Digital Citizenship

Curs de Confidențialitate și Securitate

Lecturi | Exerciții | Studii de caz | Chestionare

Erasmus+

ATHENS LIFELONG LEARNING INSTITUTE

TEAM 4 excellence

SEAL CYPRUS

Parteneriat strategic pentru dezvoltarea de resurse educaționale deschise pentru predarea cetățeniei digitale

2019-3-RO01-KA205-078053

DIGCIT

D15 - Curs de cetățenie digitală "Confidențialitate și securitate"

Revizuire: v.1.1

Rezultat intelectual	IO2 - Materiale educaționale pentru cetățenia digitală
Activitate	Dezvoltarea curriculumului de curs
Responsabil	Arbeitskreis Ostviertel e. V, Germania
Termen limită	15 martie 2021
Autori	Jan LEYE
Abstract	Cursul "Confidențialitate și securitate" se referă la riscurile și beneficiile pentru informațiile și datele personale ale cetățenilor digitali. În timp ce beneficiile sociale ale exercitării drepturilor și obligațiilor, ale hobby-urilor și ale interacțiunilor sociale online sunt imense, continuă să apară tot mai multe amenințări la adresa vieții private a fiecărui cetățean. Acest curs predă cele mai importante aspecte ale siguranței și importanța protejării vieții private a fiecăruia.
Cuvinte-cheie	Curs model; cetățenie digitală; plan de curs; confidențialitate; securitate; medii digitale; rețele sociale; riscuri de securitate pe internet; hardware; software; educație; reflecție; gândire reflexivă

Recunoaștere

Această lucrare a beneficiat de finanțare din partea Comisiei Europene în cadrul Acordului de Grant 2019-3-RO01-KA205-078053, proiectul de parteneriat strategic ERASMUS+ "Parteneriat strategic pentru dezvoltarea resurselor educaționale deschise pentru predarea cetățeniei digitale - DIGCIT".

Disclaimer

Sprijinul acordat de Comisia Europeană pentru realizarea acestei publicații nu constituie o aprobare a conținutului, care reflectă doar opiniile autorilor, iar Comisia nu poate fi considerată responsabilă pentru orice utilizare care ar putea fi dată informațiilor conținute în această publicație.

Drepturi de autor

Cuprins

Introducere

Confidențialitatea și securitatea sunt termeni vechi, dar importanța lor a crescut în ultimii ani. Modulul "Confidențialitate și securitate" explică interpretarea modernă a confidențialității ca drept al omului într-o eră digitalizată.

Manualul educațional privind cetățenia digitală al Consiliului Europei definește viața privată ca fiind un drept care "*se referă în principal la protecția personală a informațiilor online proprii și a celorlalți, în timp ce securitatea se referă mai mult la conștientizarea propriilor acțiuni și comportamente online*".

Confidențialitatea și securitatea depind una de cealaltă, cu atât mai mult într-un mediu digital. Confruntându-se cu amenințări legate de hardware, software și de utilizatorul însuși, protejarea propriei vieți private este o provocare și o responsabilitate continuă pentru orice cetățean digital.

Acest modul are ca scop creșterea gradului de conștientizare cu privire la importanța vieții private în ceea ce privește o viață împlinită și la măsurile necesare care trebuie luate pentru a proteja această viață privată. Acesta va prezenta cunoștințe și sfaturi practice cu privire la elementele fundamentale ale securității moderne în fața riscurilor moderne. Modulele vor acoperi următoarele subiecte și altele:

- Ce este confidențialitatea?
- Ce este securitatea?
- Ce sunt mediile digitale?
- Cum ne afectează viața privată?
- Cum funcționează un dispozitiv digital?
- Cum să ne comportăm în mod sigur și responsabil

1. Modulul 1 - Introducere în confidențialitate

Sursa: Unsplash

Prezentare generală a cursului

Rezumat: Acest modul acoperă elementele de bază ale confidențialității, definiția și rolul acesteia în mediul digital actual. De asemenea, prezintă importanța confidențialității ca drept al omului.

Structură:

- Prezentare generală a cursului
- Definiția confidențialității
- Confidențialitatea digitală
- Importanța vieții private
- Studiu de caz
- Lecturi suplimentare
- Exercițiu
- Feedback
- E-Quiz

Obiective de învățare:

- Înțelegeți definiția confidențialității.
- Recunoașteți importanța vieții private.
- Explicați importanța vieții private.

Definiția vieții private

Nu există o definiție recunoscută la nivel mondial a vieții private, deoarece termenul poate avea înțelesuri diferite în funcție de cultură, istorie sau experiență personală. Pe parcursul acestui curs, vom folosi o definiție care ar trebui să se aplice în mod suficient pentru majoritatea democrațiilor occidentale:

Intimitatea este capacitatea cuiva de a nu fi însoțit și observat sau, pe scurt, este dreptul de a fi lăsat în pace. A fi în intimitate înseamnă a păstra secrete informațiile și chestiunile personale și a împărtăși informațiile și chestiunile personale numai după propria voință. Protecția vieții private înseamnă, prin urmare, libertatea de a nu fi supus unei intruziuni neautorizate în spațiul personal, în informațiile și chestiunile personale.

Confuzia provine adesea din faptul că termenii "confidențialitate" și "protecția datelor" sunt utilizați ca sinonime. Ambii sunt legați unul de celălalt, dar, în timp ce viața privată se referă direct la spațiul sau sfera personală a unui individ, protecția datelor se referă în mod specific la protecția "oricărei informații referitoare la o persoană fizică (vie) identificată sau identificabilă"[1]. Viața privată acoperă toate aspectele sferei personale, cum ar fi protecția fizică a locuinței dumneavoastră. De exemplu, dacă sunteți victima unui contact fizic nedorit, dreptul dumneavoastră la intimitate a fost lezat, dar nu și dreptul la protecția datelor.

Dreptul la viață privată este un drept al omului, astfel cum este prevăzut la articolul 12 din Declarația Universală a Drepturilor Omului din 1948 (DUDO):

> *"Nimeni nu va fi supus unor ingerințe arbitrare în viața sa privată, în familie, în domiciliu sau în corespondență, nici unor atacuri la adresa onoarei și reputației sale. Orice persoană are dreptul la protecția legii împotriva unor astfel de ingerințe sau atacuri."*[2]

Sursa: internet

[1] https://edps.europa.eu/data-protection_en
[2] https://www.un.org/en/about-us/universal-declaration-of-human-rights

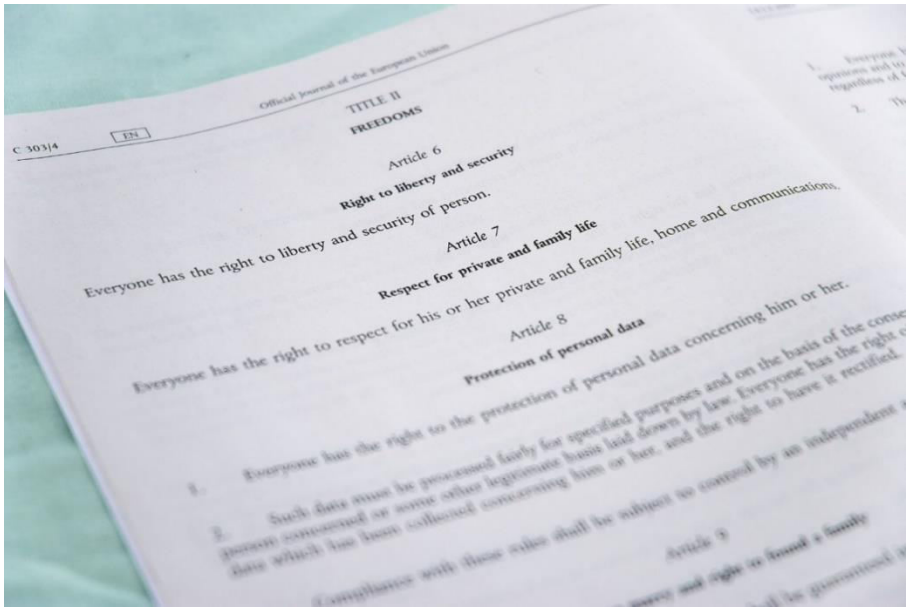
Protecția vieții private a fost recunoscută în mod special de Consiliul Europei atunci când Convenția europeană a drepturilor omului (CEDO) a fost semnată în 1950 și a intrat în vigoare în septembrie 1953. Articolul 8 din CEDO se intitulează "Dreptul la respectarea vieții private și de familie" și prevede următoarele:

> *"1. Orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului său și a corespondenței sale.*
>
> *2. Autoritățile publice nu pot interveni în exercitarea acestui drept decât în măsura în care acest lucru este prevăzut de lege și este necesar, într-o societate democratică, în interesul securității naționale, al siguranței publice sau al bunăstării economice a țării, pentru prevenirea dezordinii publice sau a criminalității, pentru protecția sănătății sau a moralei sau pentru protecția drepturilor și libertăților altora."*[3]

În plus, Uniunea Europeană recunoaște dreptul la viață privată în articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene (CFR), care a fost elaborată în 2000 și a intrat în vigoare în decembrie 2009:

> *"Articolul 7*
>
> *Respectarea vieții private și de familie*
>
> *Orice persoană are dreptul la respectarea vieții sale private și de familie, a domiciliului și a comunicațiilor.*
>
> *Articolul 8*
>
> *Protecția datelor cu caracter personal*
>
> *1. Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.*
> *2. Aceste date trebuie să fie prelucrate în mod echitabil în scopuri determinate și pe baza consimțământului persoanei în cauză sau a unui alt temei legitim prevăzut de lege. 3. Orice persoană are dreptul de a avea acces la datele care au fost colectate în ceea ce o privește și dreptul de a le rectifica.*
> *3. Respectarea acestor norme face obiectul unui control din partea unei autorități independente."*[4]

[3] https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=DE



Sursa: Wikimedia

Confidențialitatea digitală

Era digitală a adus noi oportunități și provocări deopotrivă. Atunci când vorbim despre confidențialitate într-un mediu digital, folosim de obicei termenul "confidențialitate digitală". Confidențialitatea digitală include dreptul la viață privată și toate definițiile sale aplicabile din lumea analogică, precum și protecția datelor.

Confidențialitatea digitală poate fi un termen confuz, deoarece confidențialitatea, ca termen juridic, acoperă deja toate domeniile de aplicare: Nu contează dacă viața privată este pusă în pericol în lumea reală sau în mediul digital, deoarece protecția acesteia se aplică independent de tehnologie, loc sau timp. Atunci când vorbim despre viața privată "digitală" sau "electronică", dorim, în principiu, să punem accentul pe riscurile și pericolele specifice la adresa vieții private care își au originea în noile tehnologii, cum ar fi internetul, rețelele sociale sau noile dispozitive.

Uniunea Europeană a stabilit două seturi principale de norme care protejează în mod specific drepturile de protecție a vieții private și a datelor în mediile digitale sau electronice: Directiva privind viața privată și comunicațiile electronice (ePrivacy Directive)[5] (titlul complet: Directiva privind confidențialitatea și comunicațiile electronice) și Regulamentul general privind protecția datelor[6] (GDPR). Ambele încearcă să abordeze preocupările legate de protecția vieții private și a datelor legate de internet, de exemplu prin solicitarea unei mai mari transparențe în contextul marketingului sau al urmăririi datelor cu caracter personal.

