Igiena digitală:

Handbook pentru instituțiile VET

BDA

mathemagenesis

MUĞLA SITKI KOÇMAN ÜNİVERSİTESİ

eLearning software

EduVibes

WITTENBORG University of Applied Sciences

Co-funded by the European Union

GOOD START

Good Digital Hygiene for Startups

Nr. proiect: 2022-1-LV01-KA220-VET-000086725 | Titlul proiectului: Good Digital Hygiene for Startups

Cuprins

Modulul 1 - Igiena digitală pentru profesioniștii VET

Unitatea 1 - Semnificația igienei digitale în învățământul profesional și tehnic (VET)

Igiena digitală și securitatea cibernetică

Igiena digitală se referă la practicile și obiceiurile pe care le folosesc persoanele fizice pentru a-și menține confidențialitatea, securitatea și bunăstarea generală online. Aceasta cuprinde o gamă largă de comportamente și măsuri proactive menite să protejeze informațiile personale, să prevină amenințările online și să minimizeze riscurile asociate activităților digitale. Printre exemplele de practici de igienă digitală se numără utilizarea unor parole puternice, activarea autentificării cu doi factori, actualizarea regulată a software-ului, prudența în ceea ce privește schimbul de informații personale online și gestionarea urmelor prezenței digitale. Igiena digitală este un concept care este strâns asociat cu un alt concept, și anume securitatea cibernetică. Adesea, igiena digitală este considerată un element proactiv al securității cibernetice, care ține de responsabilitatea fiecărei persoanei.

Securitatea cibernetică este un domeniu specializat dedicat protejării sistemelor, rețelelor și datelor informatice împotriva accesului neautorizat, a atacurilor cibernetice și a altor breșe de securitate. Aceasta implică implementarea de măsuri tehnice, protocoale de securitate și strategii defensive pentru a proteja resursele digitale și pentru a atenua riscurile potențiale reprezentate de diverse amenințări cibernetice. Persoanele responsabile cu securitatea cibernetică lucrează adesea pentru a identifica vulnerabilitățile sistemelor, a dezvolta soluții de securitate, a monitoriza activitățile suspecte și a răspunde la incidentele de securitate pentru a asigura integritatea, confidențialitatea și disponibilitatea informațiilor și resurselor. Prin urmare, activitățile de securitate cibernetică sunt adesea efectuate de profesioniști, spre deosebire de igiena digitală, care poate fi responsabilitatea tuturor.

Igiena digitală în organizațiile VET

Diverse organizații tind să se aștepte ca angajații lor să respecte câteva reguli generale pentru a se asigura că regulile și cele mai bune practici de igienă digitală sunt respectate. Instituțiile de educație și formare profesională (VET) au câteva linii directoare generale care sunt valabile pentru toate organizațiile care lucrează cu oameni și informațiile lor personale și cu servicii și produse proprietare care sunt dezvoltate,

stocate și partajate printr-un mediu digital. Cu toate acestea, au unele provocări specifice legate de tipul de serviciu pe care îl furnizează, precum și de natura unică a clienților lor țintă. Profesioniștii din domeniul educației se găsesc adesea într-o situație în care trebuie să ofere îndrumări suplimentare clienților lor. Acest lucru poate însemna că trebuie să fie „agenți" de igienă digitală în timp ce realizează instruirea, cum ar fi de exemplu, furnizarea serviciului dorit.

Există mai multe motive pentru care igiena digitală este considerată foarte importantă în special pentru instituțiile VET:

- **Protecția informațiilor sensibile**

Atunci când își desfășoară activitatea, instituțiile VET gestionează adesea o multitudine de informații sensibile, inclusiv înregistrările elevilor/ studenților, datele academice și detaliile financiare. Unele dintre aceste informații pot fi cruciale pentru instituție atunci când efectuează analize cu privire la activitățile de învățare sau evaluează serviciile furnizate clienților. Practicarea unei bune igiene digitale ajută la protejarea acestor informații împotriva accesului neautorizat, a încălcării securității datelor și a amenințărilor cibernetice, asigurând confidențialitatea și integritatea datelor sensibile.

- **Păstrarea reputației instituționale**

Atunci când gestionează datele care sunt încredințate unei instituții VET fără nivelul adecvat de îngrijire, instituția poate schimba, fără să vrea, modul în care clienții și partenerii săi o văd. O încălcare a securității datelor sau un incident de securitate poate avea daune reputaționale semnificative pentru o instituție VET. Prin prioritizarea practicilor de igienă digitală, instituțiile își demonstrează angajamentul față de securitate, încredere și profesionalism, sporindu-și astfel reputația în rândul părților interesate, inclusiv a elevilor/ studenților, părinților, angajatorilor și a altor organisme de reglementare.

- **Respectarea reglementărilor**

În funcție de natura muncii lor și de modul în care se conectează cu clienții lor, instituțiile VET sunt supuse diferitelor reglementări și cerințe de conformitate legate de protecția datelor, confidențialitate și securitate cibernetică. Respectarea celor mai bune practici de igienă digitală ajută la asigurarea conformității cu legile și reglementările relevante, reducând riscul amenzilor de reglementare, al penalităților și al răspunderii legale asociate cu neconformitatea.

- **Sprijin pentru învățare și predare**

Tehnologiile digitale joacă un rol crucial în educația modernă, facilitând învățarea online, proiectele de colaborare și evaluările digitale. Aceste tehnologii sunt utilizate pentru a dezvolta, gestiona și partaja materiale de instruire, pentru a organiza medii de instruire, pentru a gestiona implicarea participanților în acestea sau pentru a analiza datele colectate în timpul procesului de instruire. Prin menținerea unei infrastructuri digitale sigure și fiabile, instituțiile VET pot oferi o experiență de învățare fără probleme pentru

elevi/ studenți și profesori, încurajând inovația, creativitatea și implicarea în activitățile de predare și învățare.

- **Diminuarea riscurilor de securitate cibernetică**

Sectorul educației poate fi vizat de infractorii cibernetici care încearcă să exploateze vulnerabilitățile sistemelor și ale rețelelor digitale sau lipsa de cunoștințe și abilități ale elevilor/studenților și profesorilor care nu sunt obișnuiți să fie implicați în formarea într-un mediu digital. Implementarea măsurilor de igienă digitală ajută la diminuarea riscurilor de securitate cibernetică, inclusiv celor de tip malware, atacuri de phishing, amenințări ransomware și acces neautorizat la resurse educaționale, protejând astfel continuitatea serviciilor și operațiunilor educaționale.

- **Promovarea cetățeniei digitale responsabile**

Pentru unii dintre participanții la proces, aceasta poate fi prima oportunitate de a fi implicați în formarea profesională care se desfășoară într-un mediu digital sau utilizează un mediu digital pentru a crea, gestiona și partaja materiale de formare, desfășoară schimbul de cunoștințe și comunicarea cu alți participanți prin mijloace digitale sau utilizează instrumente digitale pentru a îndeplini sarcini administrative în timpul instruirii. Instituțiile VET au responsabilitatea de a-și educa cursanții și personalul implicat în predare cu privire la practicile digitale sigure și responsabile. Prin integrarea educației privind igiena digitală în curriculumul VET și în programele de formare, instituțiile oferă cursanților cunoștințele, abilitățile și atitudinile necesare pentru a naviga eficient în peisajul digital, pentru a-și proteja identitățile online și pentru a contribui pozitiv la societatea digitală.

- **Pregătirea pentru carierele viitoare**

În era digitală de astăzi, alfabetizarea digitală și conștientizarea securității cibernetice sunt abilități esențiale pentru persoanele care intră pe piața muncii. În timp ce învățarea unora dintre abilitățile legate de igiena digitală poate să nu fie obiectivul principal al unui elev sau student, participarea la formare le poate oferi oportunități de îmbunătățire a acelor abilități care s-ar putea dovedi utile în viitor. Profesorii și organizatorii de formare ar trebui, de asemenea, să fie conștienți de faptul că ar putea fi necesar să aloce timp și resurse pentru acest scop specific. Prin promovarea practicilor de igienă digitală, instituțiile VET echipează elevii/ studenții cu cunoștințele și abilitățile fundamentale necesare pentru a naviga printre provocările digitale în cariera lor viitoare, fie în industriile tradiționale, fie în cele digitale. Același lucru este valabil și pentru profesorii care, prin participarea la formare folosind medii și instrumente digitale, își păstrează practica de predare modernă și pot întâlni noi oportunități pentru cariera lor.

În general, igiena digitală este importantă pentru instituțiile VET la nivel de organizație, precum și pentru un angajat individual și la nivelul clienților acestora, pentru a proteja informațiile sensibile, pentru a păstra reputația instituțională, pentru a respecta reglementările, pentru a sprijini învățarea și predarea, pentru a

atenua riscurile de securitate cibernetică, pentru a promova cetățenia digitală responsabilă și pentru a pregăti cursanții și, într-o oarecare măsură, profesorii și alți angajați pentru succes într-o lume digitală. Prin prioritizarea igienei digitale, instituțiile VET pot crea un mediu de învățare sigur, securizat și favorabil, care permite cursanților să prospere în era digitală.

Unitatea 2 – Competențe și cerințe pentru profesori și formatori VET

Roluri și responsabilități pentru instituțiile VET

În primul rând, să începem cu cei care ar putea avea rolurile implicate în instruirea VET. Aceștia ar trebui să fie conștienți de problemele de igienă digitală și ar trebui să posede abilitățile necesare. În funcție de situațiile întâlnite atunci când desfășoară și participă la traininguri care se realizează într-un mediu digital, profesorii și formatorii VET se pot confrunta cu diviziuni diferite ale sarcinilor individuale care revin participanților la proces. Prin urmare, implementarea și gestionarea igienei digitale într-o instituție de educație și formare profesională (VET) poate necesita coordonarea și colaborarea între diferite părți interesate cu roluri și responsabilități diferite. Profesorii pot avea avantajul de a fi sprijiniți de un personal IT complet pregătit pentru a se ocupa de aspectele tehnice ale instruirii sau pot fi nevoiți să se bazeze pe abilitățile și cunoștințele proprii. Din acest motiv, competențele și cerințele pentru profesorii și formatorii VET pot varia în funcție de instituția din care fac parte.

Există mai multe roluri și responsabilități tipice pentru persoanele care pot fi implicate în procesul sau formarea în mediul digital de astăzi, fiecare cu propriile sarcini și cerințe de calificare:

- **Chief Information Officer (CIO) sau Chief Technology Officer (CTO)**

CIO sau CTO este preocupat în principal de dezvoltarea și supravegherea strategiei, politicilor și procedurilor de igienă digitală ale organizației. Aceștia participă la stabilirea obiectivelor organizațiilor ținând cont de igiena digitală și securitatea cibernetică. Responsabilitățile lor includ: asigurarea alinierii eforturilor de igienă digitală cu obiectivele generale IT și de securitate ale organizației; alocarea resurselor și bugetului pentru inițiativele de igienă digitală și măsurile de securitate cibernetică; furnizarea de leadership și îndrumare echipelor IT și de securitate responsabile de implementarea practicilor de igienă digitală.

- **Manager de securitate IT sau ofițer de securitate cibernetică**

Unele organizații pot avea o poziție dedicată de manager de securitate IT sau de ofițer de securitate cibernetică sau un alt post care îndeplinește rolul ca parte a fișei postului pe care îl ocupă. Un astfel de rol ar concepe și ar pune în aplicare controale de securitate cibernetică, garanții și măsuri de gestionare a riscurilor pentru a proteja sistemele, rețelele și datele instituțiilor VET. De asemenea, aceștia ar efectua evaluări periodice ale securității, audituri și scanări ale vulnerabilităților pentru a identifica și atenua potențialele amenințări și vulnerabilități, pentru a monitoriza incidentele de securitate, pentru a răspunde la incidentele de securitate cibernetică și pentru a coordona activitățile de răspuns la incidente. Ocazional, acest rol dezvoltă și oferă programe de formare și conștientizare în domeniul securității cibernetice pentru personal,

ceea ce îi face să își asume rolul de formator VET. Uneori, aceștia pot fi, de asemenea, invitați să instruiască elevii/ studenții pentru a promova bunele practici de igienă digitală în afara organizației lor ca experți.

- **Administrator IT sau Administrator de sistem**

Administratorii IT sunt responsabili pentru gestionarea infrastructurii IT a organizației și pot îndeplini unele sarcini pentru profesorii VET, în plan secund, fără a fi observați. Responsabilitățile lor includ mentenanța și administrarea sistemelor instituției VET, a serverelor și a infrastructurii de rețea în conformitate cu standardele de igienă digitală și cele mai bune practici; gestionarea conturilor de utilizator, a controalelor de acces și a permisiunilor pentru a asigura accesul securizat la resursele și datele instituției; instalarea, configurarea și actualizarea software-ului de securitate, a corecțiilor și a firmware-ului pentru a proteja împotriva vulnerabilităților și exploatărilor cunoscute care pot apărea atunci când se utilizează instrumente digitale și se efectuează acțiuni în timpul instruirii, cum ar fi partajarea materialelor de instruire sau comunicarea între participanți. Aceștia sunt, de asemenea, responsabili pentru monitorizarea jurnalelor de sistem și a alertelor pentru activități suspecte, încercări de acces neautorizat sau încălcări ale securității.

- **Responsabilul cu protecția datelor sau responsabilul cu confidențialitatea**

Responsabilii cu protecția datelor joacă un rol important în instituțiile VET, deoarece există reguli și reglementări la nivel național și internațional care necesită o atenție deosebită asupra modului în care instituțiile VET gestionează datele sensibile ale participanților la formare. Acest rol asigură respectarea reglementărilor privind protecția datelor și a legilor privind confidențialitatea care reglementează colectarea, utilizarea și stocarea datelor cu caracter personal în mediile VET; elaborează și menține politici, proceduri și documentație privind protecția datelor, inclusiv evaluări ale impactului asupra protecției datelor și notificări privind confidențialitatea; gestionează solicitările de acces ale persoanelor vizate, reclamațiile privind confidențialitatea și întrebările legate de practicile de protecție a datelor și de confidențialitate, colaborează cu echipele IT și juridice pentru a aborda incidentele și încălcările confidențialității securității datelor.

- **Tehnolog educațional sau designer instrucțional**

În timp ce rolurile anterioare pot fi întâlnite în orice organizație, tehnologul educațional sau designerul instrucțional este direct legat de formarea și educația efectuată de instituție. Responsabilitățile lor includ integrarea principiilor și practicilor de igienă digitală în curriculumul instituției VET, a materialele de instruire și activităților de predare; furnizarea de formare și sprijin profesorilor și personalului didactic cu privire la încorporarea educației de igienă digitală în practicile de predare; evaluarea și recomandarea instrumentelor și resurselor tehnologice educaționale care acordă prioritate securității, confidențialității și accesibilității pentru cursanții VET.

- **Utilizatori finali (personal și cursanți)**

Ultimul rol este adesea împărțit în două grupuri, dar ambele au responsabilități similare în ceea ce privește igiena digitală. Utilizatorii finali trebuie să respecte politicile, orientările și cele mai bune practici de igienă digitală atunci când utilizează sisteme, dispozitive și resurse online care au legătură cu instituția VET. Personalul de instruire al organizației poate fi solicitat de instituție să efectueze activități de formare sau administrative într-un mod specific stabilit de regulile și politica instituției. Ca atare, acestora li se poate solicita să participe la inițiative de sensibilizare și educare în materie de securitate cibernetică pentru a-și îmbunătăți înțelegerea riscurilor și responsabilităților digitale și pentru a raporta incidentele de securitate, activitățile suspecte și problemele de securitatea cibernetică personalului IT sau de securitate corespunzător pentru investigare și soluționare. Cu toate acestea, profesorii VET ar trebui să fie conștienți de rolul lor de consilieri pentru cursanții care ar putea avea nevoie de îndrumare atunci când în timpul instruirii utilizează un mediu digital care ar putea să nu le fie familiar.

O persoană dintr-o instituție VET poate îndeplini mai multe roluri simultan în timpul formării sau se poate concentra doar pe câteva responsabilități. Indiferent de aceasta, prin definirea unor roluri și responsabilități clare pentru persoanele implicate în implementarea și gestionarea igienei digitale într-o instituție VET, instituțiile pot colabora eficient pentru a stabili o cultură a conștientizării securității cibernetice, pentru a promova bunele practici de igienă digitală și pentru a proteja confidențialitatea, integritatea și disponibilitatea resurselor și datelor. Cu toate acestea, instituțiile vor solicita acestor persoane să posede anumite abilități și cunoștințe pentru a efectua practicile menționate mai sus.

Cadre de competențe digitale

Există cadre de competențe stabilite pentru a descrie setul de competențe care ar trebui să fie deținut de cei implicați în desfășurarea diferitelor activități într-un mediu digital. Unele dintre ele includ competențe digitale generale, în timp ce altele pot fi mai specifice pentru problemele legate de securitatea cibernetică și igiena digitală. Următoarele cadre sunt utile pentru identificarea competențelor digitale de igienă pentru profesorii și formatorii VET, precum și pentru identificarea posibilelor nevoi de formare pentru elevii/ studenții care participă la instruire în mediul digital.

