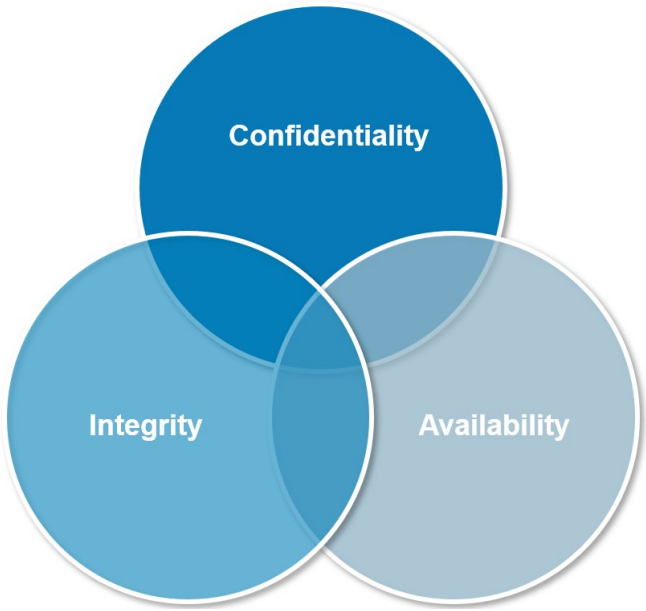


Figura 1. Elemente de securitate a informațiilor

- Confidențialitate: este protecția informațiilor împotriva accesului neautorizat și a accesului neautorizat.
- Integritate: informațiile nu sunt modificate de persoane neautorizate.
- Accesibilitate: informațiile sunt accesibile și utilizabile atunci când au nevoie de persoane autorizate.

1.1. Ce este o politică de securitate a informațiilor?

Amenințările de securitate evoluează constant, iar cerințele de conformitate devin din ce în ce mai complexe. Organizațiile trebuie să creeze o politică cuprinzătoare de securitate a informațiilor pentru a acoperi ambele provocări. O politică de securitate a informațiilor (ISP) este un set de reguli, politici și proceduri concepute pentru a se asigura că toți utilizatorii finali și rețelele dintr-o organizație îndeplinesc cerințele minime de securitate IT și protecție a datelor. O politică de securitate a informațiilor face posibilă coordonarea și aplicarea unui program de securitate și comunicarea măsurilor de securitate către terți și auditori externi.

1.2. Care este scopul unei politici de securitate a informațiilor?

O politică de securitate a informațiilor urmărește să implementeze protecții și să limiteze distribuirea datelor doar la cei cu acces autorizat. Organizațiile creează ISP-uri pentru:

- Stabiliți o abordare generală a securității informațiilor
- Documentați măsurile de securitate și politicile de control al accesului utilizatorilor
- Detectați și minimizați impactul activelor informaționale compromise, cum ar fi utilizarea greșită a datelor, rețelelor, dispozitivelor mobile, computerelor și aplicațiilor
- Protejați reputația organizației
- Respectați cerințele legale și de reglementare precum ENISA, NIST, GDPR, HIPAA și FERPA
- Protejați datele clienților lor, cum ar fi numerele de card de credit
- Furnizați mecanisme eficiente de răspuns la plângeri și întrebări legate de riscurile reale sau percepute de securitate cibernetică, cum ar fi phishing, malware și ransomware
- Limitați accesul la activele cheie ale tehnologiei informației la cei care au o utilizare acceptabilă

1.3. De ce este importantă o politică de securitate a informațiilor?

Crearea unei politici eficiente de securitate a informațiilor și care să îndeplinească toate cerințele de conformitate este un pas critic în prevenirea incidentelor de securitate, cum ar fi scurgerile de date și încălcările de date.

ISP-urile sunt importante pentru organizațiile noi și consacrate. Creșterea digitalizării înseamnă că fiecare angajat generează date și o parte din aceste date trebuie protejată împotriva accesului neautorizat. În funcție de industria dvs., acesta poate fi chiar protejat de legi și reglementări.

Datele sensibile, informațiile de identificare personală (PII) și proprietatea intelectuală trebuie protejate la un standard mai înalt decât alte date.

Indiferent dacă vă place sau nu, securitatea informațiilor (InfoSec) este importantă la fiecare nivel al organizației dumneavoastră. Și în afara organizației tale.

Politicile de securitate a informațiilor pot avea următoarele beneficii pentru o organizație:

- **Facilitează integritatea datelor, disponibilitatea și confidențialitatea —** politici eficiente de securitate a informațiilor standardizează regulile și procesele care protejează împotriva vectorilor care amenință integritatea, disponibilitatea și confidențialitatea datelor.
- **Protejează datele sensibile —** Politicile de securitate a informațiilor acordă prioritate protecției proprietății intelectuale și a datelor sensibile, cum ar fi informațiile de identificare personală (PII).
- **Minimizează riscul incidentelor de securitate —** O politică de securitate a informațiilor

ajută organizațiile să definească proceduri pentru identificarea și atenuarea vulnerabilităților și riscurilor. De asemenea, detaliază răspunsurile rapide pentru a minimiza daunele în timpul unui incident de securitate.

- **Execută programe de securitate în întreaga organizație** — Politicile de securitate a informațiilor oferă cadrul pentru operaționalizarea procedurilor.
- **Oferă o declarație clară de securitate** terților — Politicile de securitate a informațiilor rezumă poziția de securitate a organizației și explică modul în care organizația protejează resursele și activele IT. Ele facilitează răspunsul rapid la solicitările de informații ale terților din partea clienților, partenerilor și auditorilor.
- **Ajută la respectarea cerințelor de reglementare** — Crearea unei politici de securitate a informațiilor poate ajuta organizațiile să identifice lacunele de securitate legate de cerințele de reglementare și să le rezolve.

1.4. Ce ar trebui să fie într-o politică de securitate a informațiilor?

O politică de securitate a informațiilor poate fi greu de construit de la zero; trebuie să fie robust și să vă asigure organizația din toate punctele de vedere. Ar trebui să acopere toate programele, hardware-ul, parametrii fizici, resursele umane, informațiile și controlul accesului. De asemenea, trebuie să fie flexibil și să aibă spațiu pentru revizuire și actualizare și, cel mai important, trebuie să fie practic și aplicabil. Gândirea dorințelor nu vă va ajuta atunci când dezvoltați o politică de securitate a informațiilor. Trebuie să lucrați cu părțile interesate majore pentru a dezvolta o politică care să funcționeze pentru compania dvs. și pentru angajații care vor fi responsabili pentru implementarea politicii..

1. ***Politica de utilizare acceptabilă***

Această politică subliniază utilizarea acceptabilă a echipamentelor informatice și a internetului în organizația dumneavoastră. Utilizarea incorectă a internetului sau a computerelor vă deschid compania către riscuri precum atacuri de viruși, sisteme și servicii de rețea compromise și probleme legale, așa că este important să aveți în scris ce este și ce nu este utilizarea acceptabilă.
O politică de utilizare acceptabilă ar trebui să sublinieze de ce sunt responsabili angajații în ceea ce privește protecția echipamentelor companiei, cum ar fi blocarea computerelor atunci când sunt departe de birou sau protejarea tabletelor sau a altor dispozitive electronice care ar putea conține informații sensibile. De asemenea, ar trebui să sublinieze care sunt drepturile companiei și ce activități nu sunt interzise pe echipamentele și rețeaua companiei.

2. ***Politica de birou curat***

O politică de birou curat se concentrează pe protecția activelor fizice și a informațiilor. În mod ideal, această politică va asigura că toate materialele sensibile și confidențiale sunt închise sau securizate în alt mod atunci când nu sunt utilizate sau un angajat își părăsește biroul. Această

politică ar trebui să stabilească cerințele minime pentru menținerea unui birou curat, cum ar fi locul unde pot fi stocate și accesate informațiile sensibile despre angajați, proprietate intelectuală, clienți și furnizori. De asemenea, ar trebui să acopere lucruri precum ce tipuri de materiale trebuie să fie mărunțite sau aruncate, dacă parolele trebuie folosite pentru a prelua documente de la o imprimantă și ce informații sau proprietăți trebuie să fie securizate cu un lacăt fizic. Pe lângă faptul că este o parte comună și importantă a oricărei politici de securitate a informațiilor, o politică de birou curat este conformă cu ISO 27001/17799 și vă va ajuta afacerea să treacă un audit de certificare.

3. *Politica de răspuns la încălcarea datelor*

Acesta este, de asemenea, cunoscut sub numele de plan de răspuns la incident. Scopul unei politici de răspuns la încălcarea datelor este de a stabili obiectivele și viziunea asupra modului în care organizația dvs. va răspunde la o încălcare a datelor. Acest plan va ajuta la atenuarea riscurilor de a fi victima unui atac cibernetic, deoarece va detalia modul în care organizația dumneavoastră intenționează să protejeze activele de date pe parcursul procesului de răspuns la incident.

