Material tematic sesiune clasică/ online de coaching/ consiliere profesională/ orientare în carieră, individuală/ personalizată și/ sau de grup

„DreptCompAct- COMpetențe ACTuale pentru studenți la DREPT", Cod proiect: 312957

Competențe transversale în domeniul juridic. Comunicarea (VIII)

Competențe digitale, de siguranță pe internet și securitate cibernetică. (B)

În continuarea analizării competențelor digitale din perspectiva siguranței pe internet și a securității cibernetice este util să sistematizăm componentele principale ale competențelor digitale:

1. **Alfabetizarea informațională și de date** se referă la abilitatea de a găsi, evalua, utiliza și comunica informații (inclusiv date) eficient și etic în era digitală, implicând competențe de căutare, diseminare a surselor, înțelegere a contextului și aplicare responsabilă a datelor, esențiale pentru navigarea în mediul online și luarea deciziilor. Astfel, ca parte a alfabetizării digitale (DigComp), alfabetizarea informațională include căutarea, evaluarea și gestionarea eficientă a informațiilor online, motiv pentru care face parte din setul de competențe europene reglementate, care abordează provocări precum dezinformarea, controlul și dezorientarea în spațiul online. Acest fapt asigură modul în care siguranța pe internet și securitatea cibernetică sunt realizate și prin cea mai recentă strategie de securitate cibernetică a UE, prezentată în 2020, care urmărește consolidarea rezistenței colective împotriva amenințărilor cibernetice.

Componentele cheie ale alfabetizării informaționale și de date sunt: găsirea informației care presupune cunoașterea strategiilor de căutare, identificarea nevoilor de informație; evaluarea informației vizând criticarea surselor, verificarea validității și acurateței datelor; utilizarea informației care implică aplicarea etică și legală a datelor, evitând dezinformarea.

Comunicarea implică prezentarea clară și responsabilă a informațiilor găsite mai ales în contextul alfabetizării de date (Data Literacy); iar înțelegerea, interpretarea și lucrul cu date, respective transformarea lor în cunoștințe, asigurând finalizarea procesului.

Această alfabetizare informațională este esențială pentru navigarea în era digitală, care include o cantitate imensă de informații online care necesită un filtru critic, proces esențial în luarea deciziilor care presupune

filtrarea informațiilor corecte de cele manipulate și a datelor bine interpretate, fundamentale pentru o siguranță reală în mediul online.

2. **Comunicarea și colaborarea** sunt procesele esențiale de schimb de informații și de lucru împreună pentru atingerea unui scop comun, implicând atât aspecte verbale, nonverbale și paraverbale, (tipuri de comunicare pe care le-am analizat în materialele anterioare), dar și utilizarea unor instrumente digitale (Slack, Teams, Zoom, Google Meet) pentru a facilita interacțiunea în echipe, fie fizic, fie la distanță, fiind cruciale în mediul profesional și social pentru succesul proiectelor. Astfel, utilizarea aplicațiilor pentru a comunica (e-mail, chat, video) și a lucra în echipă (Google Docs, platforme online, partajare de documente prin Google Drive, Dropbox, Microsoft 365) sunt deja o realitate în viața noastră cotidiană, devenite indispensabile pentru o eficiență crescută în activitatea profesională, dar și în comunicarea interpersonală utilizând device-urile din ce în ce mai performante.

Eficiența acestora implică o comunicare clară, care previne neînțelegerile și accelerează munca, conștientizând fiecare parte că numai colaborarea stimulează creativitatea prin diverse soluții. Coeziunea implicată în procesul colaborării întărește relațiile în echipă, iar capacitatea de adaptare să permită funcționarea eficientă a echipelor hibride sau la distanță.

3. **Crearea conținutului digital** presupune producerea de informații (text, video, audio, imagini) pentru platforme online, implicând înțelegerea publicului țintă, stabilirea obiectivelor, planificarea, crearea propriu-zisă (cu ajutorul AI sau manual) și publicarea, cu scopul de a genera o conexiune între informația creată și persoana căreia îi este adresată această informație, dar și cu scopul de a adăuga valoare, folosind un mix de povești neadevărate (storytelling), date concrete și elemente vizuale pentru a capta atenția.