Importanța confidențialității

Dreptul la viață privată este o condiție prealabilă pentru libera dezvoltare a personalității, cum se prevede la articolul 22 din Declarația Universală a Drepturilor Omului:

> *"Orice persoană, în calitate de membru al societății, are dreptul la securitate socială și are dreptul la realizarea, prin efort național și cooperare internațională și în conformitate cu*

[5] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
[6] https://eur-lex.europa.eu/eli/reg/2016/679/oj

> *organizarea și resursele fiecărui stat, a drepturilor economice, sociale și culturale indispensabile pentru demnitatea sa și pentru libera dezvoltare a personalității sale."*[7]

Unele state membre ale Uniunii Europene, cum ar fi Germania sau Țările de Jos, recunosc în mod specific dreptul la personalitate în constituțiile lor respective, de exemplu articolul 2 din constituția germană, care prevede:

> *"(1) Orice persoană are dreptul la libera dezvoltare a personalității sale, în măsura în care nu încalcă drepturile altora și nu încalcă ordinea constituțională sau legea morală."*[8]

Alte state, cum ar fi Franța, au ales mijloace diferite în jurisdicția lor pentru a proteja dezvoltarea personalității.

Cu toate acestea, toate împărtășesc o concepție generală cu privire la importanța personalității, la protecția acesteia și la legătura intrinsecă a acesteia cu viața privată. Fără protecția vieții private, o ființă umană nu se poate dezvolta și trăi liber.

Studiu de caz – Proiectarea confidențialității

Confidențialitatea prin proiectare: Colectarea datelor într-un mod responsabil din punct de vedere social, fără efecte secundare asupra vieții private

În acest videoclip de la Săptămâna confidențialității 2017 de la Viena, Konark Modi explică "efectele secundare" periculoase ale actualului standard industrial aplicat de giganții din domeniul tehnologiei, care colectează cât mai multe date posibil.

Sursa: https://media.ccc.de/v/pw17-158-privacy_by_design#t=74

Modi demonstrează că viața privată poate fi respectată în timpul proiectării serviciilor online și prezintă o versiune alternativă, care respectă viața privată, a "Google Analytics".

[7] https://www.un.org/en/about-us/universal-declaration-of-human-rights
[8] https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0023

Auto-reflecție: Ce este un efect secundar în contextul colectării de date?

Exercițiul 1: Întâlnire privată în World Café

Obiective:

- Înțelegerea obiceiurilor tale de a posta date personale.
- Recunoașterea potențialelor riscuri și pericole pentru viața privată.

Durata: 30 minute

Materiale: pix și hârtie

Metode: plen, lucru în echipă

Descrierea exercițiului: Elevii sunt împărțiți în patru grupuri. Fiecare grup este repartizat la o masă cu markere permanente/hârtie sau într-o cameră de întâlnire online cu o tablă albă virtuală. Fiecărei mese/săli i se atribuie una dintre următoarele probleme de confidențialitate: (1) Furtul de identitate. (2) Dreptul de a fi uitat. (3) Personalitatea. (4) Spyware. Fiecare grup are la dispoziție 5 minute pentru a reflecta asupra acestor subiecte (Ce înseamnă ele? Care este legătura lor cu viața privată? Cunoaștem exemple? Sunt periculoase sau benefice pentru mine?) și își notează ideile pe hârtie/ tablă virtuală. După 5 minute, grupurile încep să se rotească. Cafeneaua se închide după ce fiecare grup a discutat fiecare subiect. Fiecare grup stabilește un vorbitor care prezintă rezultatele respective pentru grupul său.

Sarcini:

- Împărțiți-vă în grupuri.
- Discutați fiecare subiect timp de cinci minute.
- Împărtășiți rezultatele cu clasa (vă rugăm să rețineți că nu trebuie să împărtășiți nicio informație care v-ar putea face să vă simțiți inconfortabil).

Concluzii: Formatorul ar trebui să sublinieze importanța universală a vieții private și faptul că aceasta afectează multe părți ale vieții noastre și bunăstarea noastră.

Lecții învățate: Confidențialitatea este un subiect complex și necesită o reflecție activă.

Lecturi suplimentare

Ziua Protecției Datelor (în fiecare an, la 28 ianuarie): "În acest an, 28 ianuarie este o zi foarte specială, nu numai pentru Consiliul Europei, ci pentru întreaga comunitate globală de protecție a datelor și, mai presus de toate, pentru fiecare individ protejat de acest drept esențial." https://www.coe.int/en/web/data-protection/data-protection-day

Chestionar online

Chestionar online			
Titlul cursului:	Confidențialitate și securitate		
Titlul modulului:	Introducere în confidențialitate		
Adevărat sau Fals	Indicați dacă următoarele afirmații sunt Adevărate (A) sau False (F)		
Afirmații		A	F
1	Conform Organizației Națiunilor Unite, viața privată este un drept al omului		
2	Confidențialitatea este dreptul de a păstra secrete toate informațiile despre tine, chiar și pentru guvern		
3	Uniunea Europeană nu recunoaște în mod specific dreptul la viață privată ca fiind un drept		
4	"Viața privată" și "protecția datelor" sunt mai mult sau mai puțin sinonime		
5	GDPR este acronimul de la "Directiva generală privind dreptul la viață privată"		
6	Unele jurisdicții recunosc viața privată ca o condiție prealabilă pentru dezvoltarea liberă a personalității		
7	Respectarea legilor privind viața privată și proiectarea de software modern se exclud reciproc		
8	Protecția datelor se referă la protecția oricărei informații referitoare la o persoană fizică (vie) identificată sau identificabilă		

2. Modulul 2 - Introducere în securitate

Prezentare generală a cursului

Rezumat: Acest modul acoperă elementele fundamentale ale securității. Acesta explică definiția de bază a acesteia, relația sa cu confidențialitatea și prezintă importanța securității în mediile digitale.

Structură:

- Prezentare generală a cursului
- Definiția securității
- Importanța securității
- Studiu de caz
- Lecturi suplimentare
- Exercițiu
- Feedback
- Chestionar online

Obiective de învățare:

- Înțelegeți definiția securității.
- Recunoașteți importanța securității.
- Explică importanța securității în contextul confidențialității.

Definiția securității

Securitatea înseamnă libertatea de a fi ferit de pericole cauzate de amenințări externe sau de teama sau anxietatea legată de rău sau pericol. Drepturile omului se bazează parțial pe principiul că ființele umane tânjesc după o stare de siguranță.

În contextul cetățeniei digitale, securitatea înseamnă libertatea față de pericolul care poate fi cauzat de propriile acțiuni, inacțiuni și comportamente într-un mediu digital sau online. Ea este profund legată de confidențialitate, deoarece fără aplicarea unor măsuri de securitate adecvate, confidențialitatea este pusă în pericol. Consiliul Europei precizează pe site-ul său web:

> *"Pentru a deveni un cetățean digital, se așteaptă ca o persoană să dezvolte o abordare critică și etică pentru a naviga în mediul digital cu încredere și claritate și să acționeze în consecință."*[9]

Prin urmare, pentru a fi în siguranță, cetățeanul digital trebuie să fie conștient de potențialele riscuri și amenințări care îi pot face rău nu numai lui, ci și altor persoane. Pentru a înțelege mai bine potențialul prejudiciu cauzat de o lipsă de securitate, putem examina o listă de date personale exemplificativă:

- Numele și prenumele
- Adresa de domiciliu
- Numărul de telefon
- Adresa de e-mail
- Date de geolocalizare
- Adrese IP
- ID-uri de cookie

Scurgerea oricăreia dintre aceste date poate duce la prejudicii minore și/sau grave.

Importanța securității

Mediile digitale prezintă pericole noi și adesea destul de invizibile pentru indivizi. Pentru a explica importanța securității digitale, ne putem uita la pandemia Corona: Cu cât mai multe persoane sunt infectate cu virusul, cu atât mai mari sunt șansele ca și alte persoane să fie infectate. Imaginați-vă că dispozitivul dvs. este compromis de un malware. În funcție de tipul de malware, acesta ar putea reprezenta un pericol nu numai pentru intimitatea dumneavoastră, ci și pentru intimitatea altor persoane și ar putea afecta negativ viața acestora.

Securitatea nu trebuie privită ca un privilegiu, o opțiune sau o ofertă voluntară. Dimpotrivă, un cetățean digital responsabil trebuie să înțeleagă securitatea ca pe o responsabilitate civică pentru sine și pentru ceilalți cetățeni. Respectarea principiilor de bază ale siguranței digitale (a se vedea modulul 4) reprezintă o contribuție activă la un mediu digital mai echitabil și mai pozitiv.

Securitatea nu înseamnă niciodată doar să te protejezi pe tine însuți. Este vorba despre protejarea noastră a tuturor, inclusiv a prietenilor și a familiilor dumneavoastră.

[9] https://www.coe.int/en/web/digital-citizenship-education/privacy-and-security

Studiu de caz - STOP.THINK.CONNECT.

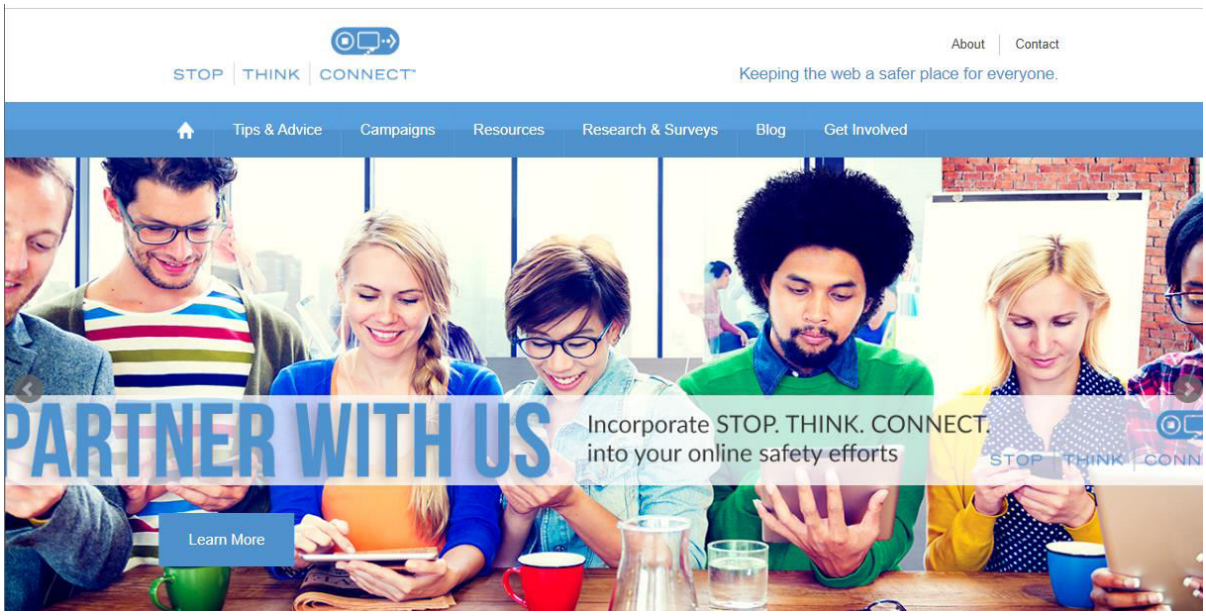
STOP.THINK.CONNECT. este prima campanie globală de sensibilizare a publicului dezvoltată pentru a-i ajuta pe toți utilizatorii de internet să își păstreze informațiile personale, comunicațiile și tranzacțiile online mai sigure.