- **Cadrul competențelor digitale pentru cetățeni (DigComp) [1]**

Cadrul DigComp 2.2, dezvoltat de Comisia Europeană, este cea mai nouă versiune a Cadrului competențelor digitale pentru cetățeni. Acesta definește componentele-cheie ale competenței digitale în cinci domenii: alfabetizarea informației și a datelor, comunicarea și colaborarea, crearea de conținut digital, siguranța și rezolvarea problemelor. Fiecare domeniu este împărțit în continuare în competențe specifice care descriu abilitățile și cunoștințele necesare pentru a fi competenți în mediile digitale.

Acest cadru servește drept ghid pentru ca persoanele fizice să își evalueze și să își îmbunătățească competențele digitale și pentru educatori și factorii de decizie politică să elaboreze programe de învățământ și politici care să sprijine educația și formarea digitală. DigComp 2.2 introduce, de asemenea, niveluri de competență și exemple de utilizare, ceea ce-l face un instrument practic pentru diverse contexte educaționale și profesionale. Cadrul subliniază importanța capacității de a funcționa eficient și corect într-o societate digitală.

- **Cadrul european al competențelor digitale (E-CF) [2]**

Cadrul european al competențelor digitale (e-CF) este un cadru standardizat pentru descrierea competențelor, abilităților și nivelurilor de competență ale profesioniștilor din domeniul tehnologiei informației și comunicațiilor (TIC), dezvoltat pentru a sprijini creșterea și mobilitatea profesioniștilor din domeniul TIC. Cadrul constă în cinci domenii de competență legate de TIC, precum Planificare, Construire, Executare, Activare și Gestionare. Acesta conține în total 41 de competențe și include niveluri de competență care descriu cunoștințele, abilitățile și autonomia la fiecare nivel, variind de la nivelul de bază la cel de expert. Include, de asemenea, eșantioane de cunoștințe și abilități legate de competențe.

e-CF are scopul de a ajuta organizațiile, managerii de resurse umane, profesorii și formatorii să dezvolte roluri pentru locuri de muncă și trasee de carieră pentru profesioniștii din domeniul TIC, să îmbunătățească gestionarea forței de muncă și să încurajeze dezvoltarea profesională în sectorul TIC. Acesta servește, de asemenea, ca instrument pentru dezvoltarea politicilor, educarea și alinierea formării în cadrul pieței digitale din Europa.

- **Cadrul european de competențe în materie de securitate cibernetică (ECSF) [3]**

Cadrul european de competențe în materie de securitate cibernetică (ECSF) este conceput pentru a armoniza și standardiza abilitățile, rolurile și competențele în materie de securitate cibernetică în întreaga Europă. Acesta servește ca o structură fundamentală pentru dezvoltarea și evaluarea abilităților de securitate cibernetică, care vizează abordarea lacunelor de competențe în domeniul securității cibernetice și îmbunătățirea strategiei de securitate cibernetică a organizațiilor și națiunilor. ECSF clasifică abilitățile de securitate cibernetică în mai multe domenii, detaliind rolurile și competențele specifice necesare în domeniul securității cibernetice. Acesta prezintă rolurile de bază în domeniul securității cibernetice care sunt de obicei necesare organizațiilor, abilitățile specifice și abilitățile necesare pentru a îndeplini eficient aceste roluri și nivelurile de competență sau nivelurile de expertiză, de la începător la expert, necesare pentru fiecare competență.

Acest cadru este util pentru diverse părți interesate, inclusiv instituții de învățământ, companii și factori de decizie politică, pentru a dezvolta programe de învățământ, programe de formare și căi de carieră în

domeniul securității cibernetice. Acesta sprijină crearea unor structuri clare de carieră în domeniul securității cibernetice, facilitând identificarea deficitului de competențe și abordarea eficace a acestora.

- **Cadrul competențelor digitale pentru educatori (DigCompEdu) [4]**

Cadrul DigCompEdu descrie cerințele pentru dezvoltarea competențelor digitale ale personalului din învățământ. Acesta este adaptat în mod specific pentru cadrele didactice de la toate nivelurile de educație, de la educația timpurie la învățământul superior și educația adulților, și se axează pe îmbunătățirea competențelor digitale necesare pentru o predare eficace în medii de învățare tot mai digitalizate. Cadrul este structurat în jurul a șase domenii de competență privind implicarea profesională (Utilizarea tehnologiilor digitale pentru comunicare, colaborare și dezvoltare profesională), resurse digitale (Crearea și modificarea resurselor digitale și gestionarea eficientă a acestora), predare și învățare (Implementarea tehnologiilor digitale pentru pregătirea, implementarea și gestionarea procesului de predare și învățare), evaluare (Valorificarea tehnologiilor digitale în scopul evaluarii învățării, pentru învățare și ca învățare), responsabilizarea cursanților (Utilizarea instrumentelor digitale pentru a spori incluziunea, personalizarea și implicarea activă a cursanților), facilitarea competențelor digitale ale cursanților (Promovarea strategică a competențelor digitale ale cursanților și utilizarea sigură și responsabilă a instrumentelor digitale). În plus, cadrul DigCompEdu identifică 22 de competențe individuale și niveluri de competență care variază de la "Nou-venit" la "Pionier", oferind o cale pentru dezvoltarea practicilor digitale ale profesorilor.

Acest cadru servește drept ghid pentru profesori, pentru a-și evalua și îmbunătăți competențele digitale, și sprijină instituțiile de învățământ în proiectarea programelor și politicilor de formare aliniate la nevoile educaționale actuale.

Cadrele menționate mai sus, deși generale pentru identificarea cerințelor persoanelor și organizațiilor care participă la orice practică din mediul digital, oferă o imagine structurată a domeniului competențelor necesare profesorilor și formatorilor VET.

Competențe pentru profesorii și formatorii VET

Într-o anumită măsură, formatorii și educatorii VET nu se deosebesc de ceilalți participanți din mediul digital. Din acest motiv, abilitățile de care au nevoie pentru a adera la bunele practici de igienă digitală sunt abilități care ar trebui să fie posedate de oricine. Aceste aptitudini cuprind o serie de abilități tehnice, comportamentale și cognitive. Ele sunt, de asemenea, un subset de competențe care pot fi denumite competențe moderne sau viitoare și, pe baza dezvoltării recente a mediului digital, acestea sunt aceleași competențe care au fost subliniate ca esențiale pentru organizații sau viitorul apropiat, cum ar fi utilizarea tehnologiilor cloud, analizarea datelor de mari dimensiuni și utilizarea instrumentelor de inteligență artificială pentru a îmbunătăți productivitatea și eficiența muncii [5,6].

Cu toate acestea, natura activității lor impune profesorilor și formatorilor din domeniul VET să acorde o atenție mai mare modului în care gestionează datele și interacționează cu alți participanți la procesul de formare. Iată câteva abilități importante necesare profesorilor și formatorilor VET în ceea ce privește o bună igienă digitală:

- **Conștientizarea generală a securității cibernetice**

Această competență include înțelegerea amenințărilor online comune, cum ar fi amenințările malware, phishing-ul și atacurile de inginerie socială, precum și cunoașterea modului de a le recunoaște și de a răspunde la acestea; cunoașterea modului de navigare pe internet în siguranță, inclusiv evitarea site-urilor web suspecte, utilizarea conexiunilor securizate (HTTPS) și prudența atunci când se descarcă fișiere sau se dă clic pe link-uri.

- **Protecția datelor și confidențialitatea**

Competența include capacitatea de a cripta date sensibile, atât în tranzit, cât și în repaus, și a ști cum să ștergi sau să elimini în siguranță datele atunci când este necesar; și înțelegerea modului de configurare a setărilor de confidențialitate pe diverse platforme și dispozitive online pentru a controla partajarea informațiilor personale.

- **Securitatea și gestionarea dispozitivelor**

Această competență include practica actualizării regulate a software-ului, a sistemelor de operare și a aplicațiilor pentru a remedia vulnerabilitățile de securitate și pentru a proteja împotriva exploatărilor cunoscute; capacitatea de a crea parole puternice și unice pentru diferite conturi și de a utiliza eficient instrumentele de gestionare a parolelor pentru a stoca și gestiona parolele în siguranță; practica de a activa și gestiona autentificarea multi-factor, acolo unde este disponibilă, pentru a adăuga un nivel suplimentar de securitate conturilor online.

- **Comunicare digitală în siguranță**

Această competență include folosirea practicilor de comunicare securizată, cum ar fi utilizarea serviciilor de e-mail criptate sau selectarea și utilizarea aplicațiilor de mesagerie securizată atunci când se partajează informații confidențiale sau comunicați cu elevi/ studenți, colegi sau parteneri din afara organizației VET; respectarea liniilor directoare pentru identificarea și evitarea e-mailurilor de phishing, a escrocheriilor și a altor tactici de inginerie socială care ar putea compromite sistemele VET sau ar putea duce la încălcări ale siguranței datelor.

- **Gestionarea amprentei digitale**

Această abilitate include înțelegerea implicațiilor amprentei digitale și luarea de măsuri pentru a minimiza expunerea informațiilor personale online; sfătuirea participanților la formare să facă același lucru.

- **Gândire critică**

Această competență include dezvoltarea și folosirea abilităților de gândire critică pentru a evalua credibilitatea surselor online, pentru a identifica dezinformarea și escrocheriile și pentru a lua decizii în cunoștință de cauză cu privire la activitățile online atunci când desfășoară sau se pregătesc activitățile de predare/ formare.

- **Învățare continuă**

Această competență include practica generală de îmbunătățire continuă a competenței; învățarea de noi instrumente și abordări pentru predarea în mediul digital sau utilizarea instrumentelor digitale moderne; și informarea cu privire la evoluția amenințărilor la adresa securității cibernetice, a problemelor de confidențialitate și a celor mai bune practici prin educație și formare continuă.

- **Cetățenie digitală și etică**

Această abilitate include practicarea cetățeniei digitale responsabile atunci când se efectuează instruire VET prin respectarea reglementărilor și respectarea drepturilor altor persoane și organizații; promovarea cetățeniei digitale responsabile în rândul cursanților prin predarea comportamentului etic, a comunicării respectuoase și a etichetei digitale în mediile online; promovarea abilităților de gândire analitică pentru a ajuta cursanții să evalueze credibilitatea informațiilor online, să recunoască riscurile digitale și să ia decizii în cunoștință de cauză cu privire la activitățile lor online; protejarea reputației digitale a persoanelor și organizațiilor care participă la proces.

Aceste abilități pot fi regăsite în cadrul DigCompEdu descris anterior, dar este posibil să nu corespundă direct competențelor individuale incluse în aceste cadre. Mai degrabă, există elemente în descrierile domeniilor de competență din cadru care corespund competențelor benefice profesorilor și formatorilor VET.

Tabelul 1. Legătura dintre competențele propuse pentru formatorii VET și domeniile de competență DigCompEdu.

Competențele profesorilor VET	Aria de competențe DigCompEDU
Conștientizarea generală a securității cibernetice	• Împuternicirea cursanților • Facilitarea competenței digitale a cursanților
Protecția datelor și confidențialitatea	• Resurse digitale • Facilitarea competențelor digitale ale cursanților

Securitatea și gestionarea dispozitivelor	• Predarea și învățarea • Facilitarea competențelor digitale ale cursanților
Comunicarea digitală în siguranță	• Implicare profesională • Evaluare
Gestionarea amprentei digitale	• Resurse digitale • Facilitarea competenței digitale a cursanților
Gândire critică	• Predarea și învățarea • Facilitarea competenței digitale a cursanților
Învățare continuă	• Implicare profesională • Facilitarea competenței digitale a cursanților
Cetățenie digitală și etică	• Împuternicirea elevilor • Facilitarea competenței digitale a cursanților

Competențele oferă profesorilor și formatorilor VET mijloacele necesare pentru a participa la activități educaționale, respectând în același timp cele mai bune practici în domeniul igienei digitale. O referință realistă a unora dintre cele mai bune practici este disponibilă sub forma unei Fișa de verificare a igienei digitale [7]. Acesta descrie 12 principii ale vieții digitale sigure, care necesită toate cunoștințe despre lumea digitală, care includ:

- menținerea la zi a software-ului de lucru, antivirus, firewall etc.,
- utilizarea parolelor sigure, gestionarea lor în siguranță și utilizarea autentificării multi-factor,
- atenție la descărcarea software-ului,
- conștientizarea phishingului și a altor încercări suspecte de compromitere a resurselor dvs.,
- limitarea amprentei digitale și sociale,
- adoptarea unei mentalități generale "securitatea pe primul loc" atunci când se gestionează informații în mediul digital.

În predarea și educația VET, dobândirea și practicarea competențelor de igienă digitală este importantă pentru a oferi un mediu sigur pentru schimbul de informații.

Unitatea 3 - Adaptarea igienei digitale la curriculumul și instruirea VET

Subiectele de igienă digitală ar trebui să fie o parte zilnică a formării VET. Profesorii și formatorii VET ar trebui să urmeze ghidurile privind o bună igienă digitală atunci când planifică și gestionează instruirea, care pune în aplicare utilizarea instrumentelor digitale ca parte a furnizării mediului de formare; producerea și distribuirea materialelor de instruire; organizarea de comunicări între cursanți și profesori - cursanți; analiza rezultatelor instruirii; și efectuarea procedurilor administrative și planificarea pentru îmbunătățirea procesului de instruire.

În plus, profesorii VET ar trebui să fie conștienți de faptul că, deși subiectul instruirii poate să nu fie un subiect legat de lumea digitală, unele dintre aceste informații pot fi necesare pentru a spori eficacitatea instruirii desfășurate. Profesorii ar trebui să rămână conștienți de posibilele experiențe anterioare ale cursanților lor și să ajusteze programul de instruire, rezervând timp și efort pentru explicarea și demonstrarea unor practici de formare care vor duce la îmbunătățirea igienei digitale pentru cursanți.

Desigur, uneori igiena digitală și alte subiecte conexe pot fi subiectul principal real al instruirii. În aceste cazuri, profesorii și formatorii VET pot continua să-și îndrume cursanții în timp ce dobândesc noi cunoștințe și dobândesc noi abilități legate de igiena digitală.

Igiena digitală din perspectiva profesorilor VET ar putea fi percepută ca practica menținerii și asigurării unor activități digitale sigure și productive în timpul instruirii, care este furnizată indiferent de subiectul acestei instruiri. Mai multe aspecte ale formării profesionale și educaționale pot necesita utilizarea unui mediu digital pentru a îmbunătăți rezultatele instruirii și pentru a spori satisfacția cursanților care participă la instruire. Profesorii ar trebui să fie conștienți de modul în care utilizarea instrumentelor digitale afectează procesul de instruire și să încerce să utilizeze integrarea unora dintre aspectele legate de igiena digitală în formarea în sine. Iată câteva dintre opțiunile de îmbunătățire a procesului de instruire:

- **Subiecte și module de curs privind siguranța digitală**

Atunci când oferiți conținut pentru instruire, propuneți să începeți o activitate specifică de formare sau solicitați cursanților să realizeze o activitate administrativă legată de instruire, introducând câteva sfaturi sub forma unor subiecte de instruire mai mici sau a unor module mai extinse care furnizează cursanților informații despre fundamentele securității cibernetice, cum ar fi: gestionarea parolelor, recunoașterea încercărilor de phishing și securizarea datelor personale și la locul de muncă. Atunci când sunt disponibile, adaptați aceste subiecte la industriile, liniile de lucru, rolurile de lucru sau activitățile specifice cursanților, legate de domeniul real de lucru al acestora sau de aria de activitate preconizată sau de viitoarea poziție de muncă pe care se pregătesc să o introducă, făcând informațiile relevante și aplicabile.

- **Ateliere practice, lucru individual și în grup**

Atunci când efectuați sarcini practice în timpul instruirii, cum ar fi, de exemplu, ateliere practice sau sarcini de lucru individuale sau de grup, implementați ateliere în care cursanții pot practica configurarea rețelelor sigure, utilizarea VPN-urilor, instalarea și gestionarea software-ului de securitate și efectuarea de verificări regulate de securitate. Sau lăsați-i să experimenteze modul în care unele dintre greșelile de care poate nu sunt conștienți se desfășoară într-un mediu de învățare sigur și pot duce la probleme. O abordare practică și oportunități de încercare și eroare ajută la solidificarea cunoștințelor teoretice prin aplicarea practică.

- **Etică și conformitate**

În timpul instruirii, includeți discuții și oferiți îndrumări cu privire la comportamentul etic online și implicațiile juridice ale acțiunilor digitale, dacă subiectele de formare teoretică sau sarcinile practice au implicații asupra unor comportamente. Aceasta poate acoperi subiecte precum legile privind confidențialitatea datelor relevante pentru subiectul formării sau rolurile și conduita profesională ale cursanților, hacking-ul etic și importanța menținerii unei prezențe profesionale online.

- **Gestionarea amprentei digitale**

Educați cursanții cu privire la gestionarea amprentelor lor digitale, subliniind impactul pe termen lung al activităților online asupra reputației personale și profesionale. Instruirea poate include modul de utilizare eficientă a rețelelor sociale, gestionarea conținutului digital și înțelegerea consecințelor postărilor online. Educați cursanții cu privire la modul în care instrumentele digitale care sunt utilizate pentru muncă pot crea, de asemenea, o amprentă digitală și modul în care aceștia ar trebui să-și gestioneze rezultatele muncii și rezultatele altora dobândite în timpul colaborării.