Pași cheie în crearea de conținut digital

- Înțelege-ți publicul, audiența prin cercetarea subiectelor de interes, a problemelor pe care aceștia o au, dar mai ales a conținutului consumat zilnic și folosește feedback-ul și sondajele pentru a adapta mesajul.
- Stabilește obiective clare care să vizeze finalitatea cum ar fi: creșterea notorietății, a vânzărilor, a conexiunii cu utilizatorul pentru fidelizarea lui

- Alege formatul și tema, care presupune decizii privind tipul de conținut (blog, video, podcast, infografic, social media), dar și alegerea unei nișe sau teme care să se potrivească publicului și obiectivelor urmărite.
- Planifică și creează care presupune la rându-i o serie de subetape, după cum urmează:
  - ✓ Scrie texte precum articole de blog, postări pe rețele sociale.
  - ✓ Creează imagini folosind instrumente AI (ex: Pippit) sau creează-le manual, adaugă text, ajustează fundalul.
  - ✓ Producția în format video/audio: înregistrează clipuri, podcasturi, folosind un echipament minim.
  - ✓ Folosește numere și date: creează credibilitate cu statistici (cifre exacte, numere impare, limbaj precis).
  - ✓ Incorporează povești credibile (storytelling): Spune povești pentru a crea o conexiune emoțională.
- Publică și distribuie:
  - ✓ Postează pe platformele potrivite (site, social media, aplicații).
  - ✓ Ajustează raportul de aspect (ex: pentru Instagram, TikTok, YouTube).
- Analizează și optimizează:
  - ✓ Urmărește performanța conținutului (like-uri, share-uri, comentarii).
  - ✓ Folosește datele pentru a-ți îmbunătăți strategia.

4. **Siguranță digitală:** presupune protejarea datelor personale, securitatea cibernetică (parole, viruși), sănătatea și bunăstarea online.

”Siguranța pe internet, cunoscută și sub numele de siguranță online, siguranță cibernetică și siguranță electronică (e-safety), se referă la politicile, practicile și procesele care reduc daunele provocate persoanelor prin utilizarea (incorectă) a tehnologiei informației.

Pe măsură ce numărul utilizatorilor de internet continuă să crească la nivel mondial, internetul, guvernele și organizațiile și-au exprimat îngrijorarea cu privire la siguranța copiilor și adolescenților, precum și a persoanelor în vârstă care utilizează internetul. Peste 45% dintre aceștia au anunțat că au suportat un fel de ***hărțuire cibernetică****. Ziua Safer Internet este sărbătorită la nivel mondial în luna februarie pentru a crește nivelul de conștientizare cu privire la siguranța pe internet. În Regatul Unit, campania Get Safe Online a primit sponsorizări din partea agenției guvernamentale Serious Organized Crime Agency (SOCA) și a unor mari companii de internet precum Microsoft și eBay"*[1]

5. **Rezolvarea problemelor:** este abilitatea cognitivă fundamentală de a identifica provocări, a le analiza și a găsi soluții eficiente, implicând mecanisme psihologice precum atenția și memoria, esențială în viața de zi cu zi, de la școală la carieră. Presupune depășirea obstacolelor pentru a atinge un scop și se învață, implicând un proces structurat de gândire pentru a ajunge la o soluție.

Și în această situație există subetape:

- Identificarea problemei, care presupune recunoașterea clară a provocării.
- Analiza problemei incluzând înțelegerea cauzelor, a contextului și a componentelor.
- Generarea soluțiilor care presupune gândirea la posibile căi de acțiune (brainstorming).
- Evaluarea soluțiilor implicând alegerea celei mai potrivite.
- Implementarea soluției care prespune punerea în practică a planului ales.
- Verificarea rezultatelor vizând analiza eficienței soluției alese.

Îmbunătățirea acestei abilități se poate realiza prin:

- Practică constantă realizată prin rezolvarea de puzzle-uri, jocuri de logică, probleme de matematică.
- Gândire critică realizată prin punerea de întrebări, analiza informațiilor din diverse perspective.
- Învățare activă realizată prin căutarea de soluții din surse multiple (cărți, online, mentorat).

[1] https://ro.wikipedia.org/wiki/Siguran%C8%9Ba_pe_internet

- Gândire laterală prin care se încearcă abordări neconvenționale (ca cele studiate de gestaltiști)

Rezolvarea problemelor tehnice de bază și utilizarea inteligentă a tehnologiei este soluția pentru rezolvarea provocărilor.