Organizația americană "National Cybersecurity Alliance" și "APWG Public Education Initiative" organizează o campanie globală de conștientizare a siguranței online numită "STOP. THINK. CONNECT.". Aceasta recomandă trei principii de bază în ceea ce privește securitatea digitală:

"STOP: Înainte de a utiliza internetul, acordați-vă timp pentru a înțelege riscurile și învățați cum să identificați eventualele probleme.

THINK: Luați-vă un moment pentru a fi siguri că drumul pe care îl aveți în față este clar. Fiți atenți la semnele de avertizare și gândiți-vă la modul în care acțiunile dvs. online ar putea afecta siguranța dvs. sau a familiei dvs.

CONNECT: Bucurați-vă de internet cu mai multă încredere, știind că ați luat măsurile corecte pentru a vă proteja pe dumneavoastră și calculatorul (și alte dispozitive)."



https://stopthinkconnect.cc/

Peste 800 de întreprinderi comerciale, instituții de învățământ, agenții guvernamentale și ONG-uri au adoptat STOP. THINK. CONNECT. ™. Treisprezece ministere guvernamentale naționale și ONG-uri de anvergură națională au desfășurat campanii naționale.

Citiți fișa informativă https://education.apwg.org/safety-messaging-convention/ și reflectați asupra modului în care organizațiile se pot alătura campaniei.

Exercițiul 2: Trasarea liniei

Obiective:

- Înțelegeți diferența dintre datele cu caracter personal și datele publice.
- Recunoașteți propriile nevoi în ceea ce privește protecția datelor.

- Justificați utilizarea datelor dumneavoastră personale.

Durata: 20 minute

Materiale: pix și hârtie

Metode: plen, aplicație creativă, scriere

Descrierea exercițiului: Gândiți-vă la următoarele exemple de date cu caracter personal: Numele dumneavoastră, vârsta, mărimea pantofilor, greutatea, hobby-urile, salariul, marca de șampon, numele primului animal de companie, culoarea lenjeriei de corp, nota de la ultimul examen/revizuirea locului de muncă, salariul dumneavoastră, ora la care ieșiți din casă. Atribuiți fiecare dintre aceste date uneia dintre următoarele patru categorii: (1) Aceste date sunt private; nu le voi împărtăși. (2) Aceste date pot fi împărtășite doar cu prietenii mei. (3) Aceste date pot fi făcute publice. (4) Nu știu unde să atribui aceste date.

Sarcini:

- Creați un tabel pe hârtie, fiecare rând reprezentând una dintre cele patru categorii.
- Atribuiți toate exemplele la una dintre cele patru categorii în termen de 5 minute.
- Împărtășiți rezultatele cu clasa (vă rugăm să rețineți că nu trebuie să împărtășiți nicio informație care v-ar putea face să vă simțiți inconfortabil).

Concluzii: Formatorul ar trebui să sublinieze motivele pentru care anumite exemple de date cu caracter personal sunt de preferat să nu fie împărtășite cu publicul de către majoritatea participanților. Plenul ar trebui să tragă concluzii și motive comune în legătură cu datele cu caracter personal și viața privată.

Lecții învățate: Datele cu caracter personal trebuie protejate. Ar trebui să nu mă grăbesc și să mă gândesc înainte de a împărtăși date cu caracter personal.

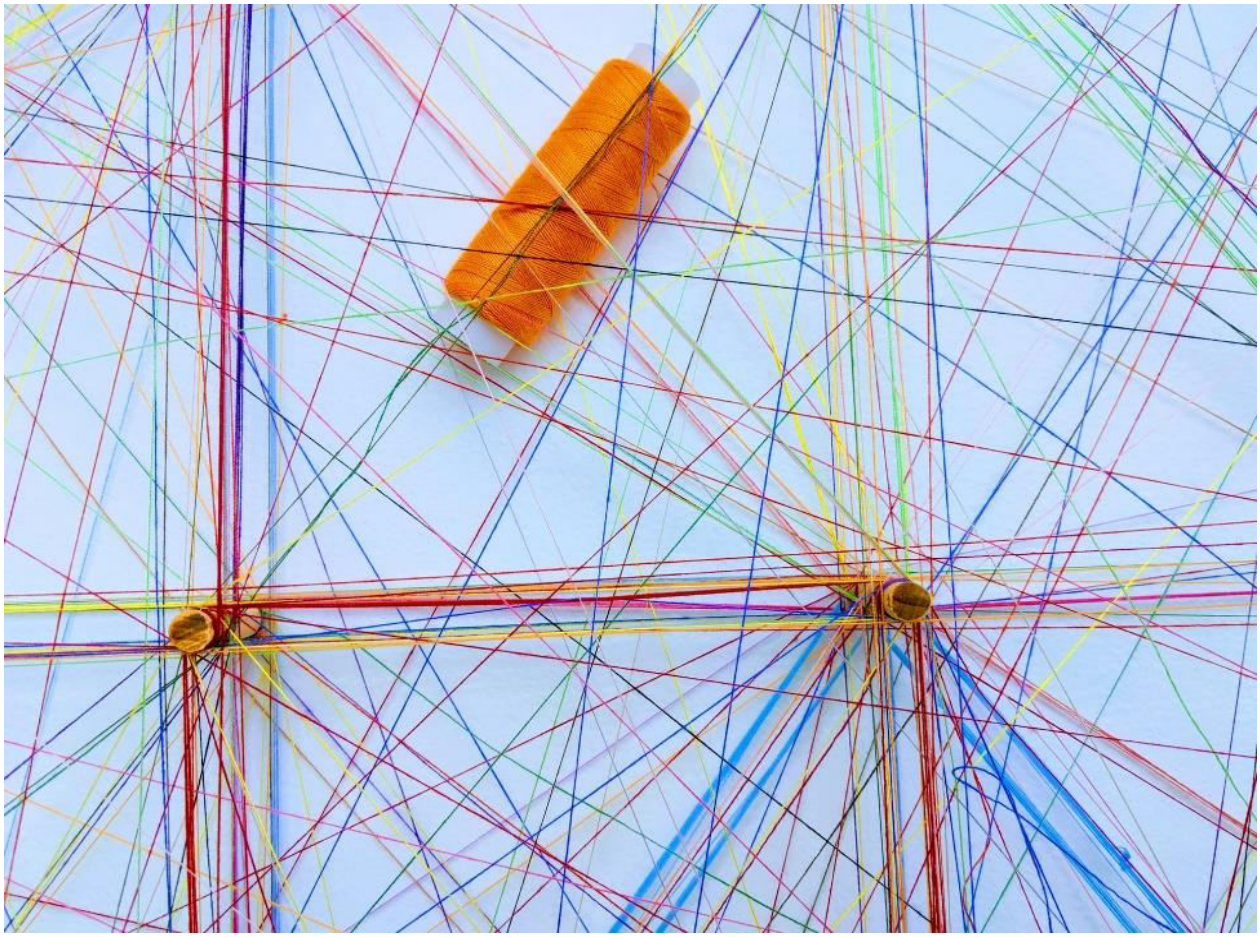
Lecturi suplimentare

- **Scurgerea de date de la Facebook:** O discuție pe Twitter despre consecințele și subestimarea scurgerii de date de la Facebook, care a afectat aproximativ 533 de milioane de utilizatori Facebook din întreaga lume.
  https://twitter.com/UnderTheBreach/status/1349671294808285184

Chestionar online

Chestionar online			
Titlul cursului:	Confidențialitate și securitate		
Titlul modulului:	Introducere în securitate		
Adevărat sau fals	Indicați dacă următoarele afirmații sunt Adevărate (A) sau False (F)		
Afirmații		A	F
1	Lipsa de securitate vă poate pune în pericol viața privată		
2	Adresa IP a smartphone-ului dvs. face parte din datele dvs. personale		
3	Securitatea se referă la libertatea dumneavoastră de a avea acces la sferele private ale altor persoane		
4	Dacă aplicați o conștientizare adecvată a securității, îi protejați și pe ceilalți oameni		
5	Securitatea este o responsabilitate civică pentru cetățenii digitali		
6	Un comportament critic și etic într-un mediu digital face parte din securitate		

3. Modulul 3 - Confidențialitatea în mediul digital



Prezentare generală a cursului

Rezumat: Acest modul explică conceptul din spatele mediilor digitale. Se concentrează pe mediile sociale și de comunicare și pe riscurile pe care acestea le prezintă pentru viața privată a utilizatorului. În ceea ce privește confidențialitatea, se reflectă în mod critic asupra importanței și problemelor celor mai mari site-uri de rețele sociale.

Structură:

- Prezentare generală a cursului
- Premisele mediilor digitale
- Riscurile rețelelor sociale și ale mesagerilor într-un mediu digital
- Studiu de caz
- Lecturi suplimentare
- Exercițiu
- Feedback
- Chestionar online

Obiective de învățare:

- Înțelegeți definiția mediilor digitale.
- Recunoașteți influența rețelelor de socializare.

- Identificați amenințările multistratificate la adresa vieții private în mediile digitale.

Premisa mediilor digitale

În prezent, definiția tehnică a unui mediu digital se referă de obicei la sistemele digitale și electronice care sunt integrate, conectate și accesibile prin intermediul world wide web sau al altor accese online. Cu toate acestea, pentru cetățenii digitali, mediile digitale sunt adesea definite de contexte și sunt experimentate ca spații online conectate, activate de tehnologie și dispozitive digitale. [10]

Mediile digitale pot fi utilizate pentru a sensibiliza publicul cu privire la drepturile omului sau la probleme care privesc societatea civilă, prin conectarea reciprocă și exprimarea opiniei. Cetățenii digitali accesează mediile digitale cu ajutorul dispozitivelor digitale, cum ar fi smartphone-urile sau laptopurile. Aceștia au acces la diferite elemente ale mediilor digitale care îndeplinesc diferite funcții.

Cu toate acestea, o participare sigură a tuturor cetățenilor digitali la mediile sociale și de comunicare este legată de un grad necesar de educație mediatică.

Pentru a experimenta cetățenia digitală, serviciile de comunicare și sociale din cadrul mediilor digitale sunt cele mai importante, de exemplu, site-urile web, platformele de rețele sociale sau mesagerii. Organizația Națiunilor Unite pentru Educație, Știință și Cultură afirmă în raportul său privind "Cultura în mediul digital":

> *"Aceasta include capacitatea de a analiza în mod critic varietatea de informații la care suntem supuși (și anume, conținutul audio-vizual), de a ne forma opinii autonome, de a ne implica activ în problemele comunității și de a stăpâni noi forme de interacțiune socială."*[11]

Deoarece mediile digitale tind să își schimbe rapid interfețele, accesele, funcțiile și comportamentele, este important să le includem în mod activ în procesele educaționale formale și non-formale pentru persoanele de toate vârstele.