Această politică ar trebui să definească cui se aplică și când intră în vigoare, inclusiv definirea unei încălcări, rolurile și responsabilitățile personalului, standardele și valorile, mecanismele de raportare, remediere și feedback.

4. *Politica privind planul de recuperare în caz de dezastru*

Această politică este diferită de un plan de răspuns la încălcarea datelor, deoarece este un plan general de urgență pentru ceea ce trebuie făcut în cazul unui dezastru sau al oricărui eveniment care cauzează o întârziere extinsă a serviciului. Această politică ar trebui să descrie procesul de recuperare a sistemelor, aplicațiilor și datelor în timpul sau după orice tip de dezastru care provoacă o întrerupere majoră. Acest plan de recuperare în caz de dezastru ar trebui actualizat anual.

Planul de urgență ar trebui să acopere aceste elemente:

- Planul de urgență. Enumerați în mod explicit cine trebuie să fie contactat, când trebuie să fie contactat și cum îi veți contacta?
- Plan de succesiune. Descrieți fluxul de responsabilitate atunci când personalul normal nu este disponibil pentru a-și îndeplini sarcinile.
- Plan de clasificare a datelor. Detaliați toate datele stocate pe toate sistemele, criticitatea și confidențialitatea acestora.
- Criticitatea listei de servicii. Enumerați toate serviciile oferite și ordinea lor de importanță.
- Plan de backup și restaurare a datelor. Detaliați pentru ce date se face backup, unde și cât de des. De asemenea, explicați cum pot fi recuperate datele.

- Plan de înlocuire a echipamentelor. Descrieți ce servicii de infrastructură sunt necesare pentru a relua furnizarea de servicii clienților.
- Comunicari publice. Documentați cine va deține funcția externă de relații publice și oferiți îndrumări cu privire la informațiile care pot și ar trebui partajate.
- Este important ca echipa de management să aloce timp pentru a testa planul de recuperare în caz de dezastru. În timpul acestor teste, cunoscute și sub denumirea de exerciții de masă, scopul este de a identifica problemele care ar putea să nu fie evidente în faza de planificare care ar putea duce la eșecul planului. În acest fel, echipa poate ajusta planul înainte să aibă loc un dezastru.

5. Politica de e-mail

E-mailul este un canal de comunicare esențial pentru companiile de toate tipurile, iar utilizarea greșită a e-mailului poate reprezenta multe amenințări la adresa securității companiei dvs., fie că este vorba de angajați care folosesc e-mailul pentru a distribui informații confidențiale sau de expunerea din neatenție a rețelei dumneavoastră la un virus. Este important ca toți angajații, contractanții și agenții care operează în numele companiei dvs. să înțeleagă utilizarea adecvată a e-mailului și să aibă politici și proceduri stabilite pentru arhivarea, semnalarea și revizuirea e-mailurilor atunci când este necesar.

Această politică trebuie să sublinieze utilizarea adecvată a adreselor de e-mail ale companiei și să acopere lucruri precum ce tipuri de comunicații sunt interzise, standardele de securitate a datelor pentru atașamente, regulile privind păstrarea e-mailurilor și dacă compania monitorizează e-mailurile. Această politică ar trebui, de asemenea, prezentată în mod clar pentru angajații dvs., astfel încât aceștia să înțeleagă responsabilitatea lor în utilizarea adreselor lor de e-mail și responsabilitatea companiei de a se asigura că e-mailurile sunt utilizate în mod corespunzător. Această politică de e-mail nu se referă la crearea unei politici „înțeleg” pentru a-i surprinde pe angajați care folosesc abuziv e-mailul, ci pentru a evita o situație în care angajații folosesc greșit un e-mail pentru că nu înțeleg ce este și ce nu este permis.

6. Politica de protecție a cheii de criptare a utilizatorului final

Este posibil ca anumite documente și comunicări din interiorul companiei dvs. sau distribuite utilizatorilor finali să fie criptate din motive de securitate. Aveți o politică în vigoare pentru protejarea acelor chei de criptare, astfel încât să nu fie dezvăluite sau utilizate în mod fraudulos.

Această politică ar trebui să sublinieze toate cerințele pentru protejarea cheilor de criptare și să enumere controalele operaționale și tehnice specifice aplicate pentru a le menține în siguranță. Aceasta include lucruri precum hardware rezistent la manipulare, proceduri de backup și ce trebuie făcut în cazul în care o cheie de criptare este pierdută, furată sau utilizată în mod fraudulos.

7. Politica de protecție prin parolă

Angajații dvs. au probabil o multitudine de parole pe care trebuie să le țină evidența și să le utilizeze zilnic, iar afacerea dvs. ar trebui să aibă standarde clare și explicite pentru crearea de parole puternice pentru computerele lor, conturile de e-mail, dispozitivele electronice și orice punct. de acces pe care îl au la datele sau la rețeaua dvs.

Această politică trebuie, de asemenea, să sublinieze ce pot și ce nu pot face angajații cu parolele lor. Ar putea părea evident că nu ar trebui să-și pună parolele într-un e-mail sau să le partajeze colegilor, dar nu ar trebui să presupuneți că acest lucru este cunoscut pentru toată lumea. Oferiți angajaților dvs. toate informațiile de care au nevoie pentru a crea parole puternice și pentru a le păstra în siguranță pentru a minimiza riscul de încălcare a datelor.

În cele din urmă, această politică ar trebui să sublinieze ce trebuie să facă dezvoltatorii și personalul IT pentru a se asigura că toate aplicațiile sau site-urile web conduse de compania dvs. respectă măsurile de securitate pentru a păstra parolele utilizatorilor în siguranță.

Cercetările efectuate în ultimul deceniu în întreaga lume arată că parolele cele mai preferate de utilizatori sunt după cum urmează:

- 123456
- password
- qwerty
- 111111
- 123123
- 987654321
- 123456789
- asdfgh

În ciuda avertismentelor anuale, această listă nu s-a schimbat prea mult. Pentru aceasta, utilizatorii sunt sfătuiți să urmeze un set de reguli de setare a parolelor. Aceste reguli sunt enumerate mai jos:

- tabilirea cerințelor de complexitate, cum ar fi îndeplinirea cerinței minime de caracter
- Nu alegerea parolelor utilizate anterior
- Schimbarea parolelor periodic și poate frecvent
- Parolele folosite nu trebuie alese dintre parolele comune și slab utilizate, ca în lista de mai sus

Institutul Național de Standarde și Tehnologie (NIST) și-a propus să rezolve problema politicilor de parole pentru a determina parolele și a atinge anumite standarde. NIST stabilește detalii despre parole și despre cum ar trebui să fie gestionate și stocate. În consecință, parolele posibile ar

trebui verificate cu o listă de valori utilizate în mod obișnuit și cunoscute. Considerațiile pentru determinarea parolelor sunt următoarele:

- Parolele furnizate de utilizator trebuie să conțină cel puțin opt caractere alfanumerice.
- Nu ar trebui să fie parole obținute din încălcări anterioare.
- Nu ar trebui să existe cuvinte din dicționar.
- Nu ar trebui să existe date între 1900-2020, cum ar fi datele de naștere.
- Fără caractere repetitive sau secvenţiale (de exemplu, aaaaaaaa sau 1234abcd)
- Cuvintele specifice utilizării prevăzute, cum ar fi numele serviciului, numele de utilizator și derivatele acestora nu ar trebui să fie.

Criteriile de mai sus ar trebui luate în considerare la determinarea parolelor și ar trebui create parole cu structuri complexe.

Complexitatea parolei: Complexitatea parolei este definită ca numărul de parole care sunt puternice pentru o parolă, adică aceasta îndeplinește un set de reguli. Cheia complexității parolei Regulile sunt următoarele:

- Parola nu poate conține numele contului sau variații ale numelui contului.
- Parola trebuie să conţină atât litere mari (A-Z) cât şi litere mici (a-z).
- Caractere speciale **(~! @ # $% ^ & * _- + = `| \ () {} [] :;" '<>,.? /)** (Acestea sunt caracterele care apar de obicei cu tasta ALT. Cu toate acestea, monedele precum simbolurile euro nu sunt considerate caractere speciale).
- Trebuie respectat numărul minim de caractere. Această valoare variază de la sistem la sistem, de la utilizator la utilizator. s-ar putea schimba.

Lungimea minimă a parolei trebuie să fie de 8 caractere, în timp ce caracterul recomandat este de 12.