- **Învățare continuă**

Fiți conștienți de faptul că mediile digitale moderne sunt în continuă schimbare. Pe baza rolului lor și a liniei de lucru din care provin sau se așteaptă să se alăture, cursanșii pot necesita noi cunoștințe despre subiecte legate de utilizarea noilor instrumente digitale. Este important să rămâneți la curent cu cele mai noi tehnologii și să fiți conștienți de cele mai noi amenințări care pot afecta cursanții care învață ceea ce predați. Creșterea gradului de conștientizare cu privire la noile opțiuni în mediul digital și introducerea de noi instrumente pentru cursanți pot duce la o calitate percepută mai bună a formării și la îmbunătățirea cunoștințelor și abilităților acestora. Căutarea oportunităților de învățare continuă și certificare în practicile de securitate digitală poate deveni o parte integrantă a curriculum-ului, indiferent de principalele subiecte de formare.

- **Evaluare și certificare**

Evaluările fac parte din instruire. Pe baza subiectului și a obiectivelor instruirii, evaluările pot fi mai mult sau mai puțin formale și pot include utilizarea instrumentelor digitale pentru a efectua evaluarea și pentru a

colecta și analiza rezultatele evaluării. O bună practică este să vă asigurați că elevii/ studenții sunt conștienți de utilizarea corectă a instrumentelor de evaluare. Conținutul evaluărilor poate include testarea cunoștințelor și abilităților dobândite în mod specific în domeniul igienei digitale, precum și cunoașterea subiectelor generale. Evaluarea și certificările pot fi folosite pentru a stimula elevii/ studenții, iar forma în care sunt prezentate rezultatele poate necesita o gândire suplimentară despre mediul digital. Elevii/ studenții pot avea nevoie de ajutor atunci când dobândesc și gestionează noile informații de certificare sau folosesc noile calificări pentru a-și spori capacitatea de angajare.

Este posibil să observați că unele dintre opțiunile de îmbunătățire a formării VET privind igiena digitală corespund competențelor identificate anterior. Toate aceste elemente pot fi încorporate în programele VET și privite din două perspective diferite: ce competențe de igienă digitală ar trebui utilizate ca parte a formării și necesită o atenție suplimentară în timpul instruirii; care sunt oportunitățile suplimentare pentru îmbunătățirea cunoștințelor și competențelor de igienă digitală în timpul instruirii, pe lângă subiectele principale. Abordarea acestor elemente poate îmbunătăți calitatea instruirii și poate oferi cursanților beneficii suplimentare în mediul lor de lucru, care se bazează în mare măsură pe opțiunile lumii digitale.

Din punct de vedere practic, aceasta înseamnă că profesorii și formatorii VET ar trebui: să introducă medii de învățare sigure și instrumente specifice pentru instruire, să stabilească direcții orientative pentru gestionarea materialelor de formare, să utilizeze instrumente de comunicare și să efectueze comunicări având în vedere protecția informațiilor personale și a informațiilor de drept privat; să gestioneze datele despre procesul de formare și rezultatele care includ adesea informații sensibile; să urmeze și să furnizeze sfaturile generale care facilitează respectarea bunelor practici de igienă digitală.

Unitatea 4 – Exemplu de bună practică – Igienă digitală pentru VET

Să parcurgem un exemplu de bună practică despre modul în care igiena digitală poate fi introdusă în instituția VET pentru siguranța instituției și pentru utilizarea de către profesorii și cursanții care participă la instruire.

Descrierea situației

O instituție de învățământ profesional și tehnic dorește să ofere formare online pentru cursanților săi pentru a evita călătoriile costisitoare și consumatoare de timp și pentru a oferi cursanților confortul de a participa la formare din propriul mediu fizic sigur. Instituția VET are un personal de formatori interni și externi care au diferite experiențe anterioare în furnizarea de instruire online și pot avea cunoștințe și competențe diferite legate de desfășurarea unei astfel de instruiri. Instituția are, de asemenea, angajați interni care desfășoară activități administrative legate de formare și care gestionează informații care sunt uneori sensibile și care ar trebui să fie reglementate de normele și orientările de conformitate. De obicei, profesorii vor trebui să utilizeze platforma Microsoft Teams pentru desfășurarea instruirii, partajarea materialelor de instruire și comunicarea cu cursanții, în timp ce personalul de asistență internă va folosi Microsoft Teams și e-mailul pentru gestionarea cursanților înainte, în timpul și după instruire și un tip de sistem de stocare a documentelor pentru gestionarea și partajarea materialelor de instruire.

Lucrurile care preocupă instituția VET sunt:

- manipularea necorespunzătoare a informațiilor cu caracter personal de către oricare dintre participanții la formare,
- utilizarea atentă a informațiilor de drept privat ale instituției și ale partenerilor externi,
- limitarea accesului la formare numai pentru publicul vizat;
- oferirea unei experiențe bogate cursanților,
- păstrarea unui anumit nivel de reputație ca un bun furnizor de servicii de formare pe piață.

Să vedem cum pot fi abordate problemele de igienă digitală în această situație.

Soluția

Acest tip de situație este complex și necesită acordarea atenției mai multor aspecte legate de igiena digitală:

- organizarea configurării platformei Microsoft Teams și gestionarea utilizatorilor în timpul instruirii,
- formarea profesorilor care conduc instruirea;
- desfășurarea sesiunilor de formare propriu-zise cu implicarea cursanților și a profesorilor,
- manipularea resurselor educaționale utilizate în timpul instruirii;

- organizarea comunicării între profesori și cursanți, dar și între cursanți,
- efectuarea de evaluări ale instruirii și colectarea de feedback.

Urmează o descriere mai detaliată a bunelor practici pentru fiecare dintre aceste aspecte.

Gestionarea configurării și conectării

Teams For Education: A fost creată a platformă Teams separată de platforma Teams utilizată pentru comunicarea zilnică și schimbul de cunoștințe de către angajații instituției VET. Microsoft Teams for Education este disponibil pentru acele instituții VET care îndeplinesc cerințele instituțiilor educaționale oficiale și oferă caracteristici suplimentare care sunt benefice pentru desfășurarea instruirii.

Single Sign-On (SSO): Implementarea SSO utilizând o platformă comună de autentificare (cum ar fi Active Directory) a fost efectuată pentru a simplifica accesul la Microsoft Teams, aplicațiile utilizate în mediul Microsoft Teams și alte instrumente utilizate central și cu aprobarea instituției VET în timpul instruirii.

Control acces bazat pe roluri: Au fost atribuite roluri și permisiuni în cadrul echipelor pe baza poziției utilizatorului. Mai exact, au fost atribuite 4 roluri, fiecare cu privilegiile sale pe platforma Teams: administrator de sistem, administrator de instruire (persoana care organizează sesiuni de instruire înainte de instruire și analizează rezultatele instruirii după aceea), profesor/ formator (persoana care conduce instruirea și sarcinile practice și gestionează materialele de instruire în timpul instruirii) și elev/ student, asigurând accesul adecvat la funcții și informații.

Practici de autentificare securizată: Dacă este cazul, utilizatorii cărora li s-au atribuit privilegii mai mari atunci când accesează informații sensibile au fost instruiți să utilizeze autentificarea multi-factor (MFA) și parole puternice pentru a spori securitatea.

Instruirea profesorilor

Ateliere de instruire Microsoft Teams: Au fost planificate și desfășurate ateliere dedicate profesorilor cu privire la modul de utilizare eficientă a Microsoft Teams, iar profesorii interni și externi au fost invitați să participe la primirea instrucțiunilor pentru conduita sigură în mediul Teams. Instruirea a inclus crearea și gestionarea echipelor și a canalelor, programarea întâlnirilor și utilizarea funcțiilor de colaborare, cum ar fi fișierele partajate și chatul.

Instruire pentru funcții avansate: Instruire suplimentară privind funcțiile avansate, cum ar fi sălile de lucru virtuale, evenimentele live și integrarea aplicațiilor terțe care pot îmbunătăți experiența de instruire, a fost oferită profesorilor și a fost oferită șansa de a practica aceste caracteristici ca sarcini practice în timpul instruirii.

Suport continuu: Pentru acei profesori care aveau nevoie de sediu, le-au fost oferite săli de curs fizice complet organizate, cu conexiuni sigure la internet. Pentru acei formatori care intenționau să utilizeze spațiile lor, au fost furnizate ghiduri pentru desfășurarea în siguranță a instruirii. Au fost stabilite informațiile de contact ale personalului dedicat asistenței IT pentru a ajuta profesorii în caz de probleme tehnice.

Desfășurarea sesiunilor de instruire

Planificarea sesiunii: Administratorii și profesorii interni au fost instruiți în utilizarea unui calendar pentru a programa sesiuni, a seta remindere și a furniza o agendă în avans în invitația la întâlnire. Au fost create invitații automate pentru cursanți pentru a minimiza riscurile de a se alătura sesiunilor de formare greșite.

Caracteristici interactive: Toți profesorii au fost sfătuiți să utilizeze caracteristicile suplimentare ale aplicației Teams, cum ar fi sondaje, chestionare și table digitale în timpul sesiunilor, pentru a implica cursanții și a îmbunătăți învățarea ori de câte ori este posibil. Utilizarea instrumentelor și funcțiilor suplimentare a fost permisă, dar profesorii au fost sfătuiți să ghideze cursanții atunci când le folosesc pentru informații suplimentare sau sarcini practice.

Sesiuni de înregistrare: Înregistrarea sesiunilor de instruire a fost sever limitată din cauza GDPR și efectuată numai cu acordul explicit al tuturor cursanților. La crearea înregistrărilor au fost stocate în siguranță și accesibile numai celor care au participat la sesiunile de instruire și numai pentru o perioadă limitată de timp. Deși înregistrările, în general, sunt considerate benefice pentru cursanți atunci când revizuiesc conținutul instruirii mai târziu, o organizație VET ar trebui să fie conștientă de riscurile legate de acestea.

Camere de discuții virtuale (Breakout Rooms): Camerele de discuții virtuale pentru activități de grup sau discuții au fost create de administratorul instruirii, s-au acordat drepturi de acces și s-a efectuat instruirea corespunzătoare a profesorilor, permițându-le acestora să treacă de la o cameră la alta pentru a ghida și monitoriza progresul instruirii.

Manipularea materialelor de instruire

Partajarea fișierelor și a resurselor: Toate materialele de instruire care au fost utilizate în timpul instruirii au fost stocate pe servere securizate. Cheile electronice ale materialelor de instruire sau copiile efective ale materialelor de instruire au fost gestionate de un administrator de instruire dedicat. Pentru materiale mai puțin sensibile, a fost folosit mediul Teams în sine.

Editare colaborativă: Atunci când colaborează la documente sau prezentări în timp real, în timpul sarcinilor practice, profesorii și cursanții au fost sfătuiți să utilizeze software oficial, cum ar fi integrarea Office 365, și să fie atenți la schimbul excesiv de informații.

Controlul versiunii: Controlul versiunilor documentelor interne care fac parte din materialele de instruire a fost introdus în cadrul organizației VET. Toți profesorii au fost sfătuiți să-și asume rolul de experți pentru materialele de instruire externe și au fost încurajați să consulte administratorii interni de formare pentru versiuni ale materialelor de instruire, ghiduri pentru cursanți și teste practice, acolo unde este cazul, pentru a reduce daunele aduse reputației organizației VET pentru că nu furnizează versiuni actualizate ale materialelor de instruire.

Comunicarea dintre cursanți și profesori

Actualizări regulate: Chat-ul Teams a fost utilizat pentru a face anunțuri, a partaja actualizări și a oferi feedback cu privire la sesiunile de instruire.

Canale dedicate: Au fost create canale pentru sesiuni specifice de formare și grupuri individuale de cursanți, facilitând discuțiile concentrate și schimbul de resurse.

Chat-uri private: Chat-urile private suplimentare între formator și cursanți au fost limitate doar la situațiile în care ambele părți au fost de acord cu o comunicare suplimentară, organizând schimbul de informații de contact la nivel central.

Evaluare și feedback

Formulare de feedback: Utilizarea Chestionarelor Microsoft sau a software-ului dedicat dezvoltat intern de instituția VET pentru a colecta feedback cu privire la sesiunile de instruire a fost impusă. Linkurile către software-ul utilizat pentru feedback au fost distribuite prin intermediul mediului Teams, asigurându-se că numai publicul vizat poate participa la feedback. Accesul la informațiile furnizate în formularele de feedback a fost limitat la administratorii interni de formare ai organizației VET.

Urmărirea performanței: Au fost utilizate funcțiile de evaluare din cadrul Teams pentru a oferi sarcini, a colecta munca și a oferi feedback notat.

Această configurare atât a mediului tehnic, cât și a procedurilor și rolurilor implicate în proces asigură un mediu de instruire cuprinzător, sigur și interactiv utilizând Microsoft Teams, satisfăcând atât nevoile profesorilor, cât și ale cursanților, menținând în același timp un standard ridicat de igienă și eficiență digitală.

Referințe

1. Vuorikari, R., Kluzer, S. și Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens, EUR 31006 EN, Oficiul pentru Publicații al Uniunii Europene, Luxemburg, 2022, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.
2. Cadrul european al competențelor digitale, https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf, [accesat la 15 aprilie 2024].
3. Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA). Profiluri de rol în cadrul competențelor europene în materie de securitate cibernetică, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles [accesat la 15 aprilie 2024].
4. Punie, Y., editor(i), Redecker, C., European Framework for the Digital Competence of Educators: DigCompEdu, EUR 28775 EN, Oficiul pentru Publicații al Uniunii Europene, Luxemburg, 2017, ISBN 978-92-79-73718-3 (print),978-92-79-73494-6 (pdf), doi:10.2760/178382 (print),10.2760/159770 (online), JRC107466.
5. Forumul Economic Mondial, "Raportul privind viitorul locurilor de muncă 2023", https://www.weforum.org/publications/the-future-of-jobs-report-2023/
6. Chui, M., Issler, M., Roberts, R., Yee, L. "McKinsey Technology Trends Outlook 2023", https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#new-and-notable
7. Foaie de înșelăciune digitală de igienă. https://digitalhygiene.net/ [accesat la 15 aprilie 2024].

Modulul 2 - Curriculum personalizat de igienă digitală pentru instituțiile VET

Introducere

Igiena digitală ocupă un rol mult mai mare și mai semnificativ în viața noastră de zi cu zi. Odată cu creșterea rapidă a digitalizării și extinderea acesteia în toate sferele activității umane, a apărut o nevoie urgentă de a ne asigura că mediile noastre digitale sunt sigure. Una dintre garanțiile primare și fundamentale în acest sens este asigurarea unei igiene digitale adecvate. Acest lucru este valabil mai ales având în vedere amenințările cibernetice în creștere cu care se confruntă instituțiile. Igiena digitală se concentrează în primul rând pe menținerea unei prezențe digitale sănătoase și sigure, iar acest lucru a devenit din ce în ce mai necesar pe măsură ce tot mai multe organizații își mută activitățile online. Acest modul este conceput pentru a oferi un curriculum complex care poate instrui cursanții la nivel profesional pentru a dezvolta, evalua și menține bune practici de igienă digitală.

Parcurgerea acestui program va permite cursantului să dobândească abilitățile analitice și practice de bază necesare pentru a evalua, menține și interveni eficient acolo unde este necesar pentru a asigura igiena digitală într-un cadru instituțional. Acesta este un program cu adevărat relevant datorită cererii ridicate de pe piață pentru profesioniștii cu abilități în acest domeniu. Prezentul program de dezvoltare a fost comparat cu cele mai bune practici din acest domeniu. În prim planul programului sunt startup-urile și profesioniștii din IMM-uri, în funcție de care au fost alese modulele și a structura. Scopul este de a construi competențe la nivelul menționat, ceea ce înseamnă că programul este conceput și structurat pentru a fi accesibil celor care doresc să-l parcurgă în întregime sau parțial. Programul este, de asemenea, conceput pentru a fi practic, cu un timp scurt de finalizare. Cu toate acestea, este, de asemenea, conceput pentru a permite cursanților să îl parcurgă în ritm propriu.

Unitatea 1 – Prezentare generală a curriculumului

Acest handbook a fost creat pentru a oferi cursanților înscriși în prezent sau care urmează să se înscrie în programul de educație și formare profesională (VET) în domeniul igienei digitale, precum și profesorilor, informații relevante cu privire la scopul, planificarea, structura și evaluarea programului. Recunoscând că nu toate instituțiile sunt la fel și necesită același nivel de competențe de igienă digitală, acest modul și diferitele părți sunt modulare în structură. Acest lucru permite persoanelor care sunt competente în anumite domenii

să se concentreze sau să treacă la alte module pe măsură ce nevoile lor evoluează. Scopul final al acestui program este de a crea o bază solidă în igiena digitală, împuternicind atât cursanții, cât și profesorii să gestioneze și să diminueze eficient riscurile cibernetice. Acest curriculum este, de asemenea, conceput pentru a acoperi părți substanțiale ale certificărilor profesionale de securitate cibernetică la nivel de bază, cum ar fi GIAC Security Essentials (GSEC) și CompTIA Security +. Prin urmare, oferă valoare adăugată și un stimulent sporit pentru cursanți să participe la acest program.