Riscurile rețelelor sociale și de mesagerie într-un mediu digital

Mediul digital prezintă riscuri pentru cetățenii digitali de toate vârstele și, odată cu apariția rețelelor de socializare și a mesageriei instantanee, problemele legate de confidențialitate par să apară mai des ca niciodată.

> *"În 2020, peste 3,6 miliarde de persoane foloseau social media la nivel mondial, un număr care se estimează că va crește la aproape 4,41 miliarde în 2025."*[12]

În cazul în care aceste servicii sunt utilizate într-un mod nechibzuit, utilizatorul poate suferi consecințe sociale, financiare, emoționale, profesionale sau juridice. Următoarea listă prezintă cele mai relevante preocupări legate de confidențialitate în legătură cu site-urile rețelelor de socializare:

- **Pierderea suveranității datelor:** Pierderea capacității dumneavoastră de a controla prelucrarea datelor dumneavoastră cu caracter personal

[10] "Handbook of Research on Educational Design and Cloud Computing in Modern Classroom Settings", p. 79, 2017, Yannis Kotsanis (Doukas School, Greece), ISBN13: 9781522530534
[11] https://en.unesco.org/creativity/sites/creativity/files/dce-policyresearch-book2-en-web.pdf
[12] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

- **Lipsa de transparență:** Lipsa capacității dumneavoastră de a fi informat cu privire la prelucrarea datelor dumneavoastră cu caracter personal
- **Percepția greșită a beneficiilor:** O situație în care beneficiul perceput al dezvăluirii unor fragmente din datele dumneavoastră personale pare a fi mai mare decât riscul perceput al împărtășirii informațiilor pe o platformă online
- **Comportament relaxat:** Subestimarea consecințelor pe care le-ar putea provoca partajarea datelor personale
- **Permanența informațiilor:** Faptul că este probabil ca informațiile dvs. personale să fie permanent disponibile online (legat de "dreptul de a fi uitat" în Uniunea Europeană)
- **Profilarea:** Amenințarea creării unui profil despre dumneavoastră prin utilizarea informațiilor personale disponibile și/sau a meta-datelor, de exemplu în cadrul publicității direcționate

În zilele noastre, una dintre cele mai mari amenințări este comportamentul relaxat pe site-urile de rețele sociale precum Facebook, Twitter, Instagram sau TikTok. Fiecare dintre aceste site-uri oferă un grad variabil de confidențialitate. Site-uri precum Facebook își forțează adesea utilizatorii să își folosească numele real, în caz contrar conturile lor ar putea fi închise, în timp ce alte site-uri de rețele sociale încurajează utilizarea pseudonimelor. Cu toate acestea, fiecare site de socializare poate oferi suficiente informații personale pentru a vă face pe dumneavoastră sau pe alții identificabili, de exemplu, prin utilizarea aceleiași imagini de profil în diferite rețele, prin postarea de fotografii cu medii ușor de recunoscut sau prin partajarea informațiilor privind locația cu profilul dumneavoastră.

În 2020, retailerul american de internet prin satelit "Viasat Savings" a realizat un sondaj în rândul a 1 000 de cetățeni americani adulți, întrebând câte persoane de pe site-urile de rețele sociale își păstrau profilurile private:

> *"Se pare că este împărțită în mod egal: aproape 50% dintre persoanele pe care le-am intervievat își păstrează conturile în modul privat, în timp ce cealaltă jumătate a ales să fie publice. Potrivit lui Kyrsten Holland, expert în internet la Viasatsavings.com, "Tinerii și bătrânii au un lucru în comun: persoanele cu vârste cuprinse între 18 și 24 de ani și cele de peste 54 de ani sunt grupurile de vârstă cele mai predispuse să își facă publice conturile de social media."*[13]

Dar chiar și atunci când vă păstrați profilul privat, cele mai importante rețele de socializare sunt deținute de companii private cu intenția de a obține profituri. Prin urmare, acestea își rezervă, de obicei, dreptul de a utiliza, combina (deosebit de valoros în cazul în care dețin mai multe servicii, de exemplu Facebook, Instagram și WhatsApp) și/sau vinde informațiile dumneavoastră personale - pe care le-ați furnizat de bunăvoie - altor companii care își pot orienta publicitatea (inclusiv campaniile politice) în funcție de interesele dumneavoastră.

În același timp, experiența ne învață că nicio companie nu poate fi de încredere că vă poate păstra în permanență datele dvs. private stocate în siguranță. În trecut, toate site-urile importante de rețele sociale au căzut victime ale scurgerilor de date:

- **Instagram, TikTok, YouTube:** "Echipa de cercetare în domeniul securității de la Comparitech a dezvăluit astăzi modul în care o bază de date nesecurizată a lăsat expuse online aproape

[13] https://www.viasatsavings.com/news/blog/are-more-people-public-or-private-on-social-media/

235 de milioane de profiluri de utilizatori Instagram, TikTok și YouTube, în ceea ce poate fi descris doar ca o scurgere masivă de date." [14]

- **Facebook: "**Echipa UpGuard Cyber Risk poate raporta acum că alte două seturi de date ale aplicațiilor Facebook dezvoltate de terți au fost găsite expuse la internetul public. Unul dintre ele, provenit de la compania media Cultura Colectiva din Mexic, cântărește 146 de gigabytes și conține peste 540 de milioane de înregistrări care detaliază comentarii, like-uri, reacții, nume de conturi, ID-uri FB și multe altele."[15]
- **Twitter:** "Un sfert de milion de utilizatori Twitter au avut conturile piratate, în cea mai recentă dintr-o serie de breșe de securitate de profil înalt la firmele de internet. Este posibil ca hackerii anonimi să fi reușit să obțină acces la aproximativ 250.000 de conturi de pe rețeaua de socializare, inclusiv nume de utilizator, adrese de e-mail și parole."[16]

Următoarele sfaturi ar trebui urmate atunci când se abordează aspecte legate de confidențialitate într-un mediu social sau de comunicare digitală:

- Respectați întotdeauna principiile de evitare și minimizare a datelor: Nu furnizați niciodată date cu caracter personal și, dacă trebuie, furnizați cât mai puține (legat de aceasta: activați întotdeauna cât mai multe setări de protecție a confidențialității)
- Nu încărcați niciodată conținut (de exemplu, fotografii sau clipuri video) pentru care nu dețineți drepturile de autor
- Nu partajați niciodată informații sau date personale ale altor persoane (de exemplu, fotografii, videoclipuri sau mesaje private) fără consimțământul explicit al acestora
- Verificați întotdeauna solicitările prietenilor sau ale familiei în mod offline
- Raportați întotdeauna utilizatorii suspecți care încearcă să vă convingă să vă împărtășiți informațiile personale - alții s-ar putea să nu fie la fel de inteligenți!

Un studiu german din 2012[17] privind confidențialitatea digitală arată că utilizatorii tineri, în special, au o abordare foarte individuală a confidențialității lor digitale. Aceștia participă adesea la mediile de comunicare și de socializare digitală într-un război între nevoia lor de participare socială și teama pentru viața lor privată. Studiul identifică trei tipuri de utilizatori cu strategii diferite de confidențialitate:

- **Persoanele care dezvăluie:** Acesta este cel mai mic grup dintre subiecții studiului. Acestea se caracterizează prin faptul că au setările de confidențialitate deschise în conturile lor online, împărtășind în același timp o mulțime de informații personale. Există relativ mai multe persoane revelatoare în rândul persoanelor mai tinere și în rândul persoanelor cu un nivel mai scăzut de educație formală. Studiul sugerează că acest grup fie își împărtășește datele în mod voluntar, fie că nu are competența și conștientizarea pentru setări de confidențialitate sigure.
- **Persoanele prudente:** Acest grup de persoane are setări de confidențialitate relativ restrictive și se feresc să împărtășească informații personale. Ele reprezintă antipodul persoanelor revelatoare. Deși vizitează frecvent rețeaua lor socială preferată, probabil că nu vor să piardă informații sociale importante.

[14] https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=e35b1371111e
[15] https://www.upguard.com/breaches/facebook-user-data-leak
[16] https://www.theguardian.com/technology/2013/feb/02/twitter-hacked-accounts-reset-security
[17] https://www.medienanstalt-nrw.de/fileadmin/lfm-nrw/Forschung/LfM-Band-71.pdf

- **Managerii de confidențialitate:** Acest grup de persoane este în permanență activ în ceea ce privește publicarea de actualizări de stare și comentarii pe rețelele sociale. Aceștia posedă o rețea vastă de contacte și îi cunosc pe mulți dintre ei și în viața reală. Aceștia par a fi experți în materie de confidențialitate în mediul digital și pot pune în balanță obiceiurile lor de partajare și protecția vieții private.

Studiul concluzionează că potențialele amenințări la adresa vieții private nu afectează aproape deloc comportamentul utilizatorului. Interesant este faptul că principiile cetățeniei digitale în sine nu sunt căutate în mod activ.

Studiu de caz - Social Media și furtul de identitate

Un articol care discută aplicarea modernă a furtului de identitate prin utilizarea rețelelor de socializare. Acesta prezintă 4 cazuri de furturi de identitate și oferă sfaturi despre cum să vă protejați de acest tip de fraudă.

Jessica Velasco pentru socialnomics.net, 13/01/2016: https://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/

> *"Studiu de caz: Cele mai multe Sarah Palin*
>
> *Fostul guvernator al Statului American Alaska, Sarah Palin, nu este străină de controverse și nici de conturi de Twitter impostori. În 2011, contul oficial de Twitter al lui Palin de la acea vreme, AKGovSarahPalin (în prezent@SarahPalinUSA), s-a pierdut tot mai mult într-o mare de conturi false.*
>
> *Într-un incident deosebit de notabil, un imitator al lui Palin a postat pe Twitter o invitație deschisă la casa familiei lui Sarah Palin pentru un grătar. Ca urmare, personalul de securitate al lui Palin a trebuit să fie trimis la reședința sa din Alaska pentru a-i descuraja pe potențialii petrecăreți.*
>
> *Acest fenomen nu se limitează doar la Sarah Palin. Multe personalități publice și politicieni, în special cei controversați, cum ar fi candidatul la alegerile prezidențiale din 2016, Donald Trump, au o mulțime de conturi false care le asumă identitatea."*

Auto-reflecție: Vă expune excesul de sharing la riscul de furt de identitate?