Când parolele sunt create cu cel puțin 8 caractere conform regulilor enumerate mai sus, aceasta înseamnă cel puțin 218.340.105.584.896 de posibilități diferite pentru o singură parolă. Probabilitatea parolei generate face un atac cu forță brută foarte dificil, dar parola nu este încă imposibil de spart. Pentru o parolă care este aproape imposibil de spart, este necesar să creșteți numărul de caractere ale parolei. Cu cât numărul minim de caractere este mai mare, cu atât este nevoie de mai mult timp pentru a sparge parola.

Pe lângă beneficiile complexității parolei, aceasta aduce și unele provocări. Una dintre principalele este uitarea parolei. Este dificil să-ți amintești o parolă mai lungă și care conține caractere speciale. Mai ales atunci când toate parolele sunt diferite, este dificil să ne amintim și să nu le confundați cu altele. Prin urmare, la crearea parolelor trebuie urmată o anumită logică.

De exemplu:

- Sunt al 2-lea copil dintr-o familie cu 3 copii!

- Puteți scrie o propoziție ca aceasta pe baza propriei vieți reale. Când iei primele caractere și caracterele speciale ale propoziției, primești o parolă ca Iat2ciafw3c!
- Am devenit membru al acestui site web (despre educație) pe 19 iulie.
- Puteți personaliza o propoziție de genul „Am devenit membru al acestui site (despre educație) pe 19 iulie în funcție de zona de interes a site-ului și data aderării, astfel încât să nu o uitați. Când obțineți primul lor personaj si personaje speciale
- Veți primi o parolă precum **IBAMoTW(ae)oJ19.**

8. Politica privind planul de răspuns de securitate

Un plan de răspuns de securitate stabilește ce trebuie să facă fiecare echipă sau unitate de afaceri în cazul unui incident de securitate, cum ar fi o încălcare a datelor. Potrivit Institutului SANS, acesta ar trebui să definească „o descriere a produsului, informații de contact, căi de escaladare, acorduri de nivel de servicii așteptate (SLA), clasificare a severității și impactului și termene de atenuare/remediere”.

Cheia pentru o politică a planului de răspuns de securitate este că ajută toate echipele să-și integreze eforturile, astfel încât orice incident de securitate care se întâmplă să poată fi atenuat cât mai repede posibil. Deși fiecare departament poate avea propriile planuri de răspuns, politica privind planul de răspuns de securitate detaliază modul în care se vor coordona între ele pentru a se asigura că răspunsul la un incident de securitate este rapid și complet.

1.5. Exemple de politici de securitate a informațiilor

Pentru a crea un plan de securitate cibernetică de succes, trebuie luate în considerare 5 probleme principale.

a. ***Identifica:*** Organizația ar trebui să înțeleagă riscurile de securitate cibernetică cu care se confruntă, astfel încât să își poată prioritiza eforturile.

b. ***Proteja***: Este vorba despre punerea în aplicare a măsurilor de protecție adecvate pentru a proteja activele de date și pentru a limita sau a limita impactul unui potențial eveniment de securitate cibernetică. Aceasta include educarea și împuternicirea membrilor personalului din cadrul organizației pentru a fi conștienți de riscuri, stabilirea de proceduri care se concentrează pe protejarea securității și a activelor rețelei și, eventual, utilizarea asigurării de răspundere cibernetică pentru a proteja financiar o companie în cazul în care un criminal cibernetic este capabil să ocolească protecțiile care sunt la locul lor.

c. ***Detecta***: Subliniază activitățile care ajută la descoperirea apariției unui atac cibernetic și permit un răspuns în timp util la eveniment. Pentru a diagnostica rapid și eficient un atac cibernetic, companiile ar trebui să implementeze protocoale de clasificare a datelor, de gestionare a activelor și de gestionare a riscurilor care să le alerteze atunci când datele par a fi compromise.

d. ***Răspunde***: Documentați acțiunile adecvate care ar trebui întreprinse în urma detectării amenințărilor la adresa securității cibernetice. Răspunsul unei companii ar trebui să includă o comunicare adecvată și detaliată cu personalul, acționarii, partenerii și clienții, precum și cu organele de aplicare a legii și consilierii juridici, după cum este necesar.

e. ***Recupera***: Determinați modul în care o organizație poate recupera și restaura orice capabilități sau servicii care au fost afectate din cauza unui atac cibernetic.

Aproape fiecare standard de securitate trebuie să includă o cerință pentru un anumit tip de plan de răspuns la incident, deoarece chiar și cele mai robuste planuri de securitate a informațiilor și programe de conformitate pot cădea victimele unei încălcări a datelor.

1.6. Exerciții de Politică de securitate a informațiilor

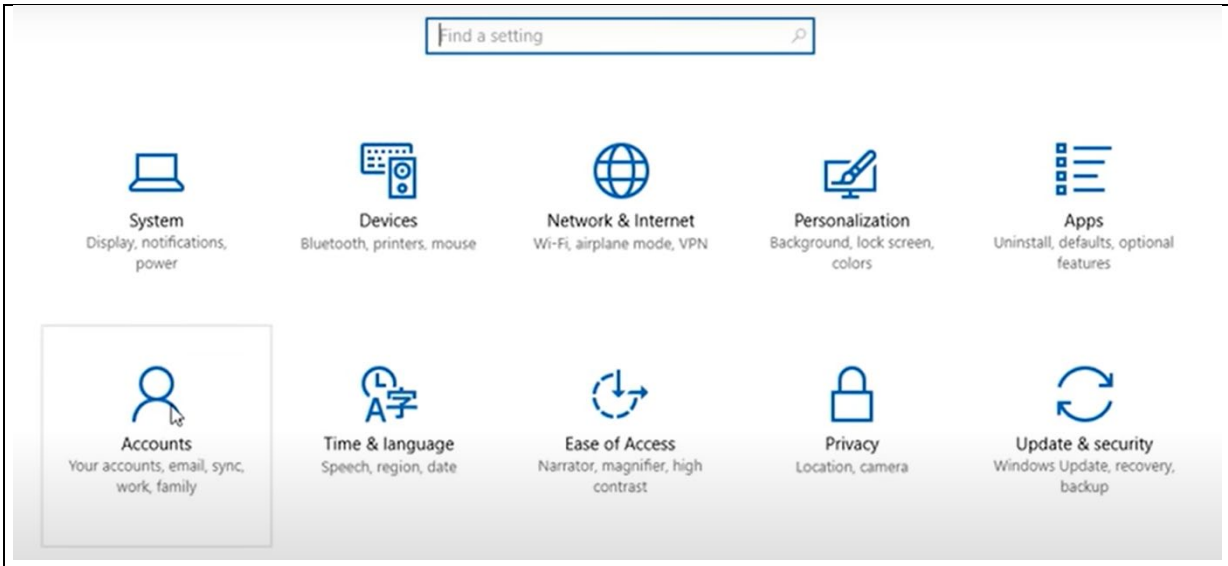
1. Blocați-vă sesiunea: Consolidați-vă conturile online activând cele mai puternice instrumente de autentificare disponibile, cum ar fi biometria (urmele biologice măsurabile ale unei persoane), cheile de securitate sau un cod unic unic generat de un instrument de aplicație pe dispozitivul dvs. mobil. Este posibil ca numele dvs. de utilizator și parolele să nu fie suficiente pentru a proteja conturi precum e-mailul, serviciile bancare și rețelele sociale.

Exerciții -1:

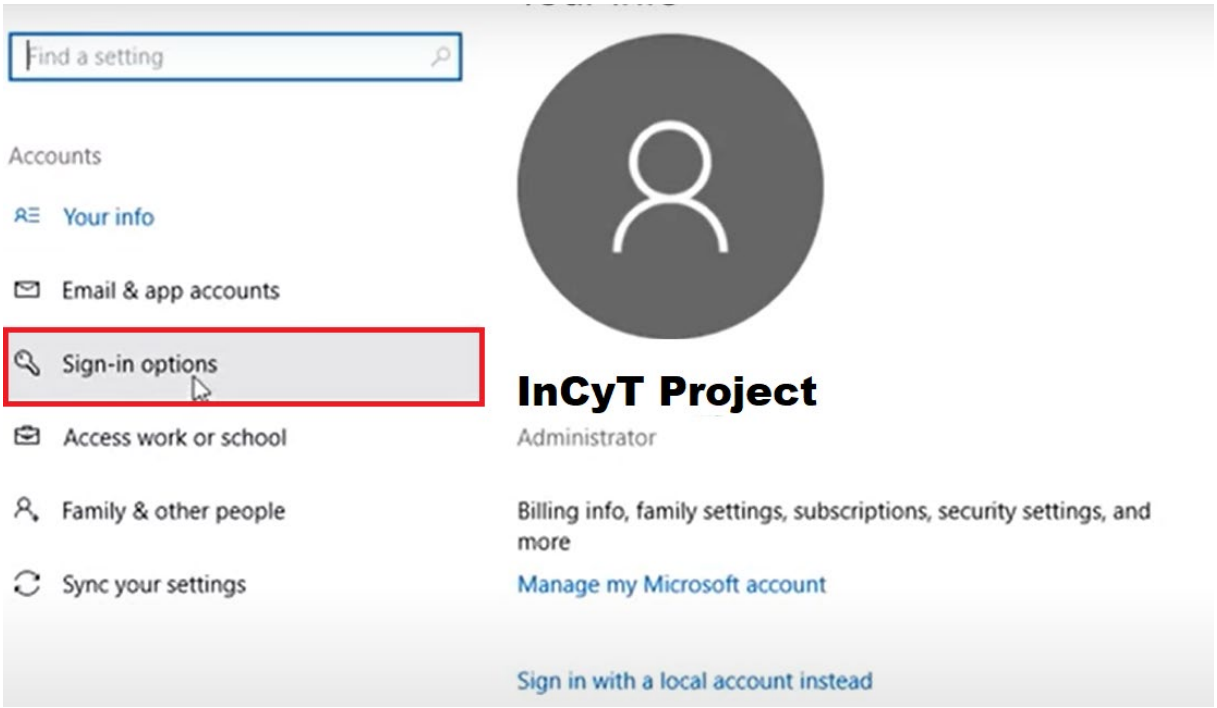
Pentru ca computerul să se blocheze automat când te ridici de pe computer.