Scopul programului și obiectivele modulului

Obiectivele principale ale modulului de igienă digitală sunt concepute pentru a îmbunătăți politica de securitate cibernetică a instituțiilor, permițând participanților:

- Să evalueze amenințările la adresa securității cibernetice cu care se confruntă organizațiile.
- Să evalueze și să implementeze securitatea de bază a rețelei.
- Să știe cum să implementeze și să mențină protocoalele de criptare de bază.
- Să evalueze și să implementeze protocoalele de gestionare și securitate a datelor.
- Să evalueze și să aplice protocoale de securitate hardware și software de bază.
- Să gestionezei securitatea în mediul mobil.

Metodologia predării

Programul folosește un amestec de instruire teoretică și aplicație practică. Acesta utilizează studii de caz, sesiuni practice de laborator și ateliere interactive pentru a se asigura că cursanții pot aplica conceptele pe care le învață în scenarii din lumea reală. Această abordare nu numai că îmbunătățește înțelegerea, ci și asigură că absolvenții sunt pregătiți pentru viitoare locuri de muncă și capabili să implementeze practici cuprinzătoare de igienă digitală imediat după finalizarea programului.

Evaluare și îmbunătățire continuă

Evaluarea în cadrul programului de igienă digitală este atât riguroasă, cât și continuă, utilizând o varietate de metode pentru a evalua cunoștințele și abilitățile participanților. Acestea includ chestionare, examene practice, evaluări bazate pe proiecte și un proiect final care încapsulează întreaga învățare a participanților. Mecanismele de feedback sunt parte integrantă a curriculum-ului, oferind participanților informații în timp util despre progresul lor și domeniile de îmbunătățire. În plus, curriculum-ul în sine este actualizat periodic pentru a se alinia la cele mai recente informații despre amenințările cibernetice și progresele tehnologice, asigurând relevanța și eficacitatea în abordarea provocărilor contemporane de securitate cibernetică.

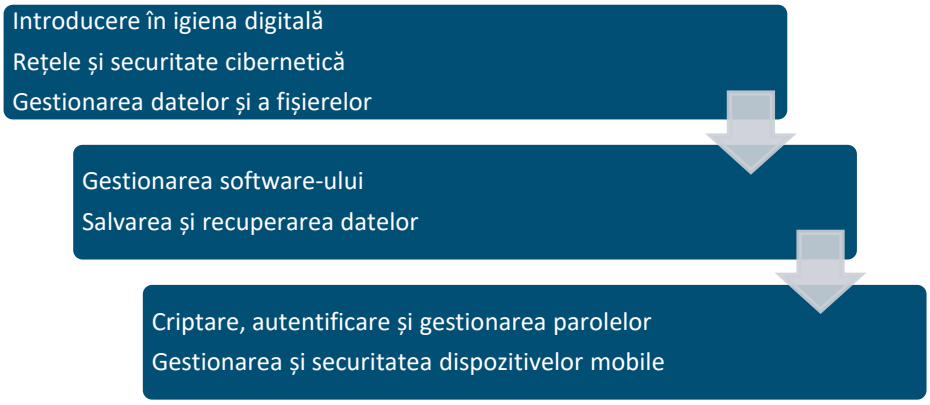
Concluzie

Programul de igienă digitală pentru instituțiile VET este conceput nu doar pentru a împărtăși cunoștințe și competențe esențiale de securitate cibernetică, ci și pentru a insufla participanților o cultură proactivă și informată a securității cibernetice. La finalul programului, participanții nu sunt doar absolvenți, ci sunt cetățeni digitali informați, echipați să contribuie semnificativ la apărarea securității cibernetice a organizațiilor lor. Acest program cuprinzător este o piatră de temelie în pregătirea următoarei generații de profesioniști în domeniul securității cibernetice, gata să abordeze provocările dinamice ale erei digitale.

Unitatea 2 – Domenii cheie de învățare

Gestionarea și securitatea dispozitivelor mobile

Cod	Arii de învățare/ subiecte
D21	Introducere în igiena digitală
D22	Rețele și securitate cibernetică
D23	Gestionarea datelor și a fișierelor
D24	Gestionarea software-ului
D25	Salvarea și recuperarea datelor
D26	Criptare, autentificare și gestionarea parolelor
D27	Gestionarea și securitatea dispozitivelor mobile



Introducere în igiena digitală

Acest subiect este conceput pentru a oferi cursanților o imagine de ansamblu cuprinzătoare asupra igienei digitale. Această prezentare generală va oferi atât o imagine de ansamblu conceptuală a conținutului, cât și unele dintre aplicațiile practice atunci când programul este vizualizat dintr-o perspectivă integrativă. Accentul principal va fi pus pe introducerea diferitelor domenii ale igienei digitale și a modului în care diferitele domenii sunt legate între ele. Acesta va oferi o imagine de ansamblu preliminară a principiilor și practicilor de bază ale igienei digitale și a modului în care diferitele componente se potrivesc împreună. Această unitate oferă cunoștințele fundamentale și înțelegerea pe care pot fi construite celelalte zone componente.

Principalele teme abordate cu privire la acest subiect

- Înțelegerea igienei digitale: O explorare a ceea ce constituie igiena digitală și de ce este esențială în era digitală de astăzi.

- Elemente esențiale pentru igiena digitală: Practici și protocoale de bază care asigură integritatea și securitatea datelor și sistemelor.
- Implicațiile de securitate ale igienei digitale: O privire detaliată asupra modului în care igiena digitală eficientă poate atenua diverse amenințări cibernetice.
- Bazele implementării igienei digitale: Pași practici pentru instituirea măsurilor de igienă digitală în contexte personale și organizaționale.
- Conformitatea în materie de securitate cibernetică: o prezentare generală a politicilor, reglementărilor și cerințelor de conformitate de bază la nivel național și la nivelul UE privind securitatea cibernetică.

Rezultatele învățării subiectului

După învățarea acestui subiect, cursanții vor putea:

- Defini igiena digitală și înțelege componentele sale critice.
- Identifica potențialele amenințări cibernetice și înțelege rolul igienei digitale în protejarea împotriva acestor amenințări.
- Implementa practici de igienă digitală de bază pe diferite platforme și dispozitive.
- Comunica importanța igienei digitale colegilor și superiorilor, pledând pentru cele mai bune practici în cadrul organizațiilor lor.
- Înțelege cerințele de bază privind conformitatea cu securitatea cibernetică

Metode de predare

Un mix de prelegeri, ateliere interactive și studii de caz vor fi folosite pentru a oferi elevilor o experiență robustă de învățare. Fiecare sesiune își propune să echilibreze cunoștințele teoretice cu aplicațiile practice, asigurându-se că cursanții pot traduce ceea ce învață în strategii acționabile la locurile lor de muncă.

Literatură recomandată

- Brooks, C.J., Grow, C., Craig, P., Short, D., (2018), Cybersecurity Essentials.
    - Această carte oferă o introducere completă în domeniul securității cibernetice și este deosebit de utilă pentru certificările de securitate cibernetică la nivel de început.
- Paula, D., Cruz, M., (2023), Cybersecurity Essentials Made Easy: A No-Nonsense Guide to Cyber Security for Beginners.
    - Această carte este o lectură esențială pentru înțelegerea provocărilor legate de securitatea cibernetică și a modului de diminuare a acestora. Este deosebit de relevantă pentru proprietarii de IMM-uri nou înființate și pentru cursanții care doresc să înțeleagă siguranța online.
- Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
    - Această resursă oferă o imagine de ansamblu accesibilă a conceptelor și provocărilor cheie din domeniul securității cibernetice, fiind o resursă excelentă pentru cursanții care își încep călătoria în înțelegerea amenințărilor cibernetice și a mecanismelor de protecție.
- Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
    - Cartea lui Bruce Schneier este esențială pentru înțelegerea domeniului confidențialității și securității datelor, oferind informații despre modul în care sunt colectate și utilizate datele personale și despre importanța practicilor solide de gestionare a datelor.

Aceste resurse sunt selectate pentru a oferi cunoștințe teoretice și competențe practice în domeniul rețelelor și securității cibernetice, sprijinind curriculum-ul și îmbunătățind experiența educațională a cursanților VET în igiena digitală.

Rețele și securitate cibernetică

Acest subiect are rolul de a le oferi cursanților competențele necesare pentru a identifica, evalua și neutraliza amenințările la adresa rețelelor. Una dintre provocările cheie cu care se confruntă organizațiile în mediile de operare actuale este asigurarea securității rețelelor. Deoarece majoritatea rețelelor sunt conectate la Internet, acestea sunt adesea expuse unor actori răuvoitori care pot încerca să exploateze vulnerabilitățile rețelei pentru a accesa rețeaua într-un mod neautorizat. Pentru a realiza acest lucru, cursanții vor fi instruiți în concepte cheie legate de rețele, protocoale comune, porturi, LAN, WAN și sisteme cloud.

Principalele teme abordate cu privire la acest subiect

- Introducere în securitatea cibernetică
- Analiza vulnerabilităților
- Evaluarea amenințărilor și a riscurilor
- Protocoale de securitate a rețelei – firewall-uri, antivirus
- Atacuri comune de securitate cibernetică
- Instrumente comune de securitate cibernetică
- Etica în securitatea cibernetică

Rezultatele învățării

- Identificarea conceptelor cheie de rețea: Cursanții vor putea descrie aspectele fundamentale ale rețelelor, inclusiv sistemele LAN, WAN și cloud și vor înțelege rolurile lor în infrastructura organizațională.
- Evaluarea vulnerabilităților rețelei: Cursanții vor dobândi abilitățile de a efectua analize de vulnerabilitate pe diferite sisteme de rețea pentru a identifica potențialele slăbiciuni de securitate.
- Implementarea măsurilor de securitate: Cursanții vor fi competenți în configurarea și gestionarea protocoalelor de securitate a rețelei, cum ar fi firewall-urile și sistemele antivirus, pentru a proteja împotriva amenințărilor cibernetice.
- Efectuarea de evaluări ale amenințărilor și riscurilor: Dotarea cursanților cu capacitatea de a evalua și prioritiza riscurile asociate amenințărilor la adresa securității cibernetice a sistemelor de rețea.
- Înțelegerea implicațiilor etice: Cursanții vor explora considerentele etice în securitatea cibernetică, înțelegând responsabilitățile protejării datelor și sistemelor împotriva accesului neautorizat.

Metode de predare

- Prelegeri interactive: Axate pe introducerea conceptelor fundamentale și avansate de rețea, a protocoalelor de securitate și a problemelor etice în securitatea cibernetică.
- Laboratoare practice: Sesiuni practice în laboratoarele de calculatoare unde cursanții pot utiliza medii de rețea reale și simulări pentru a aplica măsuri și instrumente de securitate.

- Analiza studiului de caz: Discuții și analize ale incidentelor de securitate cibernetică din lumea reală pentru a înțelege mecanismele de amenințare și contramăsurile eficiente.
- Proiecte de grup: Echipele de cursanți vor evalua o configurare ipotetică a rețelei pentru vulnerabilități și vor propune o strategie cuprinzătoare de securitate.
- Sesiuni prezentatori/ lectori invitați: Profesioniștii din domeniul securității cibernetice sunt invitați să împărtășească perspective și experiențe, subliniind provocările actuale și tehnologiile emergente.

Literatură recomandată

- Stewart, J. M., Chapple, M., & Gibson, D. (2020). *CompTIA Security+ Guide to Network Security Fundamentals* (7th ed.). Cengage Learning.
    - Acest ghid acoperă o gamă largă de subiecte fundamentale în securitatea rețelelor, potrivite pentru cursanții care își încep călătoria în securitatea cibernetică.
- Marsh, N., (2023), Cybersecurity: A Fat-Free Guide to Network Security Best Practices (Fat-Free Technology Guides).
    - Această carte oferă o perspectivă cuprinzătoare asupra amenințărilor cibernetice și a problemelor critice de securitate a rețelelor.
- Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.
    - O resursă cuprinzătoare care oferă o privire aprofundată asupra principiilor de securitate a informațiilor, inclusiv discuții detaliate privind analiza vulnerabilității, amenințarea și evaluarea riscurilor.
- Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson.
    - Textul lui Stallings oferă o acoperire cuprinzătoare a protocoalelor și standardelor de securitate a rețelelor, fiind ideal pentru cursanții care au nevoie de o înțelegere detaliată a aspectelor tehnice ale securizării rețelelor.
- Computer & Internet Security: A Hands-on Approach 3rd ed. Edition by Wenliang Du

Aceste resurse academice vor sprijini curriculumul prin furnizarea atât a cadrelor teoretice, cât și a perspectivelor practice în gestionarea și securizarea mediilor de rețea, aliniindu-se la rezultatele învățării și strategiile de predare descrise.

Gestionarea datelor și a fișierelor

Datele, așa cum am menționat anterior, reprezintă unul dintre cele mai valoroase resurse pe care le dețin instituțiile. În consecință, gestionarea acestor resurse a preluat un rol din ce în ce mai important în cadrul instituției. Acest lucru este deosebit de important din cauza creșterii preocupărilor legate de securitate în mediul cibernetic. Gestionarea corectă a datelor a devenit esențială pentru o securitate cibernetică eficientă, în special în captarea, organizarea și diseminarea informațiilor sensibile. Gestionarea datelor se referă la principiile și practicile aplicate în gestionarea și protecția datelor. În contextul securității cibernetice, gestionarea datelor se referă, de asemenea, la protecția datelor împotriva accesului, modificării și transmiterii neautorizate. În mediul actual, în care se colectează, se analizează și se diseminează volume uriașe de date, aspectele legate de gestionarea securității au câștigat în importanță. Prin urmare, există o cerere crescută de profesioniști care sunt competenți în gestionarea datelor.

Principalele teme abordate cu privire la acest subiect

- Guvernanța datelor
- Clasificarea datelor
- Criptarea în gestionarea datelor
- Monitorizarea și auditul datelor
- Backup și recuperare de date
- Integritatea și confidențialitatea datelor
- Controale de acces și autentificare

Rezultatele învățării

- Înțelegerea guvernanței datelor: Cursanții vor înțelege conceptele fundamentale ale guvernanței datelor și rolul acesteia în contextul organizațional.
- Clasificarea datele: Cursanții vor putea clasifica datele pe baza sensibilității și importanței, aplicând măsuri de securitate adecvate diferitelor tipuri de date.
- Implementarea criptării datelor: Cursanții vor înțelege și vor aplica tehnici de criptare pentru a proteja integritatea și confidențialitatea datelor în timpul stocării și transmiterii.
- Efectuarea de audituri de date: Dotarea cursanților cu competențele de a efectua monitorizări regulate ale datelor și audituri pentru a asigura respectarea politicilor și reglementărilor de securitate.
- Gestionarea recuperării datelor: Cursanții vor învăța strategii de backup și recuperare a datelor pentru a asigura disponibilitatea și continuitatea datelor în caz de pierdere a datelor sau defecțiuni ale sistemului.
- Asigurarea integrității și confidențialității datelor: Cursanții vor înțelege metodele de menținere a integrității datelor și de gestionare a setărilor de confidențialitate pentru a proteja datele utilizatorilor împotriva accesului neautorizat.
- Aplicarea controale de acces: Cursanții vor fi capabili să implementeze controale robuste de acces și metode de autentificare pentru a proteja accesul la date.

Literatură recomandată

- Ladley J., (2019)., Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program 2nd Edition.
    - Această carte oferă o viziune cuprinzătoare asupra guvernanței și securității datelor.
- Talabis, M., & Martin, J. (2015). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Syngress.
    - Această carte oferă instrumente și tehnici practice pentru evaluarea riscurilor de securitate a informațiilor, inclusiv a celor asociate cu gestionarea datelor.
- Bertino, E., & Sandhu, R. (2017). Data Privacy and Security. Springer.
    - O prezentare cuprinzătoare a confidențialității datelor și a tehnicilor de securitate, acest text este esențial pentru înțelegerea complexității protejării datelor sensibile în diverse medii.
- Swanson, M., & Guttman, B. (2016). Generally Accepted Principles and Practices for Securing Information Technology Systems. National Institute of Standards and Technology.
    - Această publicație guvernamentală oferă orientări și bune practici pentru securizarea sistemelor informatice, inclusiv secțiuni detaliate privind gestionarea datelor și controalele de securitate.

Aceste resurse academice vor îmbunătăți cadrul educațional prin furnizarea de cunoștințe teoretice și exemple practice de aplicare, permițând cursanților să devină competenți în gestionarea și securizarea eficientă a datelor organizaționale.