Exercițiul 3: Comunitate

Obiectiv:

- Înțelegerea și aplicarea modalităților de protejare a vieții private în comunitățile online

Durata: 25 de minute

Instrumente: dispozitiv digital cu conexiune activă la internet, pix și hârtie

Metode: plen, cercetare, lucru în grup

Descrierea exercițiului: Elevii lucrează împreună în grupuri mici (maximum 4 persoane). Grupul alege un site de rețea socială cu un volum mare de comunicare (de exemplu, Facebook, Twitter, Instagram, Twitch, TikTok). În mod ideal, toți elevii sunt deja activi pe site-ul ales. Ulterior, aceștia încearcă să găsească o soluție pentru fiecare dintre următoarele provocări: (1) Cum pot activa cele mai restrictive setări de confidențialitate pe profilul meu? (2) Cum pot elimina o fotografie jenantă

cu mine pe care alte persoane au partajat-o pe platformă? (3) Cum pot să raportez sau să blochez alți utilizatori? (4) Unde pot găsi termenii serviciului și ce prevăd aceștia cu privire la confidențialitatea mea? (5) Cum îmi pot șterge profilul și dacă acesta a dispărut cu adevărat?

Sarcini:

- În termen de 3 minute, alegeți un site de rețele sociale.
- Vizitați site-urile timp de cincisprezece minute și răspundeți la cele 5 întrebări cu ajutorul site-ului sau al cercetării
- Împărtășiți rezultatele cu clasa (vă rugăm să rețineți că nu trebuie să împărtășiți nicio informație care v-ar putea face să vă simțiți inconfortabil).

Concluzii: Formatorul ar trebui să se concentreze asupra obstacolelor pe care le creează site-urile rețelelor de socializare pentru a păstra accesul la datele personale ale utilizatorilor lor. Formatorul ar trebui, de asemenea, să includă experiențe din viața reală pe care unii dintre elevi le-ar fi putut face deja în legătură cu unele dintre aceste provocări.

Lecții învățate: Odată ce informațiile sunt publice, este greu să le recuperați. Fiți atenți atunci când faceți parte din marile rețele de socializare, acestea nu vă sunt prietene.

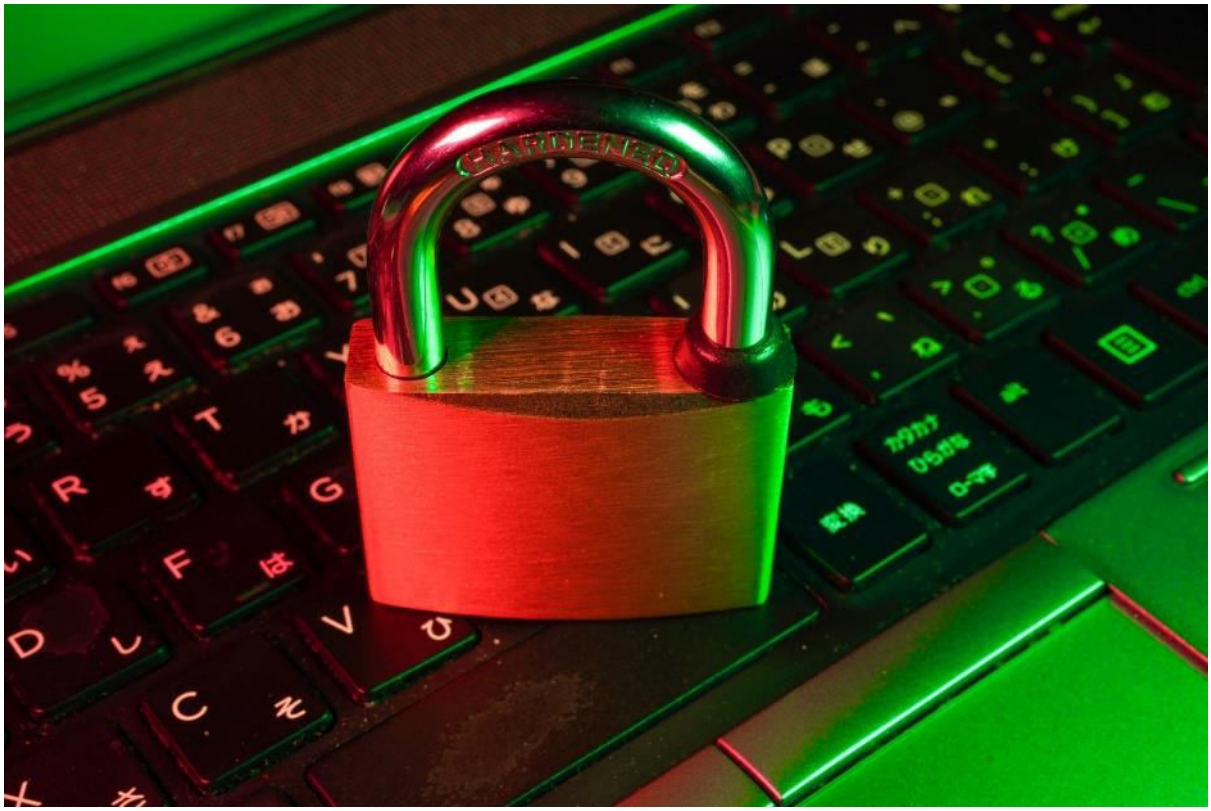
Lecturi suplimentare

De ce suntem dependenți de social media: Psihologia like-urilor: "Like-urile de pe rețelele de socializare creează dependență pentru că îți afectează creierul, similar cu consumul de substanțe chimice. Like-urile simbolizează un câștig de reputație, făcându-te să te compari în mod constant cu colegii tăi." https://steverosephd.com/why-we-are-addicted-to-likes/

Chestionar online

Chestionar online			
Titlul cursului:	Confidențialitate și securitate		
Titlul modulului:	Confidențialitatea într-un mediu digital		
Adevărat sau fals	Indicați dacă următoarele afirmații sunt Adevărate (A) sau False (F)		
Afirmații		A	F
1	Nu există niciun beneficiu societal pentru mediile digitale		
2	Peste 3 miliarde de oameni folosesc în prezent rețelele de socializare		
3	Facebook șterge automat datele mele personale după o anumită perioadă de timp		
4	În general, se poate avea încredere în marile companii de tehnologie că vor trata cu grijă datele mele personale		
5	Aplicarea metodei de evitare a datelor este cel mai sigur mod de a-mi păstra datele personale în siguranță		
6	Facebook poate utiliza datele mele pentru a-mi personaliza experiența, în conformitate cu termenii și condițiile sale de utilizare.		
7	Profilarea reprezintă un pericol pentru viața mea privată		
8	Furtul de identitate este o amenințare majoră pentru utilizatorii neexperimentați de rețele sociale		

4. Modulul 4 - Riscuri de securitate într-un mediu digital



Prezentare generală a cursului

Rezumat: Acest modul prezintă elementele de bază și diferitele amenințări la adresa hardware-ului și software-ului. Se concentrează asupra riscurilor din viața de zi cu zi și asupra rolului utilizatorului ca parte esențială a vulnerabilităților tipice de securitate.

Structură:

- Prezentare generală a cursului
- Introducere în hardware
- Introducere în software
- Amenințări la adresa hardware și software
- Studiu de caz
- Lecturi suplimentare
- Exercițiu
- Feedback
- Chestionar online

Obiective de învățare:

- Înțelegeți rolul hardware-ului și al software-ului în mediile digitale.
- Identificați riscurile individuale ale utilizării de hardware și software.
- Recunoașteți riscurile legate de utilizator în legătură cu utilizarea de hardware și software.

Introducere în hardware

În fiecare zi avem de-a face cu diferite dispozitive pentru a participa la un mediu digital, de exemplu smartphone-uri, PC-uri desktop sau bancomate. Hardware este termenul utilizat pentru a descrie componentele fizice ale acestor dispozitive. În timp ce hardware-ul în sine poate fi o vulnerabilitate critică, măsurile de securitate au fost luate în principal pentru problemele legate de software și de utilizator (s. subiectul următor).

Combinația mai multor componente hardware face ca dispozitivele noastre să funcționeze:

- Unitatea centrală de procesare (CPU) este responsabilă pentru efectuarea diverselor comenzi și calcule necesare pentru buna funcționare a dispozitivelor noastre. Veți găsi o unitate centrală de procesare în smartphone-ul dumneavoastră, în laptop, în PC-ul desktop sau în tabletă, de exemplu.
- GPU (Unitatea de procesare grafică) este responsabilă pentru orice proces solicitant din punct de vedere grafic, cum ar fi streamingul video sau jocurile video. GPU-urile cu sarcină mare de lucru necesită o cantitate mare de energie și pot procesa chiar și calcule complexe și lungi într-un timp scurt.
- HDD (Hard Disk Drive) și SSD (Solid State Drive) sunt dispozitive de stocare. Acestea sunt utilizate pentru a salva date sau software. Diferența dintre ele constă în arhitectura lor: HDD-urile folosesc o tehnologie de stocare magnetică, în timp ce SSD-urile și toate dispozitivele mobile folosesc tehnologia de memorie flash.
- Placa de bază sau placa de bază este piesa centrală a fiecărui calculator sau dispozitiv mobil. Aceasta conectează toate componentele electronice ale dispozitivului.
- Placa RAM (Random Access Memory - memorie cu acces aleatoriu) este o formă de memorie a computerului. Dispozitivul stochează programele executate în prezent, părțile de program și datele în memoria RAM. Viteza de acces la RAM și mărimea capacităților de stocare ale acesteia pot îmbunătăți drastic viteza unui dispozitiv.

Introducere în software

Software-ul se referă la toate tipurile de programe sau aplicații pe care le putem instala pe dispozitivele noastre, cum ar fi LibreOffice Writer, playerul VLC sau aplicația bancară personală. În timp ce hardware-ul este responsabil pentru efectuarea lucrului, putem folosi software-ul pentru a determina sarcina pe care dispozitivele noastre ar trebui să o îndeplinească.

Există diferite tipuri de software pentru diferite scopuri:

- Software-ul de sistem se referă la toate programele și datele care sunt utilizate pentru a controla procesele care fac ca un computer să funcționeze. Software-ul de sistem este conectat în mod complicat la hardware-ul dispozitivului respectiv și controlează utilizarea resurselor; prin urmare, acestea asigură infrastructura în calculator. Exemple pentru software-ul de sistem sunt:
    - sisteme de operare, cum ar fi Linux, Windows, Android sau iOS
    - drivere de dispozitiv pentru hardware extern, cum ar fi imprimantele sau difuzoarele.

- Software-ul de aplicație se referă la toate programele care execută sarcini specifice pentru utilizatori și care nu sunt legate de software-ul de sistem sau de utilități. Toate dispozitivele moderne pot executa o serie de programe de aplicații diferite:

  Playere media, de exemplu, playerul VLC
  Procesoare de text, de exemplu LibreOffice Writer
  Software de editare, de exemplu Adobe Premiere Pro
  Clienți de e-mail, de exemplu Mozilla Thunderbird
  Browsere web, de exemplu Mozilla Firefox.

- Aplicațiile software pot fi fie instalate de către utilizator, care, în majoritatea cazurilor, funcționează prin descărcarea datelor programului de la o sursă online, fie sunt preinstalate și incluse în anumite dispozitive, cum ar fi smartphone-urile.
- Software-ul utilitar se referă la software-ul care sprijină infrastructura, sistemele de operare sau software-ul de aplicații cu funcții suplimentare. Software-ul utilitar este adesea integrat în sistemele de operare, unele dintre ele funcționând în fundal, prin urmare distincția dintre software-ul de sistem și software-ul utilitar nu este întotdeauna clară. Exemple tipice pentru software-ul utilitar cunoscut sunt:
  - Programele antivirus
  - Programe de recuperare a datelor
  - Administratori de fișiere.