Pasul-1: Faceți clic pe butonul Setări Windows.

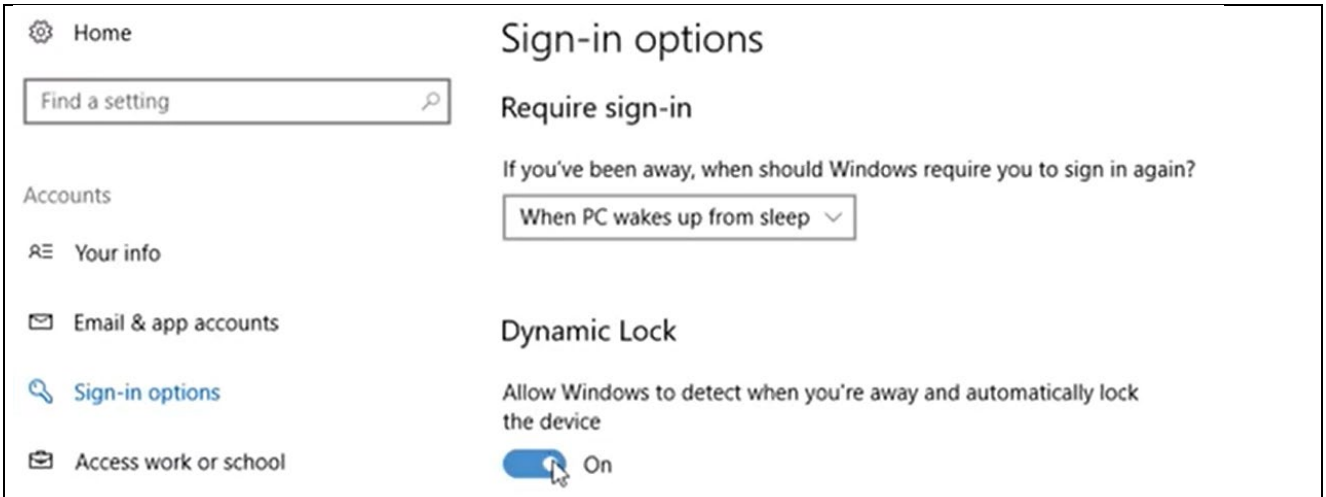
Pasul-2: Faceți clic pe fila Conturi.



Pasul-3: Faceți clic pe secțiunea Conectare.



Pasul-4: Activați pentru specificația Dynamic Lock.



2- Creați o parolă puternică: Parola are un loc important în securitatea informațiilor. Parolele slabe pot fi rezolvate într-un timp scurt cu programele de spargere a parolelor. Din acest motiv, este necesar să aveți cea mai mare grijă, luând în considerare următoarele reguli atunci când creați și utilizați parolele pe toate dispozitivele și conturile. Parola este folosită în general în multe locuri în sistemele informatice. Folosim o parolă atunci când creăm un cont de e-mail, setăm o parolă pentru autentificarea computerului și interzicem accesul la fișiere. Cu toate acestea, parolele nu ar trebui să fie slabe sau ghicibile. Parolele trebuie create conform următoarelor criterii:

a. Parolele trebuie să aibă **cel puțin 8 caractere** și să conțină cel puțin o literă mare, o literă mică, un număr și un caracter special (.-+=_,!@$#*%<>[]{}).
b. Câmpul pentru parolă **nu trebuie lăsat** necompletat sau implicit; ***123456, 01062022, qwerty, parola etc.*** nu trebuie determinată în așa fel încât să fie previzibil și ușor de spart ca cuvintele care pot fi găsite în orice dicționar.
c. c. Parolele nu trebuie să conțină informații personale (numele copilului, data nașterii sau numele instituției).
d. Ar trebui create ***parole diferite*** pentru sisteme și conturi diferite.
e. Parolele trebuie ***schimbate*** frecvent (cel puțin la fiecare 6 luni).
f. Parolele ***nu trebuie scrise*** în locuri care pot fi observate de alte persoane (cum ar fi lăsarea lor lângă computer prin scrierea pe hârtie) și nu ar trebui să fie stocate în text clar fără criptare pe un computer sau pe orice suport digital.
g. Niciun personal sau student nu trebuie să-și ***împărtășească*** parola (parola de e-mail, parola de semnătură electronică, parola PC-ului etc.) cu o altă persoană. Utilizatorii trebuie să știe că toată responsabilitatea legală care ar putea apărea în cazul partajării îi va aparține.
h. Cont unic, parolă unică: a avea o parolă separată pentru fiecare cont ajută la

împiedicarea infractorilor cibernetici. Cel puțin, separați conturile dvs. de serviciu și cele personale și asigurați-vă că conturile dvs. critice au parolele cele mai puternice.

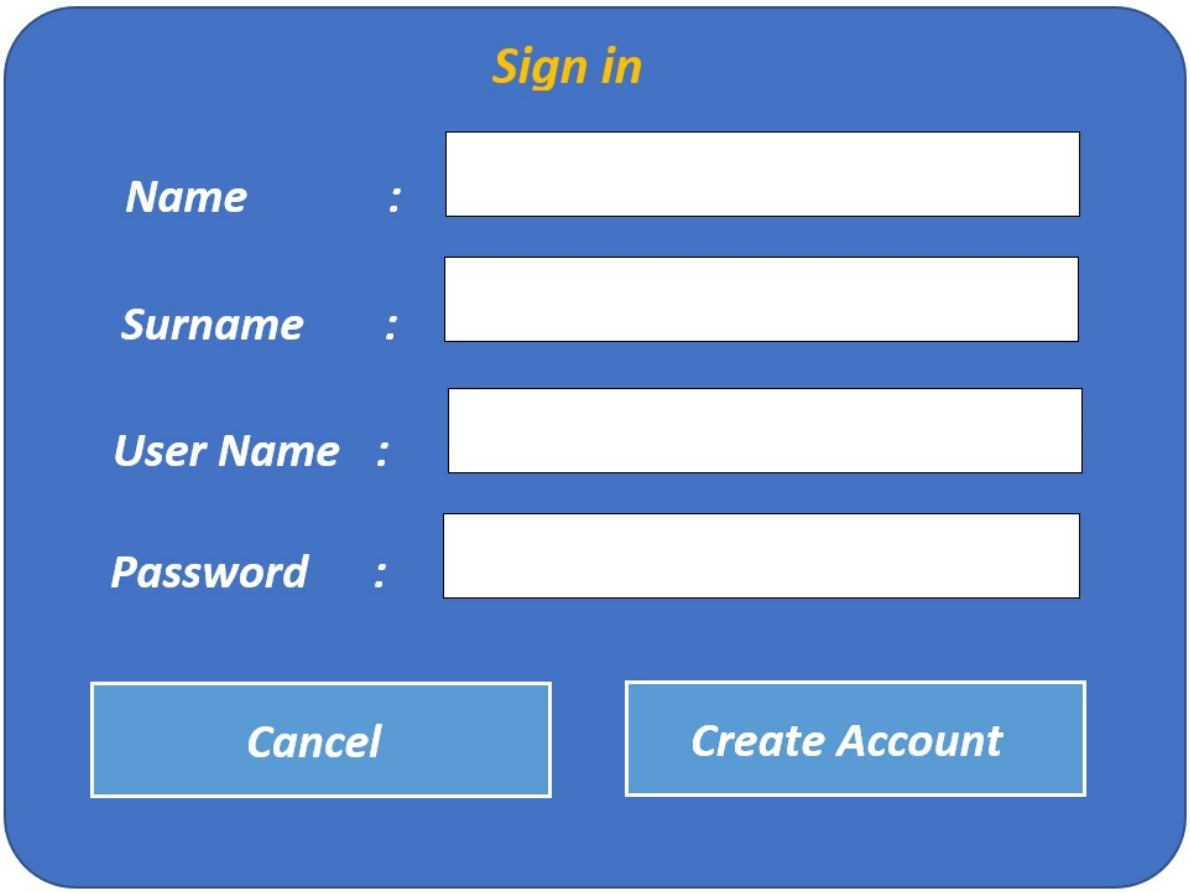
i. Amintiți-vă și păstrați-l în siguranță: parolele puternice sunt dificil de creat și reținut. Setați-vă parolele într-un mod care să fie semnificativ și memorabil doar pentru dvs. sau păstrați-le într-un loc și format sigur. Alternativ, puteți utiliza un serviciu, cum ar fi un manager de parole, pentru a vă ține evidența parolelor.