Gestaltismul (sau psihologia Gestalt) este o școală de psihologie din secolul XX, dezvoltată în Austria și Germania, care susține că percepem lumea ca **întreguri organizate (Gestalten)**, nu ca sume de elemente separate, sloganul central fiind: "**Întregul este mai mult decât suma părților sale**". Fondată de **Max Wertheimer**, Wolfgang Köhler și **Kurt Koffka**, această teorie se opune structuralismului atomist și se concentrează pe organizarea perceptivă (forme, modele), studiind fenomenele psihice holistic, ca structuri integrate. [2]

Principii cheie vizează:

- ✓ **Holismul** care este o atitudine mentală, iar educația holistă este abordarea corelată a tuturor aspectelor pe care le percepem când studiem ceva.
- ✓ **Integritatea și Structuralitatea** ca fenomene psihice cu un caracter global, care nu pot fi reduse la părțile lor simple, ci sunt structuri integrale.
- ✓ **Legea Prägnanz (Simplității)** vizează tendința de a percepe configurațiile cele mai simple și stabile.

Gestaltismul (sau psihologia Gestalt) a revoluționat studiul percepției, gândirii și rezolvării de probleme, influențând și alte domenii, precum critica literară (de exemplu, Camil Petrescu a invocat gestaltismul în crearea dramei Danton), dar inspirând continuatori precum **Kurt Lewin** (teoria câmpului) și cercetări în domeniul conformismului (Asch, Sherif).[3]

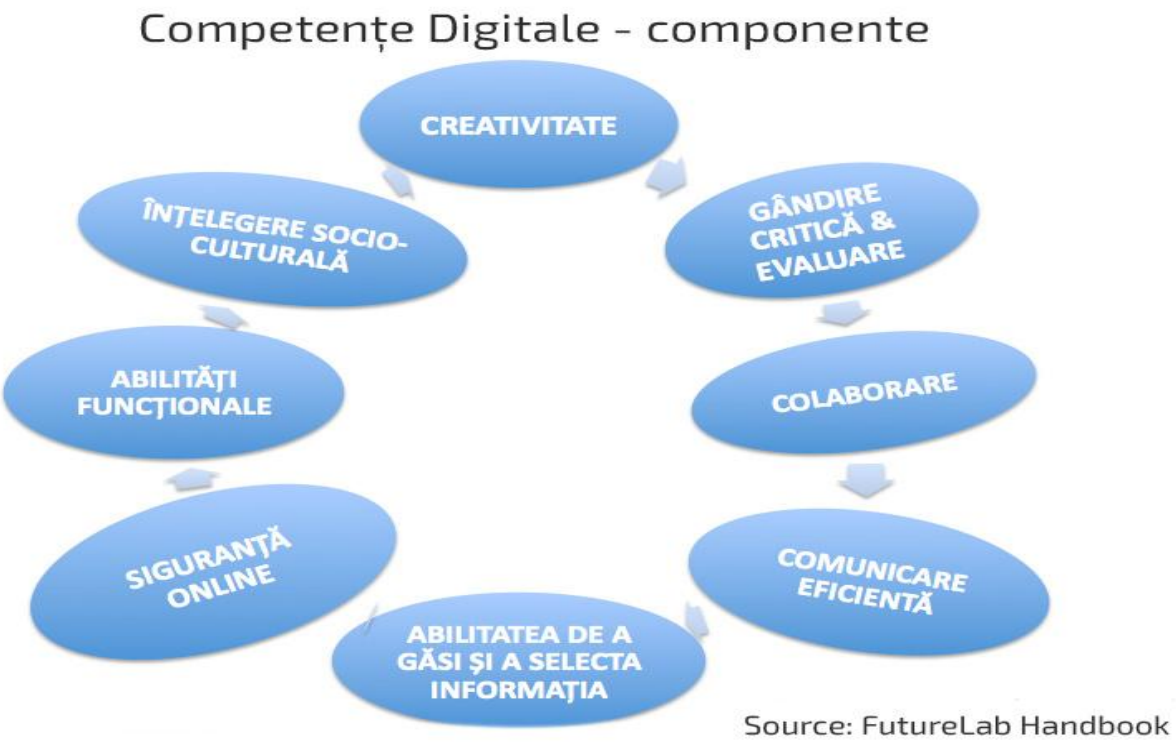
După analiza principalelor componente ale competențelor digitale este necesar să înțelegem rolul lor în societatea modernă, întrucât aceste competențe digitale sunt utile pentru a facilita incluziunea socială, unde acestea sunt esențiale pentru participarea activă în societate, dar pentru creșterea posibilității de a obține un