Amenințări pentru hardware și software

Așa cum am stabilit în modulele anterioare, trebuie să acordăm o atenție deosebită datelor și informațiilor noastre personale. Beneficiile și ușurarea pe care le oferă îndeplinirea online a multor sarcini sau a rutinelor vieții de zi cu zi pot amenința, de exemplu, viața noastră privată:

- S-ar putea să fiți bolnav și să doriți să mergeți la medic. Căutați un medic specializat folosind Google pe smartphone-ul dumneavoastră. Apoi treceți la apelarea medicului, folosind smartphone-ul și stabilind o programare, pe care o salvați în aplicația de calendar a smartphone-ului. În ziua programării, vă folosiți smartphone-ul pentru a cumpăra un bilet de tramvai și Google Maps pentru a ajunge la destinație. După programare, vizitați cea mai apropiată farmacie și cumpărați medicamentele prescrise, utilizând Google Pay cu smartphone-ul dumneavoastră.
- Căutați persoane interesante pe aplicația de întâlniri Tinder. După ce discutați o vreme cu o persoană interesantă, cu ajutorul smartphone-ului, faceți schimb de adrese de e-mail. Folosiți o aplicație de client de e-mail pe smartphone și, după un timp, faceți schimb de numere de telefon. Procedați la utilizarea WhatsApp și vă sunați din când în când. În cele din urmă, vă întâlniți pentru prima întâlnire în viața reală. Aplicația de calendar de pe smartphone vă reamintește de întâlnire și folosiți PayPal pe smartphone pentru a plăti biletele de film. Mai târziu, seara, folosiți opțiunile de plată de pe smartphone pentru a plăti băuturile la bar, înainte de a vă lua la revedere unul de la celălalt și de a chema un Uber pentru a merge acasă.

După cum arată exemplele, deseori folosim suficient de des unul și același dispozitiv în scopuri diferite, în timp ce partajăm și stocăm informații sensibile și personale. Dacă cineva are acces la acest dispozitiv, poate ajunge cu ușurință să cunoască sau cel puțin să reconstruiască cele mai intime detalii ale vieții dumneavoastră private.

1. **Riscuri hardware**

   Pe măsură ce tehnologia avansează, proiectarea componentelor hardware devine din ce în ce mai complexă. Un exemplu recent din 2018 prezintă două exemple de vulnerabilități hardware critice: "Meltdown" și "Spectre" exploatează ambele vulnerabilități ale cipurilor moderne ale procesoarelor și pot fi folosite pentru a accesa datele din programe și din sistemele de operare. Vulnerabilitățile pot fi exploatate în smartphone-uri, PC-uri desktop și, practic, în orice dispozitiv care utilizează unul dintre aceste cipuri CPU. Există și alte exemple de atacuri asupra componentelor hardware, de exemplu "RAMbleed", dar acestea sunt, de obicei, dificil de executat și necesită condiții prealabile specifice.

   Deși există modalități de a vă proteja împotriva acestor tipuri de vulnerabilități (a se vedea secțiunea următoare), cea mai mare amenințare la adresa hardware-ului dumneavoastră este accesul direct. Deși este puțin probabil ca PC-ul dvs. de birou de acasă să fie accesat de un atacator, este ușor să pierdeți un stick USB sau smartphone-ul (nu întotdeauna depinde de neglijența utilizatorului - smartphone-urile scumpe atrag hoții, de exemplu).

2. **Riscuri legate de software și de rețea**

   Riscurile legate de software și de rețea pot reprezenta o amenințare la adresa securității întregului dispozitiv. Acestea rezultă adesea fie din erori de software (de exemplu, programatorii au făcut o greșeală în timpul creării software-ului), fie din atacuri online și/sau din diferite tipuri de malware (software care acționează în mod intenționat împotriva interesului utilizatorului, dăunând calculatorului), inclusiv viruși, viermi, troieni, programe spion sau adware.

3. **Riscuri legate de utilizator**

   Utilizatorii pot reprezenta cea mai mare amenințare prin comportamente neglijente, naive sau neinformate în timp ce își folosesc dispozitivele, adesea legate de gestionarea necorespunzătoare a parolelor sau de utilizarea datelor financiare personale. Riscurile legate de utilizatori includ concepte de criminalitate cibernetică, cum ar fi ingineria socială digitală, de exemplu prin phishing. În acest caz, atacatorul se prezintă ca un partener de comunicare de încredere pentru a obține acces la date personale sau pentru a-și manipula victima în vederea efectuării unui act rău intenționat.

Studiu de caz - Escrocul preferat al bunicii mele

O bunică chineză în vârstă de 88 de ani este convinsă de un escroc că un grup operativ guvernamental de elită are nevoie de ajutorul ei pentru a demasca o rețea criminală internațională. Folosind doar apeluri telefonice, o "întâlnire secretă" într-un hotel izolat și o poveste elaborată care se referă la nevoile lui "Laolao", escrocul reușește să-i golească conturile bancare și să-i ia economiile de-o viață.

Un articol de opinie scris de Frankie Huang în New York Times, 07/12/2019:
https://www.nytimes.com/2019/12/07/opinion/sunday/china-bank-scam-grandmother.html

Auto-reflecție: Care sunt cele mai vizate victime ale escrocilor financiari?

Exercițiul 4: Invazia

Obiectiv:

- Înțelegeți de ce este importantă securitatea.
- Identificați consecințele unei securități slabe.
- Analizați problemele de securitate.

Durata: 20 de minute

Instrumente: smartphone sau computer cu conexiune activă la internet, pix și hârtie.

Metode: joc de rol, plen, aplicație creativă, aplicație practică

Descrierea exercițiului: Conectați-vă la dispozitivul dumneavoastră și imaginați-vă că altcineva are acces complet la acesta. Parcurgeți aplicațiile, fișierele media și conținutul messengerului dvs. în timp ce răspundeți la următoarele trei întrebări: (1) Ce fel de informații private, profesionale sau financiare ar putea afla atacatorul despre dumneavoastră? (2) Ce fel de informații private, profesionale sau financiare ar putea afla atacatorul despre familia și prietenii dumneavoastră? (3) Ce informații ar fi cele mai jenante de împărtășit cu un străin?

Sarcini:

- Răspundeți la toate cele trei întrebări cât de mult puteți în cincisprezece minute.
- Scrieți răspunsurile sub formă de puncte.
- Împărtășiți rezultatele cu clasa (vă rugăm să rețineți că nu trebuie să împărtășiți nicio informație care v-ar putea face să vă simțiți inconfortabil).

Concluzii: Formatorul trebuie să găsească un echilibru între cunoștințele nou dobândite și natura afectivă a sarcinii. Formatorul ar trebui să tragă concluzii concrete pentru a îmbunătăți securitatea dispozitivelor tuturor.

Lecții învățate: Securitatea dispozitivelor este importantă pe mai multe niveluri și ne protejează de prejudicii.

Lecturi suplimentare

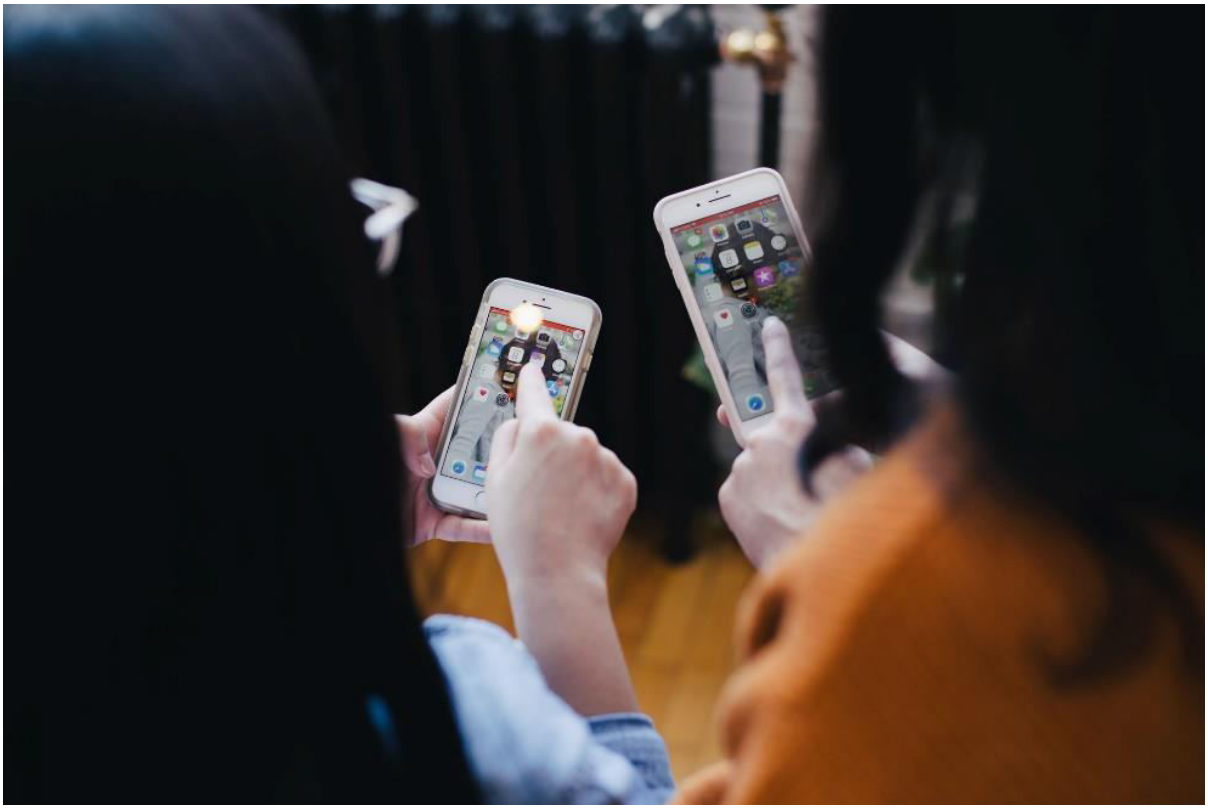
Project Zero: "Înființat în 2014, Project Zero este o echipă de cercetători în domeniul securității de la Google care studiază vulnerabilitățile de tip "zero-day" din sistemele hardware și software de care depind utilizatorii din întreaga lume." https://googleprojectzero.blogspot.com/

Firefox Monitor: Fundația Mozilla colectează scurgerile de date. Prin introducerea unei adrese de e-mail, Firefox Monitor verifică dacă această adresă a fost inclusă în scurgerile de date din trecut. Aceste informații v-ar putea ajuta să vă protejați mai bine pe dumneavoastră sau pe alții, de exemplu, de atacuri de inginerie socială. https://monitor.firefox.com/

Chestionar online

Chestionar online			
Titlul cursului:	Confidențialitate și securitate		
Titlul modulului:	Riscurile de securitate într-un mediu digital		
Adevărat sau fals	Indicați dacă următoarele afirmații sunt Adevărate (A) sau False (F)		
Afirmații		A	F
1	Sistemul meu de operare este o aplicație software		
2	Vulnerabilitățile de securitate de pe dispozitivul meu digital sunt întotdeauna legate de software		
3	Pot deschide fără ezitare o factură pe care furnizorul meu de servicii de internet mi-a trimis-o într-un fișier .zip		
4	Partajarea datelor mele de geolocalizare îmi pune în pericol viața privată		
5	Utilizatorii înșiși sunt deseori responsabili pentru scurgerile de securitate		
6	Adware-ul îmi protejează dispozitivul de reclamele nesolicitate		

5. Modulul 5 - Sfaturi de securitate pentru mediul digital



Sursa: Unsplash

Prezentare generală a cursului

Rezumat: Acest modul oferă sfaturi accesibile cu privire la probleme de securitate legate de hardware, software și utilizatori, punând accentul pe sfaturi practice ca parte importantă a protecției vieții private.