Gestionarea software-ului

Gestionarea software-ului este un element crucial al securității cibernetice. Gestionarea software-ului include procesul sistematic de planificare, implementare, monitorizare și mentenanță a software-ului pe tot parcursul ciclului său de viață. Aceasta cuprinde sarcini precum controlul versiunilor, gestionarea patch-urilor, licențierea și actualizările de securitate. Gestionarea eficientă a software-ului asigură performanță optimă, securitate și conformitate, minimizând în același timp riscurile și vulnerabilitățile. Organizațiile moderne se confruntă cu diverse provocări în ceea ce privește securitatea software-ului, cum ar fi politicile slabe privind parolele, vulnerabilitățile nesigure API fără patch-uri, phishingul și încălcările datelor, pentru a numi câteva. Prin urmare, este imperativ să aibă personal instruit care să fie pregătit pentru a gestiona eficient software-ul organizației și pentru a preveni breșele de securitate software. Acest modul va oferi cursanților cunoștințe practice de bază despre cum să gestioneze eficient software-ul organizației și să minimizeze riscul unei încălcări a securității.

Principalele teme abordate cu privire la acest subiect

- Securitatea aplicațiilor
- Testare și audit software
- Gestionarea accesului și privilegiilor utilizatorilor
- Implementarea protocoalelor de actualizare periodică
- Măsuri de securitate la nivel de puncte finale din rețea

Rezultatele învățării

- Stăpânirea securității aplicațiilor: Cursanții vor înțelege fundamentele securizării aplicațiilor de la proiectare la implementare, inclusiv vulnerabilitățile comune și strategiile de atenuare.
- Efectuarea testării și auditul software-ului: Cursanții vor dobândi competențe în diferite metode de testare și audit software pentru a identifica și rezolva problemele de securitate.
- Gestionarea accesului utilizatorilor: Cursanții vor învăța să gestioneze eficient accesul și privilegiile utilizatorilor pentru a se asigura că numai utilizatorii autorizați au acces la resursele software critice.
- Implementarea protocoale de actualizare: Echiparea cursanților cu cunoștințele necesare pentru a stabili și menține protocoale regulate de actualizare a software-ului pentru a atenua vulnerabilitățile.
- Îmbunătățirea securității punctelor finale: Cursanții vor înțelege măsurile de securitate ale punctelor finale pentru a proteja infrastructura organizațională de amenințări precum malware și ransomware.

Literatură recomandată

- Du, W., (2022), Computer Security: A hands-on approach, 3rd edition.
    - Această carte investighează managementul software-ului, vulnerabilitățile și activitățile de atenuare.

- Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). Software Security Engineering: A Guide for Project Managers. Addison-Wesley Professional.
    - Această carte oferă un ghid cuprinzător pentru integrarea practicilor de securitate în dezvoltarea de software, făcând-o esențială pentru înțelegerea securității aplicațiilor și a gestionării ciclului de viață.
- Anton, A. I., & Earp, J. B. (2004). A Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. Academy of Management Review.
    - Oferă informații despre gestionarea accesului și privilegiilor utilizatorilor prin identificarea părților interesate cheie și a nevoilor acestora, esențiale pentru gestionarea eficientă a software-ului.
- Lindqvist, U., & Neumann, P. G. (2017). The Future of Cybersecurity: Challenges and Opportunities. IEEE Security & Privacy.
    - Acest articol discută provocările și oportunitățile viitoare în domeniul securității cibernetice, inclusiv importanța actualizărilor continue de software și a măsurilor de securitate la nivel de punct final.

Aceste resurse vor sprijini programul de studiu prin furnizarea unei baze teoretice solide și a unor perspective practice asupra gestionării software-ului, asigurându-se că participanții la formare sunt bine pregătiți pentru a face față provocărilor legate de securitatea software-ului în mediile organizaționale moderne.

Salvarea și recuperarea datelor

Această secțiune este concepută pentru a oferi cursanților o înțelegere globală a procesului de salvare și recuperare a datelor și a modului în care acesta poate fi implementat. Toate organizațiile moderne trebuie să aibă politici, protocoale și sisteme adecvate de backup și recuperare. Majoritatea organizațiilor actuale sunt bazate pe date și, prin urmare, acordă o importanță deosebită gestionării datelor și resurselor lor informaționale. În principiu, majoritatea organizațiilor, în special IMM-urile, își stochează datele într-o bază de date locală sau cloud centralizată. Sistemele bazate pe cloud au devenit mai avansate și mai sigure, cu controale de gestionare foarte sofisticate, făcându-le mai puțin susceptibile la problemele tradiționale de distrugere a sistemelor fizice de stocare. Cu toate acestea, ele sunt încă susceptibile la erori umane, configurare greșită și încălcări ale datelor, prin urmare este important ca personalul IT care supraveghează astfel de sisteme să fie familiarizat cu tehnologiile, protocoalele și procesele implicate. Secțiunea este concepută pentru a oferi aceste cunoștințe cursanților.

Principalele teme abordate cu privire la acest subiect

- Gestionarea fișierelor
- Protocoale de backup/ salvare și recuperare
- Tipuri de copii de rezervă (back-up)
- Servicii și dispozitive de salvare

Rezultatele învățării

- Înțelegerea modului de gestionare a fișierelor: Cursanții vor învăța principiile gestionării eficiente a fișierelor, cruciale pentru organizarea datelor în scopuri de rezervă.

- Protocoale principale de salvare și recuperare: Cursanții vor înțelege diferite protocoale de salvare (backup) și recuperare și cum să le aplice eficient în diferite scenarii.
- Identificarea tipurilor de back-up: Cursanții vor putea distinge între diferite tipuri de copii de rezervă (complete, incrementale, diferențiale) și vor decide care este cel mai potrivit pentru situații specifice.
- Utilizarea serviciilor și dispozitivelor de salvare: Cursanții vor dobândi cunoștințe despre diverse servicii și dispozitive de salvare (backup), inclusiv soluții de stocare bazate pe cloud și locale și cum să le implementeze în siguranță.
- Atenuarea riscurilor de pierdere a datelor: ursanții vor înțelege cum să planifice și să execute o strategie de recuperare a datelor pentru a minimiza timpul de nefuncționare și pierderea datelor în cazul încălcării securității datelor sau distrugerea datelor.

Literatură recomandată

- Preston, W., (2021), Modern Data Protection: Ensuring Recoverability of All Modern Workloads.
    - Această carte se referă la protecția modernă a datelor și la modul în care aceasta este integrată în securitatea generală hardware și software.
- Data Backup And Recovery A Complete Guide - 2023 Edition
- Toigo, J. W. (2009). Disaster Recovery Planning: Preparing for the Unthinkable (3rd ed.). Prentice Hall.
    - Oferă informații cuprinzătoare despre planificarea recuperării în caz de dezastru, inclusiv discuții detaliate despre strategiile de rezervă ca o componentă critică a recuperării în caz de dezastru.
- Duffy, D. (2014). Cloud Computing: Strategies for Cloud Computing Adoption. Faithful Pen Publishing
    - Discută adoptarea cloud computing, concentrându-se pe serviciile de backup bazate pe cloud și considerentele de securitate asociate acestora.

Aceste resurse academice vor susține curriculum-ul, oferind cursanților atât o înțelegere fundamentală, cât și abilități practice în gestionarea și implementarea strategiilor de salvare (backup) și recuperare a datelor, esențiale pentru minimizarea pierderilor potențiale de date în mediile organizaționale moderne.

Criptare, autentificare și gestionarea parolelor

Datele și informațiile au devenit unul dintre cele mai importante resurse organizaționale și, în multe cazuri, reprezintă principalul factor determinant din spatele evaluării unei companii. Natura crucială a acestor resurse face imperativ ca acestea să fie tratate cu cea mai mare atenție. Unul dintre instrumentele cheie pentru protejarea resurselor de date și informații este criptografia. Criptografia este esențială pentru securitatea cibernetică, deoarece este esențială pentru protecția datelor și informațiilor sensibile și pentru comunicațiile securizate. Permite protocoale robuste de autentificare și gestionarea parolelor. Criptografia permite implementarea corectă a sistemelor de autentificare, care asigură confidențialitatea, integritatea și disponibilitatea datelor și informațiilor organizaționale pentru membrul corespunzător al personalului.

Principalele teme abordate cu privire la acest subiect

- Bazele criptografiei
- Criptare integrală
- Standarde de criptare
- Autentificare multifactor
- Managementul cheilor

- Selectarea celor mai bune standarde pentru organizație
- Cele mai bune practici în implementarea tehnologiilor de criptare

Rezultatele învățării

- Înțelegerea elementele de bază ale criptografiei: Cursanții vor învăța principiile fundamentale ale criptografiei, inclusiv istoria, scopul și mecanismele cheie.
- Implementarea criptografiei end-to-end: Cursanții vor dobândi abilități în configurarea și gestionarea criptării end-to-end pentru a securiza comunicațiile.
- Aplicarea standardelor de criptare: Cursanții vor fi familiarizați cu diferite standarde de criptare și vor învăța cum să le aplice în funcție de nevoile organizaționale.
- Utilizarea autentificării multifactoriale: Cursanții vor dobândi capacitatea de a implementa și gestiona sistemele de autentificare multifactor pentru a spori securitatea.
- Gestionarea cheilor criptografice: Cursanții vor înțelege procesele cheie de gestionare și cele mai bune practici pentru a asigura securitatea și integritatea cheilor criptografice.
- Selectarea și implementarea tehnologiilor de criptare: Cursanții vor învăța cum să selecteze tehnologii de criptare adecvate pentru afacerea lor și cele mai bune practici pentru implementare pentru a proteja datele în mod eficient.

Literatură recomandată

- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
    - Acest manual oferă o introducere cuprinzătoare în domeniul criptografiei și securității rețelelor, inclusiv acoperirea detaliată a tehnologiilor de criptare și a protocoalelor de autentificare.
- Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography (2nd ed.). CRC Press.
    - Oferă o explorare aprofundată a tehnicilor criptografice moderne, concentrându-se pe dovezi riguroase de securitate și aplicații practice.
- Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley.
    - Această carte discută despre proiectarea și implementarea sistemelor criptografice, subliniind importanța implementării adecvate pentru a preveni vulnerabilitățile.

Aceste resurse sunt selectate pentru a oferi o bază teoretică și abilități practice în criptografie, autentificare și gestionarea parolelor, susținând obiectivul curriculumului de a echipa Cursanții cu cunoștințele necesare pentru a securiza eficient datele organizaționale.

Gestionarea și securitatea dispozitivelor mobile

Organizațiile implementează din ce în ce mai mult dispozitivele mobile ca platformă de lucru majoră și mijloc de comunicare. Acest lucru este valabil în special pentru startup-uri și IMM-uri, unde a fi agil și accesibil în orice moment a devenit un criteriu major pentru succes. În timp ce tehnologia mobilă a avansat astfel încât majoritatea smartphone-urilor avansate sunt la fel de puternice și versatile ca laptopurile și desktopurile, natura wireless a acestor dispozitive le face susceptibile la actori răuvoitori care încearcă să obțină acces neautorizat. Această secțiune este concepută pentru a oferi o perspectivă asupra vulnerabilităților acestor dispozitive și ale platformelor aferente și asupra modului în care aceste riscuri pot fi reduse la minimum.

Principalele teme abordate cu privire la acest subiect

- Înțelegerea amenințărilor la adresa dispozitivelor mobile
- Evaluarea riscurilor pentru aplicațiile mobile
- Firewall-uri de comunicații inter-proces
- Tehnologii de securitate mobilă
- Controlul accesului la date mobile și gestionarea riscurilor

Rezultatele învățării

- Identificarea amenințărilor la adresa dispozitivelor mobile: Cursanții vor învăța să recunoască diverse amenințări care vizează platformele mobile și să înțeleagă impactul lor potențial.
- Evaluarea riscurilor pentru aplicațiile mobile: Cursanții vor dobândi abilități în evaluarea riscurilor asociate aplicațiilor mobile, concentrându-se asupra vulnerabilităților de securitate.
- Implementarea tehnologiilor de securitate mobilă: Cursanții vor putea implementa și gestiona tehnologii de securitate concepute special pentru dispozitivele mobile.
- Gestionarea firewall-urilor de comunicații inter-proces: Dotarea cursanților cu cunoștințele necesare pentru a configura și gestiona firewall-urile care controlează comunicațiile inter-proces pe dispozitive mobile.
- Aplicarea controalelor de acces la datele mobile: Cursanții vor învăța cum să stabilească și să aplice controale de acces la date pentru a securiza informațiile sensibile de pe dispozitivele mobile.

Literatură recomandată

- Doherty, J., (2021), Wireless and Mobile Device Security 2nd Edition.
    - Această carte analizează implicațiile integrării rapide ale dispozitivelor mobile în mediul de comunicare al organizației, preocupările legate de securitate și modul în care acestea pot fi atenuate.
- Russell, B., Van Duren, Drew., (2018), Practical Internet of Things Security - Second Edition: Design a security framework for Internet-connected Ecosystem
- Zdziarski, J. A. (2015). Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It. O'Reilly Media, Inc.
    - Această carte oferă o scufundare profundă în arhitectura de securitate a iOS, discutând vulnerabilitățile comune și oferind strategii pentru securizarea aplicațiilor iOS.
- Fried, S. (2011). Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World. CyberAge Books.
    - Acest ghid este esențial pentru cursanții și practicienii care au nevoie să înțeleagă provocările specifice de securitate prezentate de dispozitivele mobile, care sunt din ce în ce mai utilizate atât în contexte personale, cât și profesionale.

Aceste resurse vor sprijini curriculum-ul oferind atât cunoștințe fundamentale, cât și abilități specifice necesare pentru gestionarea și securizarea eficientă a dispozitivelor mobile, asigurându-se că cursanții sunt bine pregătiți pentru a aborda provocările de securitate mobilă în contexte organizaționale moderne.

Unitatea 3 – Evaluarea igienei digitale și mecanisme de feedback pentru VET

Introducere

Evaluarea și feedback-ul sunt componente cruciale ale procesului educațional, oferind atât profesorilor, cât și cursanților informații esențiale despre eficacitatea predării și învățării. În contextul unui curriculum de igienă digitală, evaluarea robustă și mecanismele de feedback sunt deosebit de importante. Acestea asigură faptul că cunoștințele și competențele predate nu sunt doar înțelese și păstrate, ci sunt aplicabile și în scenariile din lumea reală în care riscurile de securitate digitală sunt predominante.

Această unitate este concepută pentru a contura strategiile și metodologiile de evaluare a performanței cursanților și de furnizare a unui feedback constructiv pe tot parcursul programului de igienă digitală. Aceasta implică o combinație de evaluări teoretice ale cunoștințelor și evaluări practice.

Strategii de evaluare

Evaluări formative

- **Chestionare și teste scurte:** Teste frecvente și evaluări scurte vor fi efectuate pe parcursul fiecărui modul pentru a evalua înțelegerea conceptelor cheie și pentru a oferi feedback imediat. Acest lucru ajută la consolidarea învățării și la identificarea domeniilor în care sprijin ar putea avea nevoie de sprijin suplimentar.
- **Sarcini practice:** Cursanții vor primi sarcini care le cer să aplice cunoștințe teoretice unor scenarii practice, cum ar fi configurarea unui firewall, proiectarea unui plan de recuperare a datelor sau implementarea protocoalelor de criptare.
- **Evaluări între colegi:** Aceasta implică cursanții care își evaluează reciproc sarcinile sau proiectele. Evaluările între colegi pot ajuta la dezvoltarea gândirii critice și a abilităților analitice, deoarece cursanții învață să critice soluțiile de securitate cibernetică bazate pe cele mai bune practici.

Evaluări sumative

- **Examene finale:** Examinările cuprinzătoare de la sfârșitul fiecărui modul vor testa cursanții despre o gamă mai largă de subiecte acoperite pe tot parcursul cursului. Aceste examene vor include atât întrebări cu răspunsuri multiple, cât și întrebări de tip eseu pentru a evalua înțelegerea teoretică și practică a cursanților.
- **Proiecte Finale:** La sfârșitul programului, cursanțiivor întreprinde un proiect final care implică crearea sau gestionarea unor strategii cuprinzătoare de igienă digitală pentru organizații ipotetice. Acest

proiect va fi evaluat pe diverse criterii, inclusiv inovarea, aplicabilitatea și respectarea principiilor de securitate cibernetică.

Evaluare continuă

- **Recenzii de portofoliu:** Cursanții vor menține un portofoliu al muncii și realizărilor lor pe tot parcursul programului. Aceste portofolii vor fi revizuite periodic de profesori pentru a evalua progresul și pentru a oferi feedback personalizat.
- **Autoevaluarea:** Încurajarea cursanților să se angajeze în autoevaluare poate încuraja o responsabilitate mai mare pentru învățarea lor. Instrumente de autoevaluare și liste de verificare vor fi furnizate pentru a ajuta cursanții să-și evalueze înțelegerea și competențele.

Mecanisme de feedback

- **Feedback-ul profesorului:** Feedback-ul va fi furnizat sistematic pentru toate evaluările, concentrându-se pe punctele forte și punctele slabe ale muncii elevilor. Acest feedback va fi oportun, specific și constructiv, menit să încurajeze cursanții să reflecteze asupra învățării lor și să identifice domeniile de îmbunătățire.
- **Feedback între colegi:** În proiectele de grup și evaluările dintre colegi, cursanții vor fi încurajați să-și ofere feedback reciproc. Acesta va fi structurat astfel încât să se asigure că este constructiv și axat pe criterii specifice.
- **Feedback automat:** Pentru anumite tipuri de evaluări, în special chestionare și anumite exerciții practice, vor fi utilizate sisteme automate de feedback. Aceste sisteme pot oferi rezultate și informații imediate, permițând remedierea rapidă.
- **Bucle de feedback:** Crearea buclelor de feedback în cadrul curriculum-ului, unde cursanții pot reflecta asupra feedback-ului, își pot revizui munca și o pot retrimite pentru revizuire ulterioară, favorizează o mentalitate de creștere și o îmbunătățire continuă.