Exerciții-2:

Securitatea parolei atunci când creați un cont de e-mail prin intermediul furnizorului dvs. de servicii de e-mail corporativ sau al unei aplicații sau al site-ului web al unui furnizor de servicii de e-mail public

Pasul-1: Deschideți site-ul web sau aplicația.

Pasul-2: Introduceți informațiile dvs. personale pentru a crea un cont.



Pasul-3: Când creați o parolă, utilizați combinații de litere mari, minuscule, cifre și simboluri împreună.

Se pot face anumite coduri pentru a face parola ușor de reținut de către utilizator. De exemplu, puteți scrie o propoziție potrivită pentru subiect și puteți utiliza primele caractere, numere și caractere speciale ale propoziției pe care ați scris-o..

Acest proiect de securitate cibernetică este susținut de Erasmus+ 2021

Pasul-4: Ne setăm parola; TcpisbE+2021

Pasul-5: Asigurați-vă că parola este formată din cel puțin 8 caractere. Sunt de preferat 12 caractere. Se poate spune că parola pe care o folosim este potrivită deoarece are 12 caractere.

3- Acces la site-uri securizate (Safe Browser): Când intri online pentru a face cumpărături sau pentru a citi știri, folosești un browser. Browserele sunt una dintre modalitățile principale de a interacționa cu Internetul. Drept urmare, browserele sunt ținta principală pentru atacatorii cibernetici. Utilizați întotdeauna cea mai recentă versiune a browserului și păstrați-vă scutul de securitate puternic împotriva atacurilor browserului. Browserele actualizate au cele mai recente corecții de securitate și sunt mult mai greu de exploatat pentru atacatorii cibernetici. Nu sunteți sigur dacă aveți cea mai recentă actualizare a browserului? Contactați echipa de asistență tehnică sau echipa de securitate a informațiilor pentru a verifica. Rămâneți în siguranță online neconectându-vă la site-uri web atunci când primiți un avertisment de la browser. Browserele moderne pot recunoaște anumite site-uri web rău intenționate care sunt concepute pentru a dăuna. Dacă browserul dvs. vă anunță că site-ul web pe care urmează să îl vizitați este periculos, închideți acea pagină web și încercați să găsiți informațiile pe care le căutați pe un site web mai sigur. Înainte de a trimite informații sensibile online, de exemplu atunci când trimiteți informații despre cardul dvs. de credit pentru cumpărături online, asigurați-vă că browserul dvs. folosește HTTPS, care este un semn de criptare. Criptarea combină informațiile transmise între computerul dumneavoastră și destinație, astfel încât doar site-ul web autorizat să le poată citi. Pentru o conexiune sigură, căutați semne de criptare, cum ar fi adresa site-ului web care începe cu HTTPS și o pictogramă de lacăt în bara de stare.

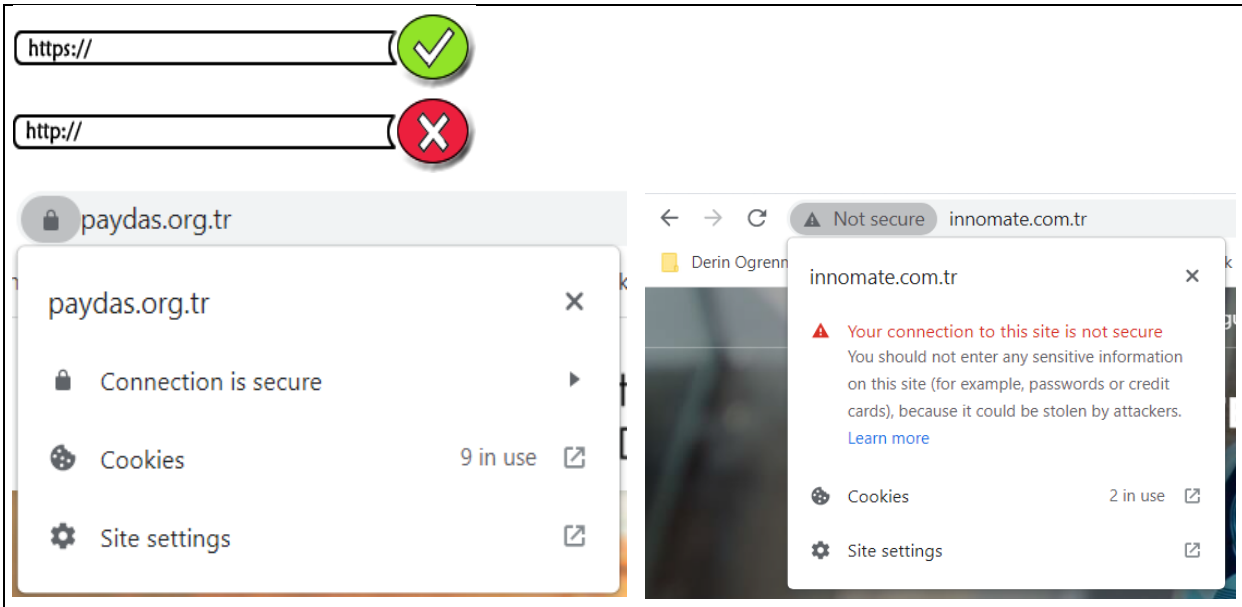


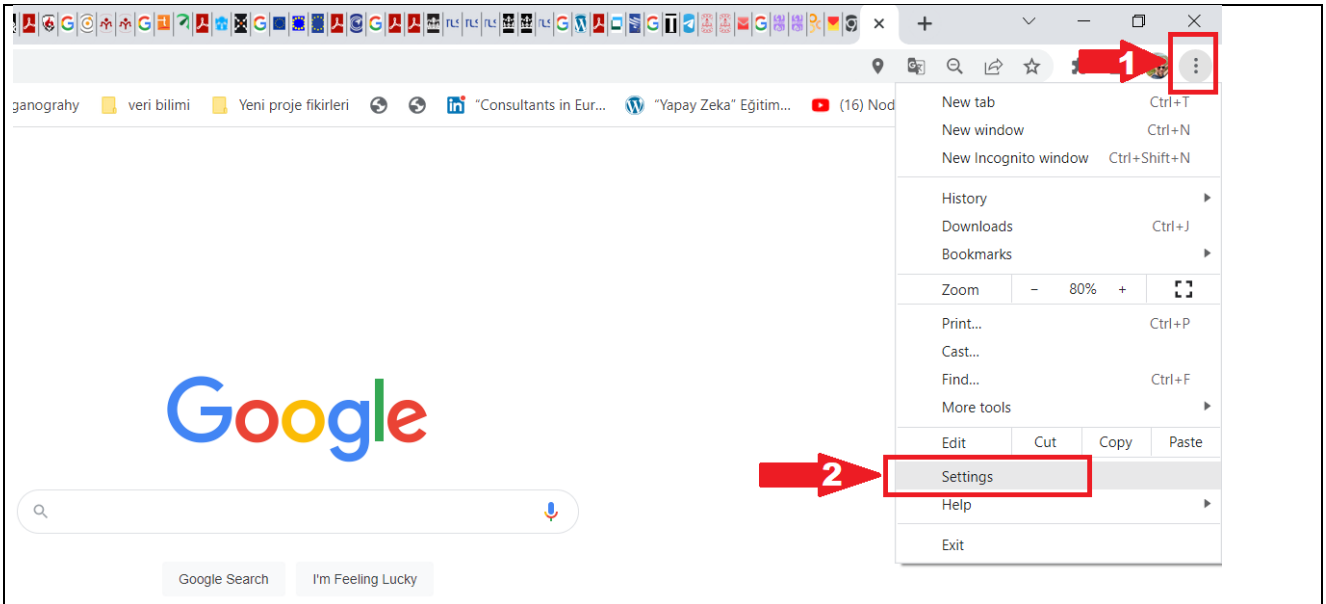
Figura 2. Site-uri web sigure și nesecurizate

Suplimente; sunt mici bucăți de software adăugate la browsere care sunt utilizate pentru funcții suplimentare, cum ar fi jocul, vizionarea de filme sau editarea textului. Fiecare supliment instalat în browser adaugă potențial vulnerabilități de securitate suplimentare. Dacă aveți absolut nevoie de ele și numai cu aprobare prealabilă, instalați suplimentele în browser. Odată instalat, utilizați întotdeauna cea mai recentă versiune a pluginului, la fel ca în browser. În cele din urmă, după ce ați terminat de vizitat un site web, asigurați-vă că sunteți deconectat. Acest lucru elimină informațiile sensibile de conectare și parolă înainte de a închide browserul. Rețineți că comportamentul dumneavoastră de navigare în siguranță și scutul de securitate sunt consolidate.