[2] **Gestaltismul** (sau psihologia Gestalt)
https://www.google.com/search?q=gestalti%C8%99ti%2C&rlz=1C1GCEA_enRO1084RO1084&oq=gestalti%C8%99ti%2C&gs_lcrp=EgZjaHJvbWUyBggAEEUYOTIHCAEQABjvBTIKCAIQABiABBiiBNIBBzgwOWowajeoAgCwAgA&sourceid=chrome&ie=UTF-8

[3] https://ro.wikipedia.org/wiki/Gestaltism

job rapid și de drum lung, întrucât aceste comptențe sunt necesare pentru majoritatea joburilor, de la cele de bază la cele specializate (analiză de date, programare, cloud computing, inclusiv juridic).

Chiar dacă la prima vedere acestea presupun ca și competențe de bază doar utilizarea Microsoft Office (Word, Excel), Google Drive, e-mail, sisteme de operare (Windows, macOS), iar ca și competențe avansate machine learning, cloud computing, dezvoltare web, totuși securitatea cibernetică, care include cunoștințe despre siguranța pe internet și protecția datelor, reprezintă ”cireașa de pe tort!”

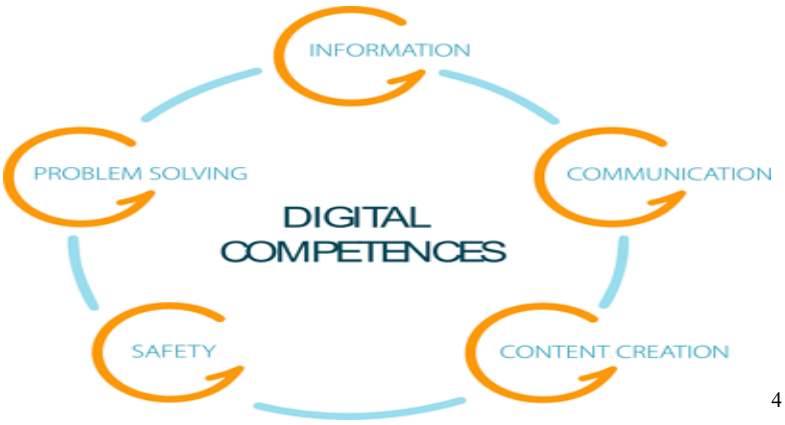


O metodă de modificare a realității în mediul online folosește crearea unei realități false în metaverse, pe rețelele de socializare, etc. Astfel, competențele digitale înseamnă abilitatea de a folosi tehnologia pentru a accesa, gestiona, crea și comunica informații, se referă și la **utilizarea programelor de editare (Photoshop), înțelegerea formatelor (JPG, PNG), optimizarea dimensiunilor pentru web (dimensiune, rezoluție) și gestionarea metadatelor imaginilor**. Practic, este vorba despre a ști cum să lucrezi cu imaginile digital, nu doar să le faci.

Competențele digitale în foto, de exemplu, implică: *manipularea imaginilor***:** Redimensionare, decupare (cropping), ajustarea culorilor (luminozitate, contrast). *cunoașterea formatelor***:** Să știi când să folosești JPG (pentru fotografii, culori complexe) versus PNG (pentru transparență) sau GIF (pentru animații simple); *Optimizarea pentru web*: reducerea dimensiunii fișierului pentru a încărca pagina mai rapid, dar menținând calitatea vizuală; *utilizarea software-ului*: cunoașterea programelor de editare grafică precum Adobe Photoshop, GIMP sau alte instrumente online; managementul metadatelor**:** Ștergerea sau modificarea datelor ascunse (EXIF) din fotografii (informații despre cameră, data, locație).

Aceste competențe sunt esențiale pentru orice job modern, de la marketing, juridic, justiție, economie la educație, permițând crearea de conținut atractiv, comunicare eficientă și rezolvarea problemelor în mediul online.