Structură:

- Prezentare generală a cursului
- Sfaturi privind securitatea hardware
- Sfaturi privind securitatea software
- Sfaturi privind securitatea legată de utilizator
- Studiu de caz
- Lecturi suplimentare
- Exercițiu
- Feedback
- Chestionar online

Obiective de învățare:

- Reamintirea mijloacelor de bază ale securității în mediile digitale.
- Elaborarea unei strategii de securitate de bază pentru a vă proteja viața privată proprie și a altor persoane.

- Dezvoltarea unei atitudini care să promoveze comportamente și interacțiuni online conștiente și responsabile.
- Aplicarea de măsuri de securitate pentru propriile dispozitive, conturi și interacțiuni digitale.

Păstrarea în siguranță a informațiilor și datelor personale nu este o sarcină ușoară, dar merită efortul de a vă proteja pe dumneavoastră și pe ceilalți de diferite tipuri de prejudicii, care vă afectează negativ viața profesională și/sau privată. Această listă conține reguli generale pe care ar trebui să le respectați întotdeauna:

Sfaturi privind securitatea hardware

- **Cumpărați hardware de la producători de încredere**: Este aproape imposibil pentru un utilizator obișnuit să afle despre vulnerabilitățile dispozitivelor de consum, cum ar fi smartphone-urile, laptopurile sau routerele. Un bun punct de plecare este locația și jurisdicția respectivă a producătorului de hardware, care ar putea să îi impună respectarea legilor privind confidențialitatea și securitatea.
- **Nu lăsați dispozitivele nesupravegheate**: Nu transportați informații sensibile pe dispozitive mobile, cum ar fi smartphone-uri sau unități USB. Dacă trebuie să o faceți, asigurați-vă că dispozitivele sunt cel puțin protejate prin parolă sau PIN sau, mai bine, criptate prin utilizarea unui software de criptare, de exemplu VeraCrypt. Dacă folosiți un computer de birou, blocați întotdeauna ecranul sau închideți-l atunci când nu îl utilizați.
- **Dezactivați setările de geolocalizare și Bluetooth**: Atâta timp cât nu aveți nevoie de ele, nu există niciun motiv pentru a le menține activate, deoarece acestea oferă potențial o mulțime de metainformații despre dumneavoastră.
- **Nu introduceți dispozitive de origine necunoscută**: Această regulă este deosebit de importantă într-un mediu de lucru profesional. Nu introduceți niciodată unități USB sau alte medii de stocare mobile în computerul dvs. de birou, dacă acesta nu a fost verificat în prealabil pentru potențiale riscuri de securitate.
- **Cumpărați dispozitive de rezervă**: Pierderea unor date importante poate cauza multe daune vieții dumneavoastră profesionale sau private (de exemplu, prin pierderea lucrării de licență). Luați-vă întotdeauna timp pentru a face în mod regulat copii de rezervă ale datelor importante și găsiți un spațiu fizic sigur pentru a stoca aceste copii de rezervă.

Sfaturi privind securitatea software

- **Păstrați software-ul actualizat:** Aceasta include software-ul de sistem, de utilitate și de aplicație. Activați actualizările automate pentru programele, aplicațiile și sistemul de operare, indiferent de dispozitivul pe care îl utilizați.
- **Utilizați software din surse de încredere:** Marile proiecte Open-Source sunt, de obicei, o resursă bună pentru software capabil și sigur, de exemplu Firefox ca browser web sau LibreOffice pentru aplicații de birou. Acordați o atenție deosebită atunci când descărcați pe dispozitivul dvs. mobil aplicații care nu sunt verificate de PlayStore sau AppStore.
- **Protejați-vă browserul:** Deoarece, de obicei, un browser este utilizat pentru a accesa WWW, este extrem de important să îl păstrați întotdeauna cât mai sigur posibil. Majoritatea browserelor acceptă instalarea de extensii, cum ar fi adblocker (de exemplu, uBlock Origin), blocatoare de urmărire (de exemplu, Facebook Container), firewall-uri (de exemplu, uMatrix) sau redirecționări automate către pagini https (de exemplu, HTTPS everywhere).
- **Instalați un software anti-malware (opțional)**: Beneficiile software-ului anti-malware sunt contestate, deoarece programele în sine prezintă un risc de securitate potențial și real.

Pentru a vă proteja sistemul, programele antivirus necesită, de obicei, un acces profund la sistem - dar, dacă programul antivirus însuși este compromis, sistemul dumneavoastră este brusc deschis atacurilor care nu ar fi avut loc în lipsa programului antivirus în primul rând. În plus, dacă sunteți un utilizator responsabil, oricum nu ar trebui să intrați niciodată în contact cu un software malware. Software-ul antivirus poate fi totuși benefic pentru utilizatorii neexperimentați, care ar putea fi mai sensibili la capcanele malware, cum ar fi atașamentele de e-mail.

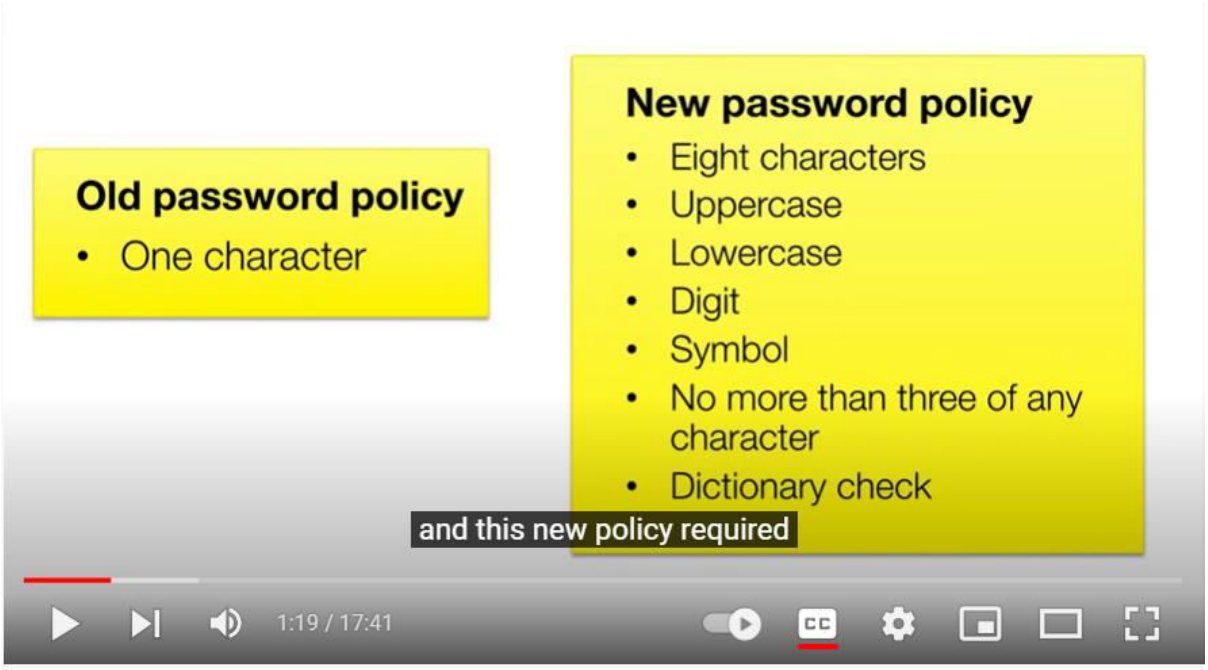
Sfaturi privind securitatea legată de utilizator

- **Aveți grijă cu sursele necunoscute:** Nu faceți niciodată clic pe linkuri sau atașamente din e-mailuri nesolicitate sau alte mesaje pe orice dispozitiv.
- **Aveți o bună gestionare a parolelor:** Utilizați un manager de parole (de exemplu KeyPass) pentru a crea parole sigure și pentru a stoca în siguranță aceste parole. Nu folosiți niciodată aceeași parolă de două ori.
- **Reducerea la minimum a utilizării informațiilor personale:** Ar trebui să vă gândiți întotdeauna dacă este necesară partajarea nesolicitată de informații și date personale într-un mediu digital, de exemplu pe rețelele de socializare. De obicei, nu există niciun beneficiu în a face acest lucru, dar vă poate dăuna mai târziu, de exemplu prin faptul că sunteți victima unor încercări de inginerie socială.
- **Evitați escrocheriile:** Învățați să nu vă încredeți în necunoscuții de pe internet sau de la un apel telefonic. Ingineria socială într-un mediu digital este deosebit de periculoasă pentru persoanele în vârstă, de exemplu, infamul grandparent scam. Informați-vă pe dumneavoastră și pe ceilalți și asigurați-vă că nu împărtășiți **niciodată** date și informații personale prin canale digitale nesigure, cum ar fi e-mailurile necriptate, chat-urile pe messenger sau apelurile telefonice.

Studiu de caz

Lorrie Faith Cranor: Ce e în neregulă cu parola ta?

"Lorrie Faith Cranor a studiat mii de parole reale pentru a descoperi greșelile surprinzătoare și foarte frecvente pe care utilizatorii - și site-urile securizate - le fac pentru a compromite securitatea. Și cum, vă veți întreba, a studiat mii de parole reale fără să compromită securitatea niciunui utilizator? Aceasta este o poveste în sine. Sunt date secrete care merită să fie cunoscute, mai ales dacă parola ta este 123456 ..."



Publicată de organizația TED la 24/06/2014: https://www.youtube.com/watch?v=0SkdP36wiAU

Auto-reflecție: Cât de puternice sunt parolele dumneavoastră?

Exercițiul 5: În siguranță împreună

Obiectiv:

- Înțelegeți de ce este importantă securitatea.
- Prezentați cele mai importante măsuri de securitate.

Durata: 20 de minute

Instrumente: pix și hârtie

Metode: plen, aplicație creativă, prezentare

Descrierea exercițiului: Fiecare elev își imaginează un membru al familiei în vârstă care și-a cumpărat primul laptop pentru a profita în sfârșit de tehnologia modernă. Acest membru al familiei știe cum să pornească noul său laptop și îi cere elevului ajutorul pentru (1) configurarea unei adrese de e-mail, (2) începerea operațiunilor bancare online, (3) crearea unui profil pe Facebook, (4) instalarea aplicației WhatsApp pentru desktop, (5) lucrul într-o cafenea în fiecare dimineață și conectarea la internet acolo. Fiecare elev pregătește o mică prezentare și se concentrează pe cele mai importante aspecte de securitate pe care dorește să le arate membrului familiei sale.