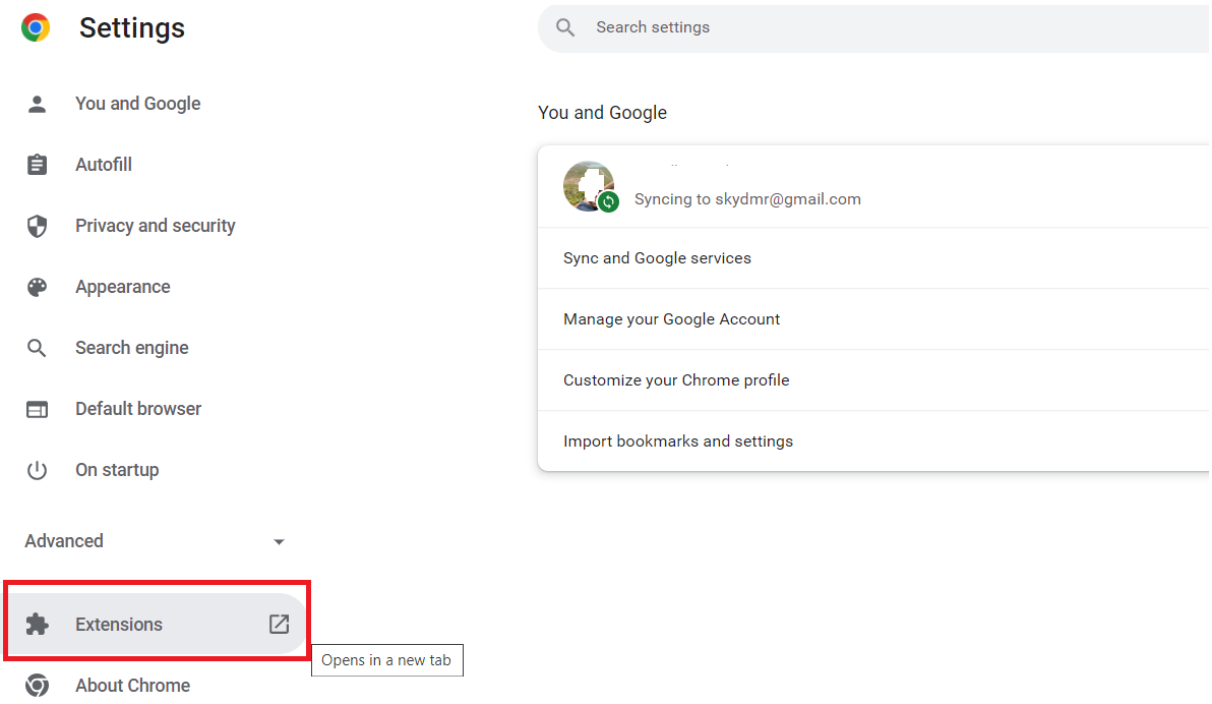
Exerciții-3:

Urmați pașii de mai jos pentru a edita plug-in-urile în browserul web.

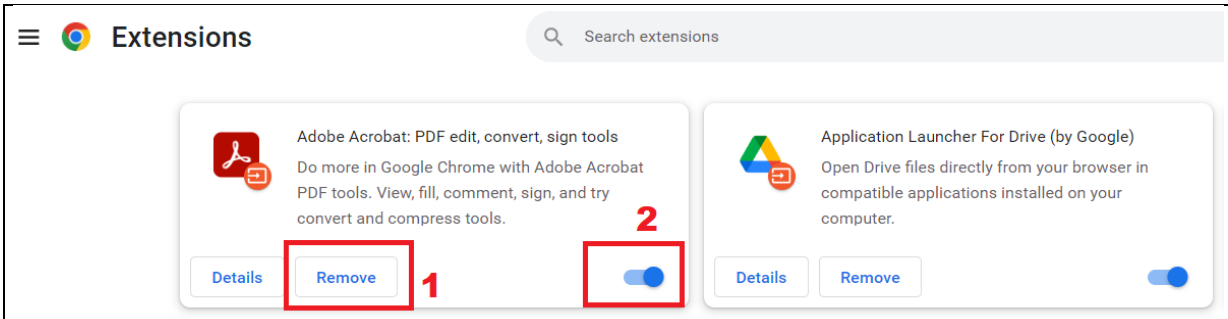
Pasul-1: Deschideți browserul web și faceți clic pe butonul „Costume și control...” din colțul din stânga sus (1). Faceți clic pe fila „Setări” din meniul derulant (2).



Pasul-2: Faceți clic pe butonul „Extensii” din fereastra care apare.



Pasul-3: Puteți vedea suplimentele instalate în browserul dvs. pe acest ecran. Dacă doriți să ștergeți suplimentul, îl puteți șterge (1) apăsând butonul „Eliminare”. Dacă doriți ca pluginul să rămână inactiv, îl puteți dezactiva din butonul „On-Off” (2).



4. E-mail, mesagerie și phishing: Aveți un e-mail în căsuța de e-mail sau un mesaj pe telefon. „Există o problemă cu contul tău și contul tău ar trebui actualizat imediat. Tot ce trebuie să faci este să dai clic pe un link.” Când primiți un mesaj cu conținut, opriți-vă și gândiți-vă înainte de a da clic! „Phishing” este un atac de inginerie socială care folosește e-mailuri sau mesaje ca momeală, cum ar fi utilizarea momeală pentru pescuit. Atacatorii cibernetici trimit mii de e-mailuri în speranța că cineva va lua momeala. E-mailurile vă solicită să efectuați o acțiune, cum ar fi să faceți clic pe un link, să deschideți un atașament sau să completați un formular. Atacatorii cibernetici nu sunt siguri exact cine va primi aceste e-mailuri, dar efectuarea uneia dintre aceste acțiuni aparent inofensive ar putea să te atragă. O formă mai sofisticată de phishing numită „Spear phishing” vizează anumite persoane. De exemplu, atunci când toată lumea din organizația noastră primește un e-mail generic de phishing referitor la un pachet nelivrat; ca și cum cinci persoane din unitatea noastră de achiziții sunt vizate cu o cerere de factură falsă. Cum știm dacă un e-mail sau un mesaj este un atac de tip phishing?

Câteva semne de căutat:

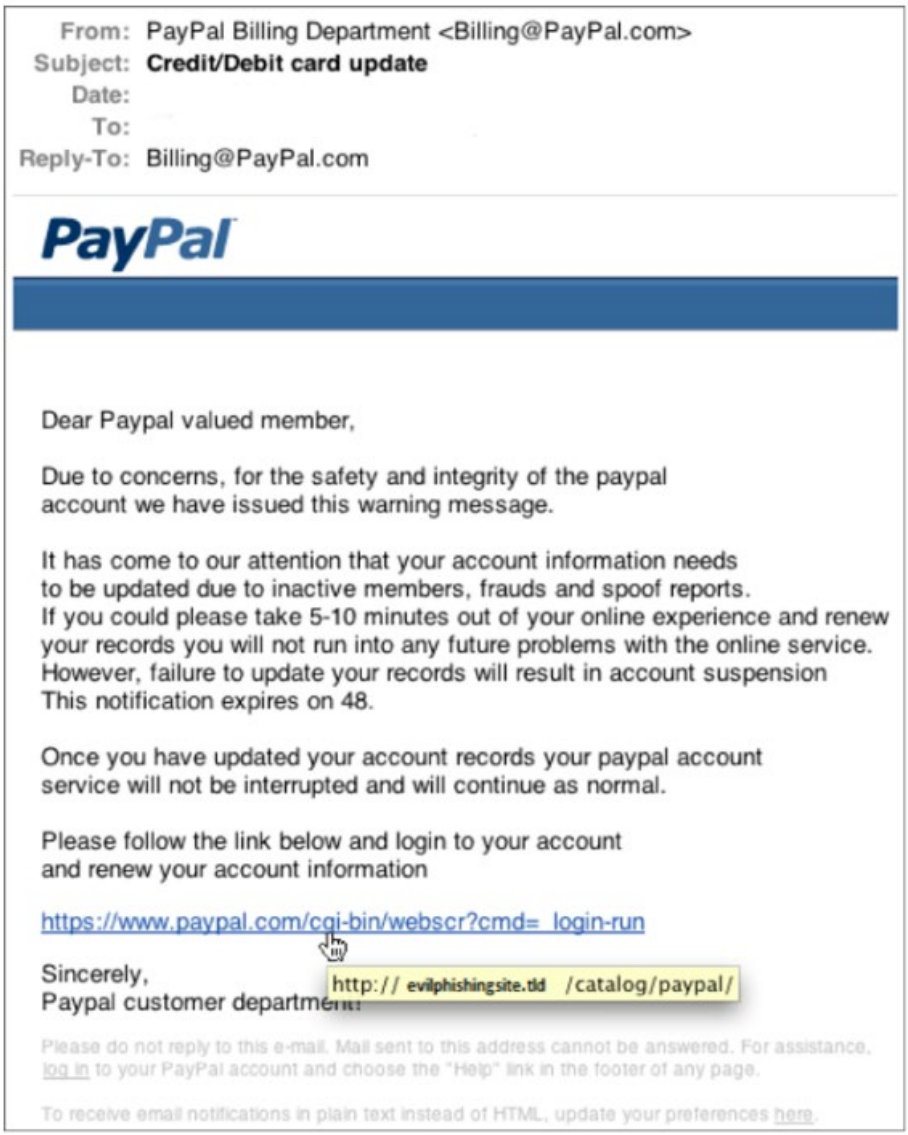
- Mesaje care încep cu „Stimate client” sau alte intrări generale de salut.
- Mesaje care necesită acțiuni imediate sau care creează un sentiment de urgență, cum ar fi amenințarea cu închiderea contului.
- Mesaje care pretind a fi de la o organizație oficială, dar care au greșeli gramaticale sau de ortografie sau care folosesc o adresă de e-mail personală, cum ar fi @gmail.com, @yahoo.com sau @hotmail.com.
- Orice mesaj care solicită informații extrem de sensibile, cum ar fi numărul cardului de credit sau parola. Fiți suspicios față de astfel de mesaje. Dacă cineva pe care îl cunoașteți, cum ar fi un coleg de muncă, vă trimite un mesaj care necesită acțiuni urgente, contactați prin diferite canale pentru a verifica dacă chiar el este cel care

v-a trimis, de exemplu printr-un apel telefonic Încercați să confirmați dacă mesajul este al lui.

Amintiți-vă, este foarte ușor pentru un atacator cibernetic să creeze un e-mail care pare să provină de la un prieten sau coleg. Pentru a fi în siguranță, ar trebui să luați întotdeauna aceste măsuri de precauție atunci când utilizați e-mailul sau mesageria. Treceți mouse-ul peste un link înainte de a da clic pe el. Aceasta va afișa adevărata destinație a linkului, astfel încât să puteți confirma că ați fost redirecționat către un site web legitim. Și mai bine este să tastați adresa site-ului direct în browser. De exemplu, dacă primiți un e-mail de la banca dvs. care vă solicită să actualizați detaliile contului, ignorați linkul trimis prin e-mail. Pur și simplu introduceți adresa site-ului web al băncii dvs. în browser și conectați-vă ca de obicei. Când mesajele au atașamente, deschideți numai atașamentele pe care le așteptați. Deoarece este posibil ca soluțiile antivirus să nu detecteze toate versiunile de malware, sunteți cea mai bună apărare pe care o avem împotriva atașamentelor infectate. Când utilizați e-mail sau mesagerie, aveți grijă să nu dezvăluiți accidental informații importante. Funcțiile de e-mail precum completarea automată facilitează trimiterea neintenționată a e-mailului către persoana greșită. De exemplu, când doriți să trimiteți un e-mail unei persoane care lucrează în unitatea dvs., puteți trimite accidental un e-mail unui prieten cu un nume similar care lucrează în altă unitate. Amintiți-vă că, odată ce un e-mail este trimis, acesta scapă de controlul dvs.

Mostre de phishing

Proba-1: În acest exemplu, e-mailul pare că a fost trimis de la PayPal.com, dar este trimis printr-un server fals. Dacă ne uităm doar la adresa web către care este direcționat, fără să facem clic pe linkul dat, putem detecta că este un e-mail recoltat de un atacator care dorește să obțină acreditări.



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date:
To:
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

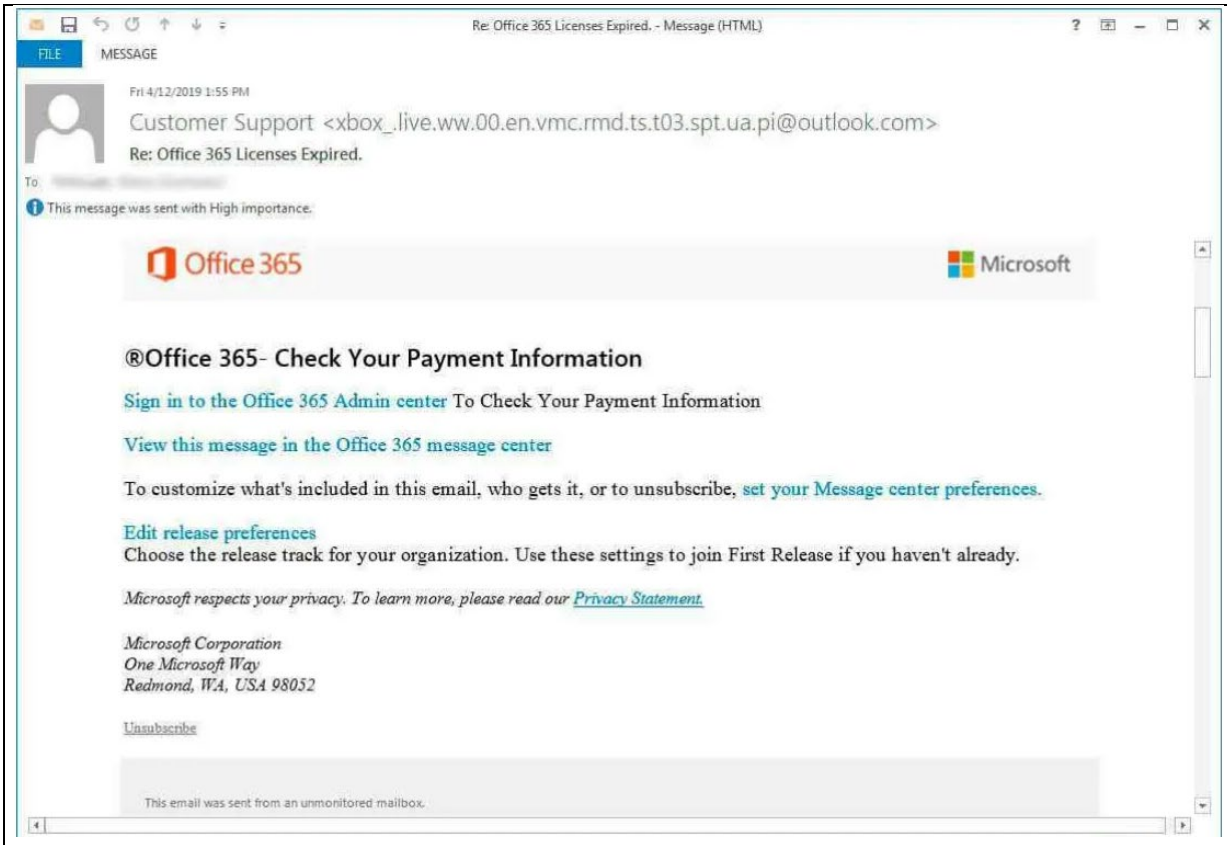
http:// evilphishingsite.tld /catalog/paypal/

Sincerely,
Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

Proba-2: În acest exemplu, un e-mail primit este un exemplu care indică faptul că licențele Office 365 ale unei organizații au expirat. Apoi, e-mailul îi spune utilizatorului să se conecteze la Centrul de administrare Office 365 pentru a verifica informațiile de plată.



Cu toate acestea, atunci când adresa de e-mail a expeditorului este examinată cu atenție, trebuie menționat că o astfel de adresă nu va exista. Pe scurt, este evident că acest e-mail nu a fost trimis de Office365.