Implementarea feedback-ului în dezvoltarea curriculumului

Feedback-ul primit prin aceste mecanisme diferite nu este doar în beneficiul cursanților. De asemenea, joacă un rol crucial în dezvoltarea curriculumului:

- **Ajustări ale curriculumului:** Revizuirile periodice ale datelor privind performanța cursanților și feedback-ul vor ajuta la identificarea domeniilor curriculumului care ar putea avea nevoie de ajustări sau îmbunătățiri.
- **Dezvoltarea profesorilor:** Feedback-ul de la cursanți poate ghida, de asemenea, nevoile de dezvoltare profesională pentru profesori, indicând domeniile în care ar putea avea nevoie de mai mult sprijin sau formare.

Concluzie

Mecanismele de evaluare și feedback concepute pentru curriculumul de igienă digitală în instituțiile VET sunt esențiale pentru a asigura îndeplinirea obiectivelor educaționale. Prin utilizarea unei varietăți de strategii de evaluare și sisteme de feedback pe canale multiple, programul nu numai că evaluează în mod eficient învățarea cursanților, ci și îmbunătățește continuu metodele de predare și proiectarea curriculumului. Această abordare dinamică asigură faptul că curriculum-ul rămâne relevant și eficient în pregătirea cursanților pentru a aborda provocările legate de igiena digitală din lumea reală.

Unitatea 4 – Bune practici din partea instituțiilor VET

Introducere

În domeniul dinamic al igienei digitale, cunoștințele teoretice asociate cu aplicațiile practice creează cel mai eficient mediu de învățare. Această unitate analizează bunele practici adoptate de instituțiile de învățământ profesional și tehnic (VET) care au integrat cu succes principiile igienei digitale în programele lor. Aceste studii de caz servesc drept repere pentru dezvoltarea și perfecționarea programelor de igienă digitală, oferind perspective asupra strategiilor și metodologiilor de succes care pot fi replicate sau adaptate de alte instituții.

Studiu de caz 1: Academia CyberVET

Prezentare generală:

Academia CyberVET este cunoscută pentru curriculum-ul său robust de igienă digitală, care combină cunoștințe academice riguroase cu aplicații din lumea reală. Această instituție a devenit un model de integrare perfectă a tehnologiilor emergente și a celor mai bune practici de securitate cibernetică în formarea profesională.

Strategii cheie:

- Parteneriate industriale: CyberVET a format parteneriate cu companii de tehnologie de vârf pentru a se asigura că curriculum-ul lor este aliniat la standardele și practicile actuale din industrie. Aceste parteneriate facilitează, de asemenea, prelegeri susținute de invitați, stagii și acces la tehnologie de vârf.
- Medii de învățare simulate: Academia a investit în crearea unor laboratoare simulate de securitate cibernetică de ultimă generație în care cursanții pot explora și minimiza în siguranță amenințările cibernetice în timp real. Această experiență practică este de neprețuit.

Rezultate:

- O creștere semnificativă a capacității de inserție profesională a cursanților, 90% dintre absolvenți asigurându-și locuri de muncă în domeniul securității cibernetice în termen de șase luni de la absolvire.
- Creșterea implicării și satisfacției cursanților, atribuită abordării practice de învățare și implicării directe a industriei.

Studiu de caz 2: TechBridge VET

Prezentare generală:

TechBridge VET se remarcă prin accentul pus pe gestionarea și securitatea dispozitivelor mobile, domenii de îngrijorare crescândă în domeniul igienei digitale.

Strategii cheie:

- Proiectarea modulară a curriculumului: Curriculum-ul de la TechBridge este extrem de modular, permițând cursanților să-și adapteze traseele de învățare în funcție de obiectivele lor de carieră și de progresele tehnologice.
- Proiecte comunitare: Cursanții participă la programe de informare comunitară în care își aplică cunoștințele pentru a ajuta întreprinderile mici locale să-și îmbunătățească măsurile de securitate digitală.

Rezultate:

- Proiectele comunitare nu numai că au sporit abilitățile practice ale cursanților, ci au și crescut gradul de conștientizare a securității cibernetice în rândul proprietarilor locali de întreprinderi mici.
- Abordarea modulară a condus la o flexibilitate ridicată în educație, adaptându-se schimbărilor rapide în tehnologie și nevoilor elevilor.

Studiu de caz 3: Institutul SecurePath

Prezentare generală:

Institutul SecurePath a integrat igiena digitală în programele sale vocaționale, demonstrând modul în care securitatea cibernetică este fundamentală pentru diferite discipline tehnice.

Strategii cheie:

- Abordare interdisciplinară: Prin integrarea lecțiilor de igienă digitală în programe precum asistența medicală, tehnologia auto și managementul afacerilor, SecurePath se asigură că toți cursanții recunosc importanța securității cibernetice în domeniile lor de interes.
- Evaluarea continuă a curriculumului: Institutul utilizează un sistem de analiză bazat pe AI pentru a-și evalua și actualiza continuu curriculum-ul pe baza celor mai recente informații despre amenințările cibernetice și a tendințelor industriei.

Rezultate:

- Cursanții din programele non-tehnologice absolvă cu o înțelegere puternică a igienei digitale, făcându-i mai versatili și mai atractivi pentru angajatori.
- Evaluarea continuă a curriculumului a menținut SecurePath în fruntea educației de igienă digitală, adaptându-se rapid la amenințările emergente.

Implicații pentru cele mai bune practici

Succesele acestor instituții ilustrează mai multe bune practici care pot fi adoptate sau adaptate de alte instituții VET:

- Colaborarea în industrie: Legăturile puternice cu industria nu numai că mențin curriculum-ul relevant, ci și sporesc perspectivele de angajare ale cursanților după absolvire.
- Aplicație practică: Învățarea practică prin laboratoare, simulări sau proiecte comunitare este crucială pentru înțelegerea și aplicarea eficientă a principiilor igienei digitale.
- Flexibilitate și interdisciplinaritate: O abordare flexibilă și interdisciplinară asigură faptul că educația digitală în domeniul igienei digitale se poate adapta rapid la schimbări și poate satisface o gamă largă de domenii profesionale.
- Feedback și îmbunătățire continuă: Evaluarea continuă și revizuirea curriculum-ului pe baza feedback-ului de la diverse părți interesate, inclusiv cursanți, cadre didactice și parteneri din industrie, asigură eficacitatea și relevanța programului.

Studiu de caz 4: Colegiul Digital Defenders

Prezentare generală:

Colegiul Digital Defenders este renumit pentru abordarea sa specializată în predarea securității cibernetice, punând accentul în special pe hacking-ul etic și tehnicile criminalistice digitale. Această instituție VET se angajează să producă profesioniști calificați gata să abordeze complexitatea amenințărilor cibernetice în contextul digital modern.

Strategii cheie:

- Module de hacking etic: Încorporând module extinse privind hacking-ul etic, colegiul oferă cursanților abilitățile de a identifica și exploata vulnerabilitățile sistemului, toate într-un cadru controlat, etic și legal.

- Criminalistică cibernetică din lumea reală: Cursanții se angajează în exerciții practice de criminalistică cibernetică care imită scenariile de încălcare a datelor din lumea reală, ajutându-i să înțeleagă cum să urmărească, să analizeze și să atenueze încălcările în mod eficient.

Rezultate:

- Absolvenții sunt cunoscuți pentru abordarea proactivă a securității cibernetice, cu multe poziții sigure în sectoare cu mize mari, cum ar fi finanțele și guvernul.
- Experiența practică în hacking-ul etic și criminalistica cibernetică a condus la un nivel ridicat de implicare în rândul cursanților, promovând o înțelegere profundă a implicațiilor practice ale amenințărilor cibernetice.

Studiu de caz 5: Institutul InnovateTech

Prezentare generală:

Institutul InnovateTech s-a diferențiat prin integrarea tendințelor tehnologice avansate, cum ar fi inteligența artificială (AI) și învățarea automată (Machine Learning - ML), în curriculum-ul său de igienă digitală. Această abordare pregătește cursanții pentru un mediu de lucru al securității cibernetice din ce în ce mai bazat pe AI.

Strategii cheie:

- Soluții de securitate bazate pe AI: Instruirea cursanților să utilizeze AI și ML în dezvoltarea unor măsuri sofisticate de securitate cibernetică, rămânând astfel înaintea infractorilor cibernetici care utilizează și ei tehnologii avansate.
- Proiecte de colaborare cu companii de tehnologie: Cursanții lucrează la proiecte în colaborare cu companiile de tehnologie, creând soluții de securitate bazate pe AI, care le oferă informații în timp real despre provocările și cerințele industriei.

Rezultate:

- Cursanții au dezvoltat mai multe instrumente de securitate bazate pe AI, care au fost adoptate de companiile partenere, prezentând impactul lor direct asupra soluțiilor actuale de securitate cibernetică.
- Integrarea AI și ML în educația digitală privind igiena nu numai că a făcut curriculum-ul mai robust, ci și a crescut semnificativ capacitatea de angajare a cursanților în industriile bazate pe tehnologie.

Rezumatul bunelor practici

Aceste studii de caz suplimentare realizate de Colegiul Digital Defenders și Institutul InnovateTech consolidează și mai mult aspectele critice ale unui curriculum de igienă digitală de succes în instituțiile VET:

- Specializare și formare avansată: Programele care oferă instruire specializată în domenii cu cerere ridicată de securitate cibernetică, cum ar fi hacking-ul etic și AI, pot spori semnificativ relevanța și atractivitatea curriculum-ului.
- Aplicarea practică în lumea reală a abilităților învățate, fie prin criminalistică cibernetică, fie prin proiecte industriale colaborative, asigură faptul că cursanții nu sunt doar familiarizați cu conceptele teoretice, ci și cu aplicarea acestora în situații reale.
- Curriculum inovator și pregătit pentru viitor: Menținerea curriculum-ului aliniat la cele mai recente progrese tehnologice pregătește cursanții pentru amenințările și oportunitățile emergente, transformându-i în resurse valoroase în orice rol de securitate cibernetică pe care și-l asumă post-absolvire.
- Aceste exemple prezintă diversele strategii care pot fi implementate pentru a îmbunătăți în mod eficient educația privind igiena digitală, fiecare contribuind în mod unic la obiectivul general de promovare a profesioniștilor calificați pentru a proteja activele digitale într-un mediu cibernetic din ce în ce mai complex.

Concluzie

Cele cinci studii de caz explorate: Academia CyberVET, TechBridge VET, Institutul SecurePath, Colegiul Digital Defenders și Institutul InnovateTech oferă o gamă bogată de strategii și abordări de succes în integrarea igienei digitale în programele de educație și formare profesională (VET). Fiecare instituție, cu accentul și metodologia sa unică, subliniază rolul esențial al educației practice, aliniate la industrie și inovatoare în pregătirea cursanților pentru a naviga în complexitatea securității cibernetice în lumea digitală modernă.

Principalele idei de reținut și cele mai bune practici

- Colaborarea și alinierea cu industria: O temă comună în toate studiile de caz este importanța menținerii unor legături puternice cu liderii și companiile din industrie. Aceste parteneriate nu numai că mențin curriculum-ul actualizat cu cele mai recente tehnologii și practici, ci și sporesc capacitatea de angajare a cursanților prin stagii, proiecte reale și expunerea la standardele industriei.
- Experiență practică: Fiecare instituție subliniază necesitatea aplicării practice a conceptelor învățate. Fie prin laboratoare cibernetice, medii simulate sau investigații criminalistice din lumea reală,

experiența practică este crucială. Nu numai că cimentează cunoștințele teoretice, ci pregătește cursanții pentru provocările de pe piața muncii cu care se vor confrunta în cariera lor.

- Module specializate și formare avansată: Instituții precum Colegiul Digital Defenders subliniază beneficiile oferirii de formare specializată în domenii precum hacking-ul etic și criminalistica cibernetică. În mod similar, concentrarea Institutului InnovateTech asupra soluțiilor de securitate bazate pe AI ilustrează avantajul integrării tehnologiilor de ultimă oră în curriculum, pregătind cursanțiipentru tendințele și inovațiile viitoare în domeniul securității cibernetice.
- Abordări de învățare interdisciplinare și flexibile: Integrarea igienei digitale de către Institutul SecurePath în diferite programe profesionale exemplifică valoarea unei abordări interdisciplinare, care lărgește aplicabilitatea și relevanța educației în domeniul securității cibernetice. În plus, proiectarea modulară a curriculumului TechBridge VET permite o mai mare flexibilitate, adaptând schimbările tehnologice rapide și interesele diverse ale cursanților.
- Îmbunătățirea și adaptarea continuă: Utilizarea analizelor bazate pe AI de către Institutul SecurePath pentru evaluarea continuă a curriculumului și protocoalele dinamice de actualizare de la Institutului InnovateTech subliniază importanța evaluării și adaptării continue. Menținerea curriculum-ului receptiv la evoluția amenințărilor cibernetice asigură faptul că programele educaționale rămân relevante și eficiente.

Sinteza informațiilor din aceste diverse instituții VET arată că eficacitatea unui curriculum de igienă digitală depinde de capacitatea sa de a îmbina cunoștințele teoretice cu abilitățile practice, de a se adapta la progresele tehnologice și de a promova conexiuni puternice în industrie. Aceste elemente sunt esențiale în pregătirea cursanților nu doar pentru a răspunde cerințelor actuale ale domeniului securității cibernetice, ci și pentru a inova și a conduce în fața provocărilor viitoare. Această abordare holistică nu numai că îmbunătățește experiența de învățare, ci și sporește semnificativ capacitatea de angajare și disponibilitatea absolvenților de a proteja activele digitale într-o lume conectată la nivel global. Pe măsură ce instituțiile VET continuă să evolueze și să-și perfecționeze programele, lecțiile extrase din aceste studii de caz oferă planuri valoroase pentru dezvoltarea unor programe robuste și cuprinzătoare de igienă digitală, care sunt echipate pentru a face față provocărilor domeniului securității cibernetice.

Resurse:

1. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.
2. Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.
3. Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography* (2nd ed.). CRC Press.
4. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.
5. Chapple, M., Seidl, D., & Stewart, J. M. (2018). *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide* (8th ed.). Sybex.
6. Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). *Software Security Engineering: A Guide for Project Managers*. Addison-Wesley Professional.
7. Conklin, W. A., White, G., Cothren, C., Williams, D., & Davis, R. (2016). *Principles of Computer Security: CompTIA Security+ and Beyond* (5th ed.). McGraw-Hill Education.
8. Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Prentice Hall.
9. Bejtlich, R. (2013). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press.
10. Zdziarski, J. A. (2015). *Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It*. O'Reilly Media.
11. Tipton, H. F., & Nozaki, M. K. (2013). *Official (ISC)2 Guide to the CISSP CBK* (4th ed.). CRC Press.
12. Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach Publications.
13. Kim, D., & Solomon, M. G. (2016). *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning.
14. Caloyannides, M. A. (2010). *Privacy Protection and Computer Forensics* (2nd ed.). Artech House.
15. Toigo, J. W. (2009). *Disaster Recovery Planning: Preparing for the Unthinkable* (3rd ed.). Prentice Hall.
16. Ross, R. S. (2013). *Managing Information Security Risks: The OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) Approach*. Addison-Wesley.
17. Bodmer, C., Kilger, M., Carpenter, G., & Jones, J. (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. McGraw-Hill Osborne Media.
18. Enck, W. (2011). *Understanding Android Security*. IEEE Security & Privacy Magazine.
19. Anton, A. I., & Earp, J. B. (2004). *A Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts*. Academy of Management Review.
20. Liska, A., & Gallo, T. (2016). *Rethinking the Security of the Internet of Things*. Elsevier.

21. Clarke, N. L., & Furnell, S. M. (2016). *Cybersecurity Education: Strategies and Best Practices*. Springer.
22. Bishop, M. (2018). *Computer Security: Art and Science*. Addison-Wesley.
23. Eckert, J. W. (2017). *CompTIA Linux+ Guide to Linux Certification*. Cengage Learning.

24. Skoudis, E., & Zeltser, L. (2019). *Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall.
25. Easttom, C. (2019). *Modern Cryptography: Applied Mathematics for Encryption and Information Security*. McGraw-Hill Education.
26. Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson.
27. Andress, J., & Winterfeld, S. (2014). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Syngress.
28. Goodrich, M. T., & Tamassia, R. (2019). *Introduction to Computer Security*. Pearson.
29. Dafoulas, G. A., & Maia, C. (2015). *Global Security, Safety, and Sustainability: Tomorrow's Challenges of Cyber Security*. Springer.