Sarcini:

- Scrieți cel puțin trei puncte cu cele mai importante aspecte de securitate pentru fiecare dintre cele 5 scenarii în 15 minute.
- Împărtășiți rezultatele cu clasa (vă rugăm să rețineți că nu trebuie să împărtășiți nicio informație care v-ar putea face să vă simțiți inconfortabil).

Concluzii: Formatorul ar trebui să sublinieze ce concluzii pot trage elevii din acest exercițiu pentru propriile obiceiuri de securitate. De asemenea, ar trebui să facă apel la sentimentul de comunitate de a se ajuta unii pe alții pentru a rămâne în siguranță.

Lecțiile învățate: Securitatea este importantă pentru a ne proteja de rău și ar trebui să ne sprijinim reciproc pentru a rămâne în siguranță.

Lecturi suplimentare

Will Styler: "Deci, vă amintiți disertația la care lucram? [...] Ei bine, o mare parte din munca pe care am făcut-o a dispărut, pentru că am luat niște decizii proaste și am avut foarte mult ghinion. Aș vrea să vă împărtășesc ce am făcut greșit și cum să nu mai fiți în poziția mea." https://wstyler.ucsd.edu/posts/lost_dissertation_files.html

Chestionar online

Chestionar online			
Titlul cursului:	Confidențialitate și securitate		
Titlul modulului:	Sfaturi de securitate pentru mediul digital		
Adevărat sau fals	Indicați dacă următoarele afirmații sunt Adevărate (A) sau False (F)		
Afirmații		A	F
1	Folosirea aceleiași parole peste tot este suficient de sigură dacă nu o partajați niciodată.		
2	Actualizările automate de securitate îmi pot proteja sistemul de operare		
3	Programele anti-malware fac întotdeauna ca dispozitivul meu să fie mai sigur		
4	Vulnerabilitățile de securitate de pe dispozitivul meu digital sunt întotdeauna legate de software		
5	Smartphone-ul meu este sigur dacă este protejat cu PIN		
6	Pot executa în siguranță pe smartphone-ul meu un fișier APK pe care l-am descărcat de pe un site web		

6. Teste de evaluare

Modulul 1

1) Care dintre propozițiile de mai jos se potrivește mai degrabă unei descrieri a securității online și nu a confidențialității online?
   a) Protecția personală a fiecăruia
   b) Protecția informațiilor online ale altor persoane
   c) Conștientizarea proprie a acțiunilor și comportamentului online

2) Care dintre următoarele seturi de reguli protejează confidențialitatea în mediile digitale sau electronice?
   a) Directiva privind ePrivacy (confidențialitatea electronică)
   b) Directiva privind e-securitate
   c) Directiva privind confidențialitate și securitate

3) Care este titlul complet al setului de norme al Directivei privind ePrivacy (confidențialitatea electronică)?
   a) Directiva privind confidențialitatea electronică și comportamentele online
   b) Directiva privind confidențialitatea și securitatea online
   c) Directiva privind confidențialitate și comunicații electronice

4) Ce înseamnă GDPR?
   a) Regulamentul general privind confidențialitatea datelor
   b) Regulamentul general privind protecția datelor
   c) Norme generale privind protecția datelor

Modulul 2

1) Când este Ziua Protecției Datelor?
   a) 28 ianuarie
   b) 28 iunie
   c) 28 decembrie

2) Care este numele campaniei globale de sensibilizare cu privire la siguranța online organizată de Alianța Națională pentru Securitate Cibernetică și de Inițiativa APWG pentru educație publică?
   a) STOP.THINK.CONNECT (OPREŞTE-TE. GÂNDEȘTE. CONECTEAZĂ-TE)

b) STOP.ReTHINK.CONTACT (OPREŞTE-TE. REGÂNDEȘTE. CONTACTEAZĂ)

c) START.THINK.COMMENT (ÎNCEPE. GÂNDEȘTE. COMENTEAZĂ)

3) Ce conținut aveți voie să publicați online?

a) Orice fotografii luate de la Google

b) Fotografii realizate de prietenii mei

c) Propriile mele fotografii

4) Care dintre următoarele tipuri de utilizatori au mai puțină grija de setările lor de confidențialitate?

a) Persoanele prudente

b) Persoanele revelatoare

c) Managerii de confidențialitate

Modulul 3

1) Care dintre următorii este responsabil pentru efectuarea diferitelor comenzi și calcule necesare pentru buna funcționare a dispozitivelor?

a) CPU (Unitatea Centrală de Procesare)

b) GPU (Unitate de Procesare Grafică)

c) HDD (Hard Disk Drive)

2) Ce înseamnă RAM?

a) Memorie suplimentară de la distanță (Remote Additional Memory)

b) Memorie cu acces aleator (Random Access Memory)

c) Gamă importantă de măsuri (Range Amount Measures)

3) Care dintre următoarele se referă la un software utilitar?

a) Linux

b) VLC Player

c) Un program anti-virus

4) Ce este un "Meltdown"?

a) vulnerabilitate hardware

b) Un software de aplicație

c) Un software de sistem

Modulul 4

1) Ce fel de riscuri sunt legate de malware, spyware și adware?
   a) Riscuri hardware
   b) Riscuri de software și de rețea
   c) Riscuri legate de utilizator

2) De ce fel de securitate este legată utilizarea unui manager de parole?
   a) Securitate hardware
   b) Securitate software
   c) Securitate legată de utilizator

3) Ce face un adware?
   a) Generează automat reclame online
   b) Blochează reclamele automate
   c) Ajută la formatarea hardware-ului

4) Care dintre următoarele se referă la software de aplicație?
   a) Browsere web
   b) Sisteme de operare
   c) Programe de recuperare a datelor

Modulul 5

1) Care dintre următoarele NU sunt utilizate ca dispozitive de stocare?
   a) HDD (Hard Disk Drive)
   b) SSD (Solid State Drive)
   c) GPU (Unitate de procesare grafică)

2) Care dintre următoarele propoziții este corectă?
   a) Setările de social media îmi oferă o protecție completă a datelor personale
   b) Trebuie să ajustez setările de confidențialitate pe rețelele de socializare pentru a-mi proteja datele

c) Datele mele pe social media sunt pe deplin protejate de îndată ce postez doar propriile mele fotografii

3) De ce riscuri este legată de criminalitatea informatică?

a) Riscuri legate de utilizator

b) Riscuri software

c) Riscuri hardware

4) Unde poate apărea scam-ul (înșelătoria)?

a) Numai offline

b) Numai online

c) Offline și online

7. Bibliografie

Council of Europe (2014). Guide to human rights for internet users

Netter, M., Herbst, S., Pernul, G. (2013). Interdisciplinary Impact Analysis of Privacy in Social Networks

Ladan, M. I. (2015). Social Networks: Privacy Issues and Precautions

Schenk, M., Niemann, J., Reinmann, G., Roßnagel, A. (2012). Digitale Privatsphäre: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen

Gross, R., Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook case)

Anexe

Fișe de verificare a testelor de evaluare

Fișa de verificare a testelor de evaluare pentru Modulul 1 - răspunsuri corecte

1c

2a

3c

4b

Fișa de verificare a testelor de evaluare pentru Modulul 2 - răspunsuri corecte

1a

2a

3c

4b

Fișa de verificare a testelor de evaluare pentru Modulul 3 - răspunsuri corecte

1a

2b

3c

4a

Fișa de verificare a testelor de evaluare pentru Modulul 4 - răspunsuri corecte

1b

2c

3a

4a

Fișa de verificare a testelor de evaluare pentru Modulul 5 - răspunsuri corecte

1c

2b

3a

4c

Lista de verificare a designului instrucțional pentru lucrătorii de tineret

Nr	Criterii	Da	Nu
1. Obiective			
1.1	Obiectivele sunt stabilite în mod clar pentru cel care învață?		
1.2	Sunt cerințele cursului în concordanță cu obiectivele?		
1.3	Capitolele/subiectele acoperă în detaliu obiectivele cursului?		
1.4	Obiectivele învățării corespund rezultatelor învățării?		
1.5	Conținutul general și structura cursului îndeplinesc obiectivele de instruire ale acestuia?		
2. Structură			
2.1	Cursul are o prezentare sau un program de studiu concis și cuprinzător?		
2.2	Include cursul exemple, analogii, studii de caz, simulări, reprezentări grafice și întrebări interactive?		
2.3	Folosește structura cursului metode și proceduri adecvate pentru a măsura rezultatele învățării cursanților?		
3. Conținut			
3.1	Conținutul curge fără probleme, fără greșeli gramaticale, sintactice și de dactilografiere?		
3.2	Este conținutul actualizat?		
3.3	Este conținutul aliniat cu programa școlară?		
3.4	Sunt rezultatele dorite încorporate în conținut?		
3.5	Este conținutul în conformitate cu legile privind drepturile de autor și tot materialul citat este citat corect?		
3.6	Cursul angajează studenții în gândirea critică și abstractă?		
3.7	Cursul are condiții prealabile sau necesită un background tehnic?		
4. Evaluare			
4.1	Sarcinile sunt relevante, eficiente și angajează cursanții într-o varietate de tipuri de activități?		
4.2	Întrebările practice și de evaluare sunt interactive?		
4.3	Sarcinile practice și de evaluare se concentrează pe obiectivele cursului?		
5. Tehnologie - Design			
5.1	Este designul clar și coerent, cu indicații adecvate?		
5.2	Sunt imaginile și grafica de înaltă calitate și adecvate pentru curs?		
5.3	Este cursul ușor de navigat și oferă asistență tehnică și de gestionare a cursului?		
5.4	Este structura de navigare a cursului coerentă și fiabilă?		
5.5	Sunt definite cerințele de hardware și software ale cursului?		
5.6	Este sincronizat textul audio și cel de pe ecran?		
5.7	Arhitectura cursului permite instructorilor să adauge conținut, activități și evaluări suplimentare?		

Feedback pe subiect pentru tineri

Evaluarea modulului						
Titlul cursului:						
Titlul modulului:						
Partea A:	Pe o scală de la 1 la 5, unde 1 reprezintă cel mai scăzut și 5 cel mai ridicat nivel de acord, indicați ce părere aveți despre următoarele aspecte					
Observații		1	2	3	4	5
1	Subiectul a fost interesant					
2	Cred că subiectele abordate au fost importante					
3	Mi-ar plăcea să aflu mai multe despre acest domeniu					
4	Am învățat lucruri noi pe care probabil le voi aplica în viitor					
5	Aș dori să îmi îmbunătățesc competențele în domeniu					
6	Este posibil să recomand acest curs					
Partea B:	În spațiul prevăzut, vă rugăm să includeți orice comentariu sau recomandare pe care doriți să o faceți.					
Partea C:	În spațiul prevăzut, vă rugăm să includeți adresa dvs. de e-mail, dacă doriți să fiți ținut la curent cu acest proiect.					