5. Retele sociale

Site-urile de rețele sociale ne ajută să împărtășim informații și să comunicăm cu ceilalți. Din păcate, aceste site-uri facilitează atacatorii cibernetici să vă urmărească și să învețe ce faceți. Protejați-vă protejând fiecare cont cu o parolă puternică și unică. Mai bine, utilizați o parolă diferită pentru fiecare cont și utilizați autentificarea cu doi factori, dacă este disponibilă. Multe site-uri de rețele sociale acceptă și aplicații terță parte. Instalați numai aplicațiile de care aveți nevoie din surse de încredere și numai. Verificați evaluarea, comentariile și permisiunile oricărei aplicații înainte de a o instala. Dacă nu mai aveți nevoie de o aplicație, dezinstalați-o sau dezactivați-i accesul la profilul de rețea socială.

La fel ca e-mailul și mesageria, atacatorii cibernetici pot încerca să vă înșele pe site-urile de rețele sociale. El poate trimite mesaje pretinzând că este prietenul tău. Dacă primiți un mesaj ciudat sau suspect de la un prieten, contactați-l prin e-mail sau telefon, nu răspunzând la mesaj. În cele din

urmă, pentru a ne proteja Instituția, nu publicați informații confidențiale despre Instituția noastră pe niciun site web. Dacă aveți întrebări despre ceea ce puteți publica sau împărtăși despre post, vă rugăm să întrebați supervizorul dvs.

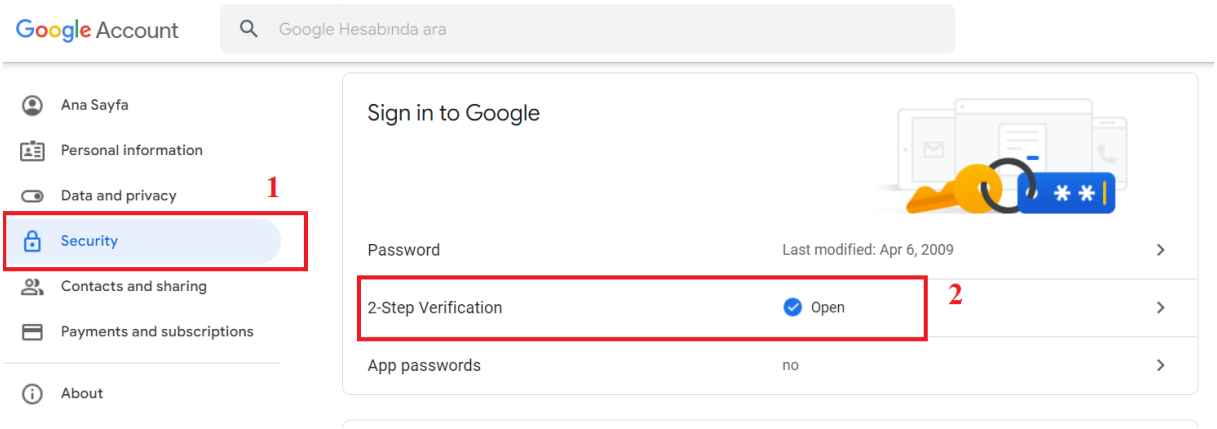
După activarea autentificării în doi factori (verificare), un cod de securitate va fi trimis către telefon sau aplicație de autentificare de fiecare dată când vă conectați la contul dvs. de pe un dispozitiv sau browser nou. Trebuie să introduceți acest cod și vi se va permite să vă autentificați. Dacă un criminal cibernetic încearcă să se conecteze la contul tău, nu poate face acest lucru dacă nu are acces la telefonul tău mobil. De asemenea, veți putea observa o încercare de a vă conecta la contul dvs. deoarece veți primi o notificare cu un cod. Nu împărtășiți niciodată acest cod cu alții! Un atacator va încerca să o ia. Dacă ați primit codul, dar nu ați încercat să vă conectați, ștergeți mesajul cu cod și schimbați-vă parola cât mai curând posibil.

Exerciții-4:

Efectuați autentificare în doi factori - verificare pentru a accesa contul de e-mail pe care l-ați creat. Prima dintre aceste procese este parola pe care o utilizați pentru a accesa contul. Celălalt poate fi un cod de verificare (SMS) care trebuie trimis pe telefonul dvs. sau un link de confirmare care trebuie trimis la o altă adresă de e-mail.
Captura de ecran de mai jos arată cum să activați caracteristica de autentificare cu doi factori a contului Gmail.

Finalizați procesul și încercați să vă accesați din nou contul de e-mail.

Pasul-1: Deschideți Contul dvs. Google.
Pasul-2: Faceți clic în secțiunea „Setări”..
Pasul-3: Selectați fila „Securitate” din meniul din partea stângă a paginii care se deschide (1). Apoi activați funcția „Verificare în doi pași” din mijlocul paginii.



1.7. Cele mai bune practici pentru politici de succes de securitate a informațiilor

1. **Clasificarea informațiilor și a datelor:** vă poate face sau distruge programul de securitate. Informațiile și clasificarea slabă a datelor vă pot lăsa sistemele deschise atacurilor. În plus, lipsa unei gestionări ineficiente a resurselor poate genera cheltuieli generale. O politică clară de clasificare ajută organizațiile să preia controlul asupra distribuției activelor lor de securitate.
2. **Operațiuni și administrare IT:** ar trebui să lucreze împreună pentru a îndeplini cerințele de conformitate și securitate. Lipsa de cooperare între departamente poate duce la erori de configurare. Echipele care lucrează împreună pot coordona evaluarea și identificarea riscurilor prin toate departamentele pentru a reduce riscurile.
3. **Plan de răspuns la incidente de securitate:** Ajută la inițierea acțiunilor adecvate de remediere în timpul incidentelor de securitate. O strategie de incident de securitate oferă un ghid, care include răspunsul inițial la amenințare, identificarea priorităților și soluțiile adecvate.
4. **Politica SaaS și cloud —** oferă organizației linii directoare clare privind adoptarea cloud și SaaS, care pot oferi fundația unui ecosistem cloud unificat. Această politică poate ajuta la atenuarea complicațiilor ineficiente și a utilizării slabe a resurselor cloud.
5. **Politici de utilizare acceptabilă (AUP):** Ajută la prevenirea încălcării datelor care apar prin

utilizarea greșită a resurselor companiei. AUP-urile transparente ajută la menținerea întregului personal în conformitate cu utilizarea corectă a resurselor tehnologice ale companiei.

6. **Politica de acces și management al identității (IAM):** subliniază modul în care administratorii IT autorizează sistemele și aplicațiile către angajații potriviți și modul în care angajații creează parole pentru a se conforma cu standardele de securitate. O simplă politică de parole poate reduce riscurile de identitate și acces.
7. **Politica de securitate a datelor:** prezintă cerințele tehnice și standardele minime acceptabile pentru securitatea datelor pentru a se conforma cu legile și reglementările relevante
8. **Reglementări privind confidențialitatea:** reglementările aplicate de guvern, cum ar fi Regulamentul general privind protecția datelor (GDPR), protejează confidențialitatea utilizatorilor finali. Organizațiile care nu protejează confidențialitatea utilizatorilor riscă să-și piardă autoritatea și pot fi amendate.
9. **Politica privind dispozitivele personale și mobile:** prezintă dacă angajaților li se permite să folosească dispozitive personale pentru a accesa infrastructura companiei și cum să reducă riscul de expunere la activele deținute de angajați. În prezent, majoritatea organizațiilor s-au mutat în cloud. Companiile care încurajează angajații să acceseze activele software ale companiei din orice locație riscă să introducă vulnerabilități prin intermediul dispozitivelor personale precum laptopuri și smartphone-uri. Crearea unei politici de securitate adecvată a dispozitivelor personale poate ajuta la prevenirea expunerii la amenințări prin intermediul activelor deținute de angajați.
10. **Politica de acces la distanță:** Prezintă metode acceptabile de conectare de la distanță la rețelele interne
11. **Politica de e-mail/comunicare:** prezintă modul în care angajații pot folosi canalul de comunicare electronică ales de companie, cum ar fi e-mailul, slack sau rețelele sociale
12. **Politica de recuperare în caz de dezastru:** Subliniază contribuția echipelor IT și de securitate cibernetică a organizației într-un plan general de continuitate a afacerii
13. **Planul de continuitate a afacerii (BCP):** Coordonează eforturile în întreaga organizație și este utilizat în cazul unui dezastru pentru a restabili afacerea la starea de funcționare
14. **Politică de răspuns la incident (IR):** O abordare organizată a modului în care organizația va gestiona și remedia un incident
15. **Politica de management al schimbărilor:** Se referă la procesul formal de efectuare a modificărilor IT, dezvoltarea software și securitate

Referințe:

http://bid.ankara.edu.tr/2018/10/02/siber-guvenlik-farkindaligi/
https://purplesec.us/resources/cyber-security-policy-templates/#Email
http://ix-one.com/domainhostingFAQ/article/MS_27805.html
https://www.siberguvenlik.web.tr/index.php/2019/07/22/kimlik-avcilari-sahte-yonetici-uyarilari-ile-office-365-yoneticilerini-hedefliyor/