Folosirea competențelor digitale aduce avantaje importante în selecția candidatului perfect pentru angajatorul vremurilor noastre. Analizând schema de mai jos înțelegem importanța folosirii acestora pentru obținerea de informații din on line, pentru comunicare, pentru rezolvarea problemelor zilnice la job, pentru securitatea informațiilor și continutului creat la job în munca cotidiană, dar și crearea de conținut.



[4]

[4] Sursa: https://www.undelucram.ro/ro/cumlucram/competentele-digitale-in-cv-cresc-sansele-de-angajare-1062

Din perspectiva securității cibernetice, competențele digitale includ ca și componente cheie:

- Protecția Datelor presupune criptarea informațiilor sensibile, backup-uri regulate.
- Securitatea Rețelelor realizată prin Firewalls și sisteme de detectare a intruziunilor (IDS/IPS).
- Managementul identității presupune autentificarea puternică (parole, 2FA).
- Conștientizare și training: Educarea utilizatorilor despre riscuri (phishing, malware).
- Răspunsul la incidente de securitate cibernetică include realizarea de planuri de contingență pentru atacuri cibernetice.

Domeniile de aplicare în materie de siguranță cibernetică sunt la nivel:

- ✓ **Individual** prin protejarea conturilor bancare, a e-mailurilor, a datelor personale pe smartphone-uri și calculatoare.
- ✓ **Organizațional** prin protejarea infrastructurii IT, a proprietății intelectuale și a datelor clienților âm afaceri.
- ✓ **Național/Global** prin securizarea infrastructurilor critice (energie, finanțe, sănătate) și prin combaterea criminalității cibernetice la nivel de stat.

Sintetizând amenințările principale pentru securitatea cibernetică, constatăm că domeniul este încă necunoscut pentru cei mai mulți, fiind greu de procesat pentru unii:

- **Malware:** Viruși, ransomware, spyware.
- **Phishing & Inginerie Socială:** Păcălirea utilizatorilor să dezvăluie informații.
- **Atacuri DDoS:** Suprasolicitarea serviciilor online.
- **Vulnerabilități Software:** Bug-uri nepatch-uite în aplicații sau sisteme de operare.

Sintetizând, din punct de vedere practic, siguranța pe internet și securitatea cibernetică vizează:

- Amenințări cibernetice: care vizează recunoașterea amenințărilor comune precum phishing, malware, atacuri de tip scam și alte forme de atacuri informatice.
- Protecția datelor personale prin implementarea unor măsuri de securitate a datelor, cum ar fi parole sigure, autentificarea cu doi factori și utilizarea software-ului antivirus.

- Confidențialitatea online vizează înțelegerea importanței protejării datelor personale și profesionale, precum și a limitării accesului la informații sensibile.

- Utilizarea în siguranță a platformelor online presupune cunoașterea riscurilor asociate utilizării rețelelor sociale și a altor platforme online și adoptarea unor măsuri de precauție.

Competențele digitale, în contextul codului COR (Clasificarea Ocupațiilor din România), se referă la cunoștințele și abilitățile necesare pentru utilizarea eficientă a tehnologiei digitale în diverse profesii. Codurile COR specifice pot varia în funcție de nivelul de competență și domeniul de activitate, dar un cod frecvent asociat cu competențele digitale este 413201, pentru Operator introducere, validare și prelucrare date.

România are specialiști în zona IT și instituții cheie precum DNSC (Directoratul Național de Securitate Cibernetică)[5], care este structura instituțională care aplică legislația în domeniu, dar și montorizează activitatea în online, fiind structura de contact pentru incidente cibernetice.

"În această nouă eră digitală, securitatea cibernetică trebuie să fie mai mult decât o serie de protocoale tehnice. Aceasta trebuie să fie o parte integrantă a viziunii strategice a fiecărei organizații, iar acest ghid este conceput să ofere instrumentele necesare pentru a naviga acest peisaj complex și pentru a transforma securitatea cibernetică într-un avantaj competitiv."[6]

Concluzii: În esență, securitatea cibernetică urmărește să creeze un spațiu digital mai sigur, protejând atât indivizii, cât și organizațiile de pericolele digitale.