Resurse online și site-uri web:

- Agenția pentru securitatea cibernetică și securitatea infrastructurii (CISA)
    - Site-ul: https://www.cisa.gov/
    - CISA oferă o multitudine de resurse privind cele mai bune practici și amenințări la adresa securității cibernetice, oferind orientări, instrumente și alerte care sunt esențiale pentru educația și conștientizarea securității cibernetice.
- Cadrul de securitate cibernetică al Institutului Național de Standarde și Tehnologie (NIST)
    - Site-ul: https://www.nist.gov/cyberframework
    - Cadrul NIST este un standard utilizat pe scară largă pentru gestionarea riscurilor de securitate cibernetică și oferă îndrumări structurate care pot fi integrate în curriculum-urile educaționale.
- Open Web Application Security Project (OWASP)
    - Site-ul: https://owasp.org/
    - OWASP este o comunitate online care oferă resurse gratuite și deschise privind securitatea aplicațiilor web, inclusiv instrumente, standarde și cele mai bune practici.
- Institutul SANS
    - Site-ul: https://www.sans.org/
    - Un lider recunoscut în formarea în domeniul securității cibernetice, Institutul SANS oferă o varietate de lucrări de cercetare, materiale de instruire și linii directoare de securitate.
- Krebs despre securitate
    - Site-ul: https://krebsonsecurity.com/
    - Condus de jurnalistul Brian Krebs, acest blog oferă știri și investigații aprofundate de securitate, concentrându-se pe cele mai recente amenințări și încălcări.
- Institutul Infosec
    - Site-ul: https://resources.infosecinstitute.com/

- Institutul Infosec oferă resurse și instruire axate pe securitatea informațiilor, inclusiv articole perspicace și actualizări din industrie.

- The Hacker News
  - Site-ul: https://thehackernews.com/
  - O revistă online de știri despre securitatea cibernetică, The Hacker News oferă informații actualizate despre amenințările și inovațiile actuale de securitate cibernetică.

- Bruce Schneier Blog
  - Site-ul: https://www.schneier.com/
  - Bruce Schneier este un renumit tehnolog de securitate al cărui blog oferă informații despre problemele de securitate și confidențialitate din lumea digitală.

Modulul 3: Implementare și susținere

Unitatea 1 - Construirea unei culturi de igienă digitală în startup-uri și instituții VET

Ce este cultura igienei digitale?

După cum am descoperit în modulele anterioare, igiena digitală este un termen care a apărut pentru prima dată la începutul secolului pentru a explica principiile practicilor digitale sigure, organizate și etice, care vizează protejarea eficientă a datelor, a confidențialității și a integrității unui sistem[1]. În acest modul, vom explora aplicarea sistemică a acestor principii la scară mai largă, personalizate pentru furnizorii VET din întreaga Europă și vom oferi sugestii privind construirea unei culturi mai bune a igienei digitale, care va inspira inovarea și entuziasmul în organizații.

Deci, ce este mai exact cultura igienei digitale? La fel ca multe alte culturi de rețea care se străduiesc să creeze o organizație de succes, indiferent dacă este centrată pe structură sau explorare[2], cultura igienei digitale se concentrează în jurul unei mentalități comune. În această mentalitate, fiecare membru crede în misiunea organizației și formulează strategii care se bazează pe responsabilitatea colectivă și integrarea practicilor digitale sigure.

Să explorăm modul în care cultura igienei digitale poate fi extinsă de la nivelul conducerii la grupurile de lucru și până la fiecare individ.

Dezvoltarea culturii igienei digitale la nivel de conducere

Într-o eră post-Covid, în care munca la distanță este noua normalitate, iar vulnerabilitățile din lumea digitală pot fi atât emoționale, cât și tehnice [3] (de exemplu, atacuri de inginerie socială care ar putea lua forma unei povești emoționale care este o încercare de phishing), situația necesită nu numai un manager, ci și un lider care poate naviga în complexitatea eficientă a lumii digitale, demonstrând în același timp practicile de igienă digitală ca parte integrantă a valorilor organizaționale. Mai jos sunt câteva dintre punctele importante în care un lider poate promova o cultură de igienă digitală sigură și de susținere:

- **Încurajarea flexibilității organizaționale** [4]:

Liderii trebuie să se asigure că organizațiile lor sunt adaptabile la progresele digitale, precum și la provocările care ar putea apărea din cauza practicilor digitale. Pentru a-și ghida echipa prin aceste schimbări, toți liderii ar trebui să-și înțeleagă mai întâi poziția, deciziile și emoțiile [5] în diferite circumstanțe înainte de a-i motiva pe ceilalți printr-un obiectiv comun.

- **Abordarea provocărilor de management [5]:**

Liderii din orice organizație trebuie să recunoască potențialele provocări de management care ar putea apărea în urma digitalizării, cum ar fi amenințările la adresa securității cibernetice, preocupările legate de confidențialitate, lacunele de calificare sau problemele ridicate de munca la distanță. Ei ar trebui să fie pregătiți să evalueze abilitățile echipelor lor în menținerea igienei digitale. Acest lucru necesită un anumit nivel de expertiză tehnică. Prin urmare, se recomandă ca liderii să înțeleagă și să articuleze eficient problemele tehnice cu echipele lor.

- **Crearea unor relații și procese de colaborare:**

Liderii din orice organizație ar trebui să creeze relații cu o gamă largă de părți interesate, atât la nivel intern, cât și la nivel extern. Acest lucru necesită ca aceștia să fie foarte coordonați și responsabili, precum și să își asume responsabilitatea de a încuraja un sentiment puternic de colaborare între angajați și alte părți interesate.

- **Investiții în educație și formare:**

Liderii din orice organizație ar trebui să investească în educația și formarea continuă a lor și a angajaților lor pentru a rămâne la curent cu cele mai recente practici și tehnologii de igienă digitală. Unele organizații din domeniul securității cibernetice [7], precum și unele organisme guvernamentale din Europa, cum ar fi Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), oferă o varietate de cursuri online și față în față pe tema sensibilizării cu privire la securitatea cibernetică și la gestionarea crizelor [8].

Dezvoltarea culturii igienei digitale la nivel de grup

După stabilirea unui parcurs pentru o strategie de igienă digitală, preocupările legate de securitatea cibernetică ale oricărei organizații ar trebui discutate și la nivel de grup. Grupurile de lucru, inclusiv departamentele, programele, elevii/ studenții sau managerii de proiect, pot contribui în mod semnificativ la promovarea unei culturi a igienei digitale în cadrul instituțiilor lor, cu sprijinul și colaborarea echipelor relevante de răspuns la incidente de securitate cibernetică (CERT).

Mai jos sunt câteva puncte importante pe care fiecare grup de lucru le poate folosi pentru a crea o cultură digitală a igienei:

- **Stabilirea unei comunicări eficiente în grupuri:**

O metodă eficientă de comunicare pentru grupuri este de a începe întâlniri sau cursuri cu discuții legate de securitatea cibernetică. Fiecare grup poate aloca cinci minute la început pentru întrebările membrilor. În timpul acestor întâlniri, se pot stabili reguli și orientări cu privire la modul în care dispozitivele trebuie utilizate în cadrul departamentelor sau al sălilor de clasă, pentru a consolida cultura igienei digitale [9].

O altă metodă utilă pentru grupuri poate fi solicitarea semnăturilor electronice sau a codurilor QR pentru documentele partajate care pot determina dacă un e-mail sau o tranzacție digitală este efectuată de un membru al grupului [10]. Un alt factor care necesită atenție este alegerea opțiunilor de stocare mai sigure, cum ar fi cloud, mai degrabă decât unitățile de memorie USB [10].

- **Stabilirea unor metode eficiente de documentare a atacurilor digitale:**

Documentarea atacurilor digitale este un aspect critic al menținerii securității cibernetice. Toate organizațiile ar trebui să explice în mod clar liniile directoare pentru documentare. Unele dintre procedurile de elaborare a documentației pentru atacurile digitale pot fi următoarele [: 11]:

Pasul 1: Păstrați un jurnal organizat: În cazul unui incident, încurajați fiecare membru al echipei voastre să includă anumite informații, precum data, ora, adresa de e-mail, linkurile relevante, numele conturilor și metadatele.

Pasul 2: Implementați șabloane structurate: Utilizați șabloane gata făcute pentru a documenta incidentele de încălcare a datelor. De exemplu, puteți utiliza șablonul jurnalului de incidente de la Access Now, un ONG internațional care își propune să protejeze drepturile civile digitale ale oamenilor din întreaga lume.

Pasul 3: Utilizați diverse formate de documentare: Încurajați-vă membrii echipei să utilizeze o gamă diversă de formate pentru a-și documenta problemele. Ei pot utiliza Internet Archive's Wayback Machine pentru a salva o pagină web sau pot folosi instrumente de captură video pentru a înregistra videoclipuri ca dovadă a problemelor lor.

Pasul 4: Stocați informații în siguranță: Creați copii de rezervă pe propriile dispozitive, în opțiuni de stocare de încredere și protejați-vă fișierele cu criptare, dacă este posibil.

- **Stabilirea evaluărilor periodice ale igienei digitale:**

Efectuarea periodică de audituri și evaluări ale riscurilor poate contribui la identificarea vulnerabilităților și la asigurarea respectării practicilor de igienă digitală [11]. Unele dintre modalitățile de stabilire a evaluărilor regulate ale igienei digitale sunt următoarele:

- Dezvoltarea unei rutine de obiceiuri de igienă cibernetică, cum ar fi scanarea pentru viruși, schimbarea parolelor, actualizarea software-ului și curățarea hard disk-urilor [12].
- Utilizarea instrumentelor potrivite, cum ar fi un firewall de rețea, software antivirus, soluții de criptare sau backup [13].
- Căutați asistență de la servicii fiabile, care oferă scanarea vulnerabilităților, scanarea aplicațiilor web și evaluări de phishing [14].

Dezvoltarea culturii igienei digitale la nivel individual

Factorii umani sunt una dintre cele mai slabe componente ale securității cibernetice. Câteva exemple de erori umane în ceea ce privește practicile digitale pot include gestionarea slabă a parolelor, ștergerea accidentală a datelor sau a fi victima phishingului sau a altor escrocherii de inginerie socială. Cu toate acestea, este întotdeauna posibil să se reducă riscurile acordând atenție și urmând practicile digitale de igienă.

Iată câteva puncte cheie în care fiecare individ poate contribui la crearea unei culturi de igienă în cadrul unei organizații:

- **Fii atent la amprenta ta digitală [15]:**

Navigarea în spațiile online poate fi complexă, iar oamenii ar trebui să fie vigilenți cu privire la amprenta lor digitală. Mecanismele de urmărire ale browserelor web, furnizorilor de e-mail, aplicațiilor mobile, motoarelor de căutare și platformelor de socializare pot compromite confidențialitatea personală. Pentru a spori securitatea în activitățile zilnice de navigare pe web, urmați acești pași:

Pasul 1: Fiți atenți la informațiile partajate pe platformele sociale și deconectați-vă de la conturile dvs. de socializare, deoarece site-urile de socializare pot rula analize pe conturile dvs., chiar dacă nu le utilizați [16].

Pasul 2: Folosiți browsere care respectă confidențialitatea, cum ar fi duckduckgo.com și startpage.com, care acordă prioritate confidențialității și oferă utilizatorilor rezultate de căutare fără urmărire personalizată.

Pasul 3: Fiți conștienți de activitățile online ale cercurilor dvs. sociale[16]: Recunoașteți că prezența online a prietenilor și a familiei vă poate afecta securitatea digitală. Sfătuiți-i cu privire la practicile online sigure.

Pasul 4: Fiți conștienți de setările smartphone-ului: La fel ca laptopurile, smartphone-urile sunt, de asemenea, un aspect crucial al activităților dvs. online. Prioritizați securitatea deconectându-vă constant de la aplicațiile care conțin informații sensibile. Deconectarea va fi, de asemenea, benefică pentru productivitatea muncii. Un studiu privind monitorizarea utilizării smartphone-urilor a constatat că, prin deconectarea și renunțarea la cookie-urile de urmărire, participanții au petrecut mai puțin timp în fiecare sesiune [17].

- **Acordați atenție actualizărilor software:**

Actualizările frecvente ale software-ului sunt esențiale pentru o bună igienă digitală, deoarece neactualizarea software-ului sau a browserelor web poate duce la vulnerabilități grave.

Un exemplu recent care demonstrează importanța actualizărilor software a apărut în 2021, când Adobe a dezvăluit că întrerupe Flash, vulnerabilitățile de securitate jucând un rol important în decizia lor [18]. Vulnerabilitățile de securitate în cauză includeau posibilitatea de a eluda în mod eficient măsurile de securitate ale browserului web. Echipele de intervenție în caz de urgență informatică (CERT) au trebuit să

abordeze problemele. După cum arată acest exemplu, acordarea atenției actualizărilor este o parte importantă a protejării software-ului și aplicațiilor împotriva vulnerabilităților.

- **Utilizați parole puternice[19]:**

Parolele slabe care sunt ușor de ghicit ar putea expune persoanele și organizațiile la riscul de încălcare a datelor. Astfel, nu utilizați numele sau ziua de naștere ca parolă. Cele mai puternice parole sunt cele care vor fi ușor de reținut, dar greu de spart. Iată câteva sfaturi despre crearea parolelor puternice și cum să le amintiți[19]:

PASUL 1: Construiți o propoziție cu simboluri diferite, care vor include litere mari și mici. De exemplu, o propoziție precum "Îmi plac merele, dar urăsc portocalele" poate fi transformată în "IL@bIH0"

PASUL 2: Utilizați autentificarea cu doi factori: Pe lângă crearea de parole robuste, îmbunătățiți-vă securitatea cu autentificarea cu doi factori (2FA). Autentificarea adaugă un nivel suplimentar de securitate, solicitând un al doilea pas de verificare, cum ar fi un cod trimis pe dispozitivul dvs. mobil, ceea ce va reduce riscul accesului autorizat.

PASUL 3: Păstrați parolele confidențiale și stocați-le în siguranță, dacă este necesar, cu un manager de parole sau cu o aplicație de autentificare, cum ar fi Dashlane sau 1Password. (Cu toate acestea, rețineți că securitatea acestor manageri este la fel de puternică ca veriga lor cea mai slabă!)

PASUL 4: Asigurați siguranța parolelor dvs. actualizându-le în mod regulat.

- **Clicuri prudente: fiți conștienți de phishing[14]:**

Phishing-ul își propune să păcălească oamenii să-și ofere informațiile sensibile, acționând ca o sursă de încredere. Phishing-ul este o infracțiune gravă. Dacă escrocii păcălesc oamenii să ofere informații personale, aceștia le pot accesa conturile de e-mail, bancare sau de socializare. Prin urmare, dacă ceva pare puțin neobișnuit sau poate un e-mail vă cere să verificați informațiile personale, mai ales cu un atașament sau un link, vă îndeamnă să faceți clic, în primul rând, aveți încredere în instinctele dvs. și gândiți-vă înainte de a face clic.

Unitatea 2 - Monitorizarea, revizuirea și îmbunătățirea continuă a practicilor de igienă digitală

Gândiți-vă la prezența dvs. digitală ca la un bun valoros, cum ar fi casa sau mașina dvs. Deoarece vi s-ar cere să aveți sesiuni regulate de mentenanță pentru a vă menține mașina sau casa în siguranță și funcțională, în același mod, verificarea practicilor de igienă digitală este importantă pentru a vă menține continuu sistemele sigure și funcționale. În această unitate, vom analiza practicile pe care le puteți realiza la nivel instituțional și individual pentru a vă menține competențele actualizate pe măsură ce tehnologia excelează.

Practici la nivel instituțional

Iată câteva dintre instrumentele și metodele care pot fi utile pentru monitorizarea, evaluarea și îmbunătățirea igienei digitale la nivel instituțional.

- **Găsiți cele mai recente reglementări UE:**

Înțelegerea și implementarea celor mai recente reglementări ajută instituțiile să identifice cele mai presante probleme și să acționeze în consecință pentru a atenua amenințările și a valorifica beneficiile.

Una dintre cele mai serioase provocări de care factorii de decizie politică au fost preocupați este IA. Pe 9 decembrie 2023, Uniunea Europeană a introdus o nouă lege numită "AI Act", care își propune să "valorifice beneficiile potențiale ale tehnologiei, încercând în același timp să protejeze împotriva posibilelor sale riscuri, cum ar fi automatizarea locurilor de muncă[20]". Informarea permanentă cu privire la cele mai recente reglementări ale Uniunii Europene privind IA este esențială pentru practici digitale responsabile și autorizate. Puteți consulta reglementările actualizate, cum ar fi Legea AI, online de pe pagina legislațiilor Uniunii Europene, pentru a asigura conformitatea cu liniile directoare și pentru a evita potențialele implicații juridice.

- **Verificări de securitate:**

Efectuarea unei revizuiri cuprinzătoare a setărilor de securitate este crucială în ceea ce privește monitorizarea eficienței liniilor directoare privind igiena digitală. Puteți utiliza verificările de securitate de rutină ale Google și Facebook, care vă ghidează prin măsuri de confidențialitate, permisiuni și control asupra celor mai recente activități. De asemenea, puteți utiliza surse online care vă permit să căutați în mai multe încălcări ale securității datelor, cum ar fi haveibeenpwnd.com pentru a fi conștienți de riscurile și frecvența încălcării securității datelor.