Din perspectiva consilierii în carieră, există oportunități în domeniul securității cibernetice și a unor posibile job-uri pentru specialiști TIC dar și pentru pasionații domeniului, care se pot perfecționa în acest domeniu unde cunoșterea este accelerate…titulatura job-urilor este edificatoare, și confirmată chiar cu poziții specifice în COR, inclusiv prin în cea de formator digital, pentru cei care predau sau formează pe alții în domeniul digital (cod COR 242401). De exemplu, un curs de operator introducere, validare și prelucrare date poate fi echivalent cu codul COR 413201 și atestă competențele digitale de bază pentru acest rol. Unii angajatori pot solicita și cursuri de specializare în securitatea informației (cod COR 121118), conform unei oferte de formare.

[5] https://www.dnsc.ro/
[6] Pdv exprimat de Dan Cîmpean, Directorul Directoratului Național de Securitate Cibernetică, p 16- https://www.dnsc.ro/vezi/document/principii-strategice-de-securitate-cibernetica-pentru-managementul-organizatiei, doc atașat în BD a proiectului, pentru această team.

Titulatura job-urilor representative:

- ✓ Analist de Securitate (IT Security Analyst)- specialistul care protejează sistemele informatice ale unei organizații, monitorizând traficul de rețea, identificând vulnerabilități, prevenind atacurile cibernetice, analizând logurile de securitate, gestionând incidente și implementând politici de securitate, fiind la curent cu noile amenințări pentru a răspunde eficient la ele. (conform definiției AI)

- ✓ Specialist Securitate Cibernetică (Cybersecurity Specialist)- protejează sistemele, rețelele și datele digitale împotriva amenințărilor, monitorizând, detectând, prevenind și răspunzând la atacuri, analizând vulnerabilități și implementând măsuri de securitate precum firewall-uri, criptografie și politici de securitate, având cunoștințe solide de IT, criptografie, analiză de risc și comunicare eficientă pentru a educa și colabora. (conform definiției AI)

- ✓ Administrator de Rețea (Network Administrator) este specialistul IT responsabil cu gestionarea, mentenanța, securitatea și funcționarea optimă a rețelelor de calculatoare (LAN, WAN) ale unei companii, asigurând conectivitatea, alocarea resurselor (IP-uri, permisiuni), monitorizarea, rezolvarea problemelor și protejarea sistemului împotriva atacurilor cibernetice, rolul variind de la configurarea hardware/software la suport tehnic pentru utilizatori, în funcție de mărimea organizației. (conform definiției AI)

- ✓ Analist SOC (Security Operations Center Analyst) monitorizează, analizează și răspunde la incidentele de securitate cibernetică, lucrând în centre de operațiuni de securitate pentru a proteja rețelele companiilor împotriva amenințărilor, investigând alerte, triind incidente și escaladându-le sau rezolvându-le, având nivele diferite de responsabilitate (Tier 1, 2, 3), de la triaj inițial la vânătoare de amenințări avansate. (conform definiției AI)

Top 10 Reguli de siguranță pe Internet - Protejați informațiile personale în mediul online![7]

1. Utilizați parole unice și puternice.
2. Faceți achiziții online doar pe site-uri securizate.
3. Securizați-vă conferințele online.
4. Asigurați-vă de siguranța conexiunii la Internet.

[7] https://stisc.gov.md/sites/default/files/ghiduri/Top%2010%20reguli%20de%20siguran%C8%9B%C4%83%20pe%20Internet_0.pdf

5. Utilizați o conexiune VPN sigură
6. Practicați navigarea în siguranță pe Internet.
7. Activați setările de confidențialitate.
8. Mențineți soluția Antivirus actualizată.
9. Fiți atenți la sursele din care descărcați de pe Internet.
10. Fiți precauți când postați în mediul online!

Pentru că orice material teoretic, oricât de bine ar fi structurat și sintetizat, pentru a fi eficient și a asigura înțelegerea mecanismelor de funcționare, trebuie completat cu exemple practice, după cum urmează:

Aplicații recomandate:

Hacker Warns: Millions Are Being Watched Right Now (Check These Devices ASAP)

21.45 min - 30 iun. 2025- https://www.youtube.com/watch?v=lN061EITkdE

How to Evade Phone Surveillance in Emergencies - Rob Braxman Tech - 22.16 min- 29 ian. 2025

https://www.youtube.com/watch?v=_I9bFIrFhDs

Cybersecurity- https://www.youtube.com/watch?v=Uy60wy20ADE

7 Cybersecurity Tips NOBODY Tells You (but are EASY to do)- 13.48 min