- **Analiza SWOT:**

SWOT este un acronim pentru puncte tari, puncte slabe, oportunități și amenințări și este o metodă de analiză strategică care va crea o foaie de parcurs pentru definirea poziției oricărei organizații și a strategiilor pentru dezvoltarea viitoare.

Iată câteva sfaturi de care trebuie să țineți cont în timp ce efectuați o analiză SWOT pentru organizația dvs., conform unui studiu privind pregătirea electronică a întreprinderilor[21]:

1. **Pregătirea pentru analiza SWOT:**
    a. ÎNCEPEȚI CU UN SCOP: Luați în considerare scopul și efectele pe termen lung ale aplicării unei analize SWOT.
    b. DEFINIȚI ZONELE care trebuie ANALIZATE: Identificați domenii specifice legate de cultura igienei digitale, de exemplu, conștientizarea angajaților, respectarea protocoalelor de securitate, a infrastructurii etc.
    c. SEMNAȚI ECHIPELE la ZONELE DEFINITE: Formați echipe care sunt experți în domeniile pe care doriți să le analizați și asigurați-vă că toate echipele diferite sunt aliniate la metodologia de efectuare a analizei.
2. **Analiza punctelor tari și a punctelor slabe:**
    a. Identificați-vă punctele tari și punctele slabe: Punctele tari și punctele slabe ale unei organizații sunt semne ale factorilor interni care arată eficacitatea și ineficiența acelei organizații. Este important să se includă justificări pentru ca deciziile privind un anumit factor să fie considerat o deficiență. (De exemplu, aplicațiile învechite pot fi considerate o slăbiciune datorită susceptibilității atacului asupra sistemelor).
    b. DETERMINAȚI RELEVANȚA PROBLEMELOR IDENTIFICATE: Determinarea a ceea ce este o slăbiciune și ce este un punct tare poate fi confuză. Cercetătorii sugerează [21] folosirea "Metodei celor 100 de puncte" pentru a le evalua și prioritiza. Fiecare membru al echipei poate avea 100 de puncte atribuite unui punct forte sau unei slăbiciuni, iar cu cât sunt atribuite mai multe puncte, cu atât este considerat mai semnificativ. După ce toată lumea își atribuie punctele, echipa le face media pentru a determina importanța lor generală.
3. **Analiza oportunităților și amenințărilor:**
    a. Evaluați relevanța și probabilitatea amenințărilor încercând să le organizați în aceste categorii: economice, sociale, politice, tehnologice și de mediu.
    b. Calculați oportunitățile asociate fiecărei dezvoltări. Acestea ar putea fi resurse financiare, o creștere a interesului public sau oportunități internaționale.
4. **Dezvoltarea matricei SWOT:** Selectați punctele forte, punctele slabe, oportunitățile și amenințările și grupați-le în funcție de cea mai înaltă semnificație pentru cultura igienei digitale a organizației dvs. Elaborați planuri de acțiune bazate pe strategii identificate care ar putea: (1) să se concentreze pe corectarea punctelor slabe profitând de oportunitățile dvs., (2) să se concentreze pe valorificarea unui punct tare pentru a profita de o oportunitate, (3) să se concentreze pe minimizarea unei slăbiciuni pentru

a evita o amenințare sau (4) să se concentreze pe a profita de un punct tare pentru a preveni o amenințare.

5. **Revizuiți-vă rezultatele**: revizuiți periodic progresul strategiilor implementate și repetați periodic analiza SWOT pentru a vă adapta la noile evoluții din peisajul digital.

- **Copii de rezervă regulate:**

  Copiile de rezervă sunt esențiale atunci când este nevoie să recuperați informații sensibile, în caz de pierdere a parolei, incidente tehnice etc. Uneori, monitorizarea cauzelor unui accident de sistem este posibilă și prin revizuirea vulnerabilităților sau erorilor de securitate din sistem. Utilizarea unui sistem de backup open-source, cum ar fi UrBackUp, care vă permite să păstrați o copie a documentelor dvs., poate fi un instrument valoros pentru monitorizarea și revizuirea practicilor de igienă digitală în caz de urgență.

Practici la nivel individual

Fiecare individ joacă un rol semnificativ în dezvoltarea unei practici de igienă digitală și pot fi luate numeroase măsuri pentru a revizui, monitoriza și dezvolta practicile existente. Iată câteva modalități de a vă îmbunătăți igiena digitală la nivel individual.

- **Conștientizare și educație:**

Adoptarea alfabetizării digitale nu înseamnă doar cunoașterea instrumentelor și metodelor, ci și înțelegerea peisajului tehnologic în continuă evoluție. Educarea noastră cu privire la amenințările online și menținerea la curent poate fi realizată prin participarea la oportunități de învățare continuă, cum ar fi cursurile Microsoft Digital Literacy, în care participanții pot învăța despre elementele de bază ale alfabetizării digitale, cum ar fi lucrul cu un computer, precum și competențe avansate, cum ar fi crearea de conținut online. În mod similar, cercetătorii[22] subliniază importanța predării cu privire la educația în domeniul mass-mediei și la utilizarea sigură și responsabilă a internetului, care ar trebui să reflecte experiențele și interesele reale ale persoanelor.

- **Comportament online responsabil:**

Comportamentul nostru online are consecințe în lumea reală. După cum s-a subliniat în studiile academice[23], este esențial ca cineva să se angajeze etic online, precum și să fie alfabetizat digital. Comportamentul responsabil online presupune implicarea în discuții online cu respect și sensibilitate. În plus, cunoașterea politicilor digitale contribuie la o comunitate online mai sigură și mai respectuoasă. Dacă nu sunteți sigur dacă acțiunile dvs. digitale implică bune practici, puteți utiliza ghidul Good Digital Citizen al Universității din Michigan.

- **Revizuire și adaptare:**

La fel ca orice aspect al lumii digitale, peisajul tehnologic este dinamic și ne cere să ne adaptăm continuu practicile. Prin urmare, revizuirea acțiunilor noastre digitale, adaptarea la escrocherii, recunoașterea încercărilor de phishing și precauția cu ceea ce descărcați sunt aspecte esențiale ale menținerii siguranței online.

Un instrument care vă poate ajuta să revizuiți practicile și să vă actualizați în mod regulat este Cadrul competențelor digitale sau DigComp. Este un instrument de referință pentru instituții, persoane fizice și educatori, dezvoltat de UE și care continuă să fie actualizat cu ultima sa versiune 2.2 de la data publicării acestui manual. DigComp este disponibil pe site-ul publicațiilor UE.

Actualizările regulate ale DigComp asigură faptul că cadrul rămâne relevant și reflectă mediul digital actual. La fel ca DigComp, puteți, de asemenea, să revizuiți și să actualizați practicile de igienă digitală pentru a vă asigura că acestea se aliniază la nevoile actuale ale organizației dvs. și să luați în considerare includerea abilităților legate de tehnologiile emergente.

Unitatea 3 - Viitorul igienei digitale: provocări și oportunități

Pe măsură ce ne îndreptăm spre viitor, ne așteptăm să vedem noi provocări și oportunități în dezvoltarea tehnologică. Peisajul în evoluție al tehnologiilor digitale, în special inteligența artificială (IA), creează noi complexități, pe măsură ce aceasta capătă mai multe abilități și competențe. Înțelegerea acestor complexități și oportunități este esențială pentru a asigura o experiență sigură, securizată și inovatoare pentru toți. În această unitate, vom analiza unele dintre cele mai presante probleme pentru viitorul igienei digitale, cu un accent specific pe tehnologiile emergente și pe ceea ce ar putea aduce acestea pentru inovare.

A-Tehnologii emergente

Mai multe tehnologii emergente, cum ar fi Blockchain, robotică, Internet of Things (IoT), realitate augmentată (AR) și realitate virtuală (VR), au fost de așteptat să modeleze viitorul. Dintre acestea, chatbot-urile generative AI precum ChatGPT au făcut cele mai multe valuri, încă de la înființarea sa în 2022.

Creșterea IA aduce noi dimensiuni igienei digitale și securității cibernetice. Tehnologiile IA pot "răspunde deja la întrebări, pot scrie poezii, pot genera cod de computer și pot purta conversații".[24] Unii experți consideră că IA va pune în pericol mulți angajați, deoarece locurile de muncă vor fi automatizate[25], în timp ce multe întreprinderi utilizează deja IA generativă pentru activitățile lor[26]. Deci, cum poate o instituție de învățământ, cum ar fi instituțiile VET, să beneficieze de posibilitățile IA?

- **Îmbunătățirea experienței de învățare:**

În domeniul educației și formării profesionale, IA generativă poate avea un mare potențial în a revoluționa experiența de învățare. Cercetătorii sugerează că IA poate crea scenarii, simulări sau evaluări realiste care să corespundă nevoilor, intereselor și abilităților cursantului[27]. Scenariile realiste pot oferi experiențe practice, captivante, care pot crea experiențe cruciale pentru domenii precum asistența medicală. În plus, educația în domeniul sănătății poate beneficia enorm de optimizarea sarcinilor de rutină, de stabilirea diagnosticelor sau de oferirea de medicamente personalizate care necesită discuții despre realizarea de conversații în jurul confidențialității și guvernanței robuste [28].

- **Îmbunătățirea predării și evaluării:**

Adaptarea la tendințele industriei și integrarea IA în predarea și evaluarea în instituții VET poate ajuta profesorii să-și optimizeze fluxul de lucru. ONG-urile și organizațiile internaționale explorează deja posibilitățile de îmbunătățire a acurateței, completitudinii și calității generale a muncii cursanților, ceea ce poate oferi, de asemenea, feedback imediat[29]. La fel ca în educația medicală, oferind IA capacitatea de a evalua activitatea cursanților va ridica, fără îndoială, întrebări cu privire la etica IA, un punct important de discuție pe care profesorii și părinții ar trebui să îl aibă în vedere.

- **Sisteme adaptive de management al cursanților:**

Sistemele de management al învățării (LMS) au extins deja orizonturile profesorilor VET, deoarece oferă materiale de predare și învățare într-o singură locație, precum și urmărirea progresului și performanței cursanților[30]. Cu IA, a crescut posibilitatea de a revoluționa LMS [31]. LMS bazat pe IA poate face sarcini avansate dincolo de automatizare, care pot include prezicerea performanței cursanților, permițând astfel profesorilor să creeze strategii pentru îmbunătățirea performanței cursanților [32]

B-Provocări în materie de reglementare

În unitățile de mai sus am explorat deja modul în care noile progrese tehnologice devin mai schimbătoare în diverse industrii și sisteme educaționale. Aceste progrese necesită ca toate părțile interesate să fie responsabile și să încurajeze utilizarea mai sigură a tehnologiilor emergente. Probleme precum confidențialitatea datelor, părtinirea/ biasarea algoritmică, utilizarea etică și responsabilitatea necesită cadre de reglementare cuprinzătoare.

- **Confidențialitatea datelor în educație**

În contextul educației, în special al educației online, care gestionează volume mari de date, există preocupări cu privire la confidențialitate și securitate [33]. Accesul neautorizat la un cloud sau utilizarea abuzivă a informațiilor sensibile reprezintă un risc semnificativ pentru instituțiile de învățământ și, începând din 2018, Regulamentul general al UE privind protecția datelor (GDPR) impune tuturor instituțiilor din interiorul și din afara UE să respecte obiecțiile sale privind protecția și circulația datelor cu caracter personal [34]. Prin urmare, este încurajat ca fiecare instituție VET să monitorizeze conformitatea cu GDPR și să aplice măsurile necesare pe măsură ce acesta evoluează.

- **Părtinire/ biasarea algoritmică**

Un LMS alimentat de IA poate moșteni bias-uri din datele utilizate pentru a-l antrena. În ceea ce privește ocuparea forței de muncă, procedurile de angajare bazate pe IA pot fi deosebit de dăunătoare pentru unele grupuri, așa cum s-a descoperit în cazul unui proces de recrutare Amazon în care sistemul predictiv a fost instruit cu majoritatea CV-urilor candidaților de sex masculin. Acest lucru a creat o prejudecată în care candidații de sex masculin au devenit mai preferabili decât candidații femei [35]. Profesorii înșiși ar trebui să fie conștienți de acest aspect al sistemelor bazate pe IA și să verifice încrucișat propriile prejudecăți despre cursanți. De asemenea, este din ce în ce mai important ca factorii de decizie politică să încurajeze dezvoltarea unor algoritmi transparenți și care să poată fi auditați.

- **Etica tehnologiilor emergente**

Similar preocupărilor legate de părtinirea/ biasarea algoritmică, integrarea tehnologiilor emergente, cum ar fi IA, în educație ridică întrebări semnificative. Care ar trebui să fie rolul tehnologiilor emergente în educație

în ceea ce privește luarea deciziilor? Există diferențe semnificative între diverse grupuri de cursanți cu privire la modul în care tehnologiile emergente influențează învățarea lor?

În domeniul IA, cercetătorii consideră că viața privată, părtinirea, supravegherea și autonomia sunt domenii-cheie care indică provocări etice pentru utilizarea acestor sisteme în educație [37]. Aceste domenii, precum și exemplele de întrebări de mai sus necesită mai multe oportunități de dezvoltare profesională pentru profesori pentru a educa generațiile viitoare cu privire la utilizarea etică și dezvoltarea IA. În acest context, inițiative precum Cadrul competențelor digitale al UE (DigComp) pot servi drept ghid valoros.

Recunoscând importanța promovării utilizării etice a IA, factorii de decizie executivă, cum ar fi Consiliul European, sunt deja în proces de definire a orientărilor etice și de promovare a transparenței care vor menține companiile tehnologice responsabile. Pe lângă Regulamentul privind Legea privind IA, menționat mai sus, Uniunea Europeană elaborează, de asemenea, politici pentru a sprijini și a încuraja utilizarea tehnologiilor emergente, cum ar fi realitatea virtuală, robotica și biotehnologia, care se preconizează că vor avea efecte mai mari asupra vieții cetățenilor [38].

C-Oportunități pentru inovare

Potrivit unui raport OCDE din 2021, realitatea virtuală, realitatea augmentată, robotica și inteligența artificială au devenit din ce în ce mai răspândite în VET pentru multe industrii, cum ar fi logistica, agricultura, ospitalitatea, energia și tehnologia informației, și vor deveni și mai răspândite în următorii ani [39]. În această secțiune, vom analiza modul în care diferite industrii utilizează deja aceste tehnologii și ce potențial se află în față.

- **Tehnologia informației (IT)**

Tehnologiile emergente, cum ar fi laboratoarele cloud de realitate virtuală, pot oferi elevilor/ studenților IT o experiență practică în diverse domenii, cum ar fi configurarea rețelei sau securitatea cibernetică [40]. Cybersecurity Labs simulează amenințările și atacurile cibernetice, oferind cursanților VET un mediu practic pentru a înțelege vulnerabilitățile din sistemele digitale fără a avea riscuri în lumea reală. Sisteme precum calculul de înaltă performanță, precum și tehnologia blockchain, oferă noi modalități de formare pentru securitatea cibernetică [41].

- **Logistică și transport**

Produsele comerciale precum jocurile de simulare pot ajuta cursanții să facă față provocărilor din lumea reală, iar în cazul logisticii, un joc disponibil în comerț numit „Simulatorul de camioane și logistică” face exact acest lucru, în care cursanții pot efectua sarcini logistice de la început până la sfârșit. Deoarece tehnologia joacă un rol crucial în planificarea sarcinilor complexe, furnizorii VET, profesorii și cursanții trebuie să practice

o bună igienă digitală și să asigure integritatea informațiilor în rețelele logistice, împărtășind în același timp informații cu produsele comercializate.

- **Agricultură**

De la drone la IA, tehnologiile emergente au potențialul de a crește productivitatea agriculturii și a practicilor agricole, de a reduce impactul asupra mediului și de a asigura venituri sporite. Modelele de cercetare cu drone cu rezoluție mai mare pot duce la o planificare mai eficientă a irigării și la o monitorizare mai precisă a culturilor și a animalelor [42]. În mod similar, RA poate fi utilizată pentru a promova agricultura inteligentă [43,] care vizează minimizarea riscurilor, creșterea randamentelor culturilor și reducerea stresului în agroindustrie [44]. Dar, riscurile asociate cu utilizarea unora dintre aceste tehnologii nu ar trebui neglijate[45]. Prin menținerea unei bune igiene cibernetice și încorporarea practicilor responsabile de IA, riscurile utilizării IA, RA și a altor tehnologii emergente pot fi atenuate.

- **Ospitalitate**

Ospitalitatea este unul dintre sectoarele semnificative din multe țări din Europa, contribuind la economie și asigurând în același timp milioane de locuri de muncă. Tehnologiile emergente pot oferi experiențe de învățare imersive pentru cursanții din domeniul ospitalității și turismului. Simulările de management hotelier și scenariile de servicii pentru clienți bazate pe internetul lucrurilor, care permit controlul temperaturii camerei, al iluminatului și al altor caracteristici, pot crea experiențe mai bune pentru oaspeți[46]. Modelele de instruire RV care au experiență în purtarea căștilor au fost deja utilizate de liderii proeminenți ai ospitalității din industrie [47]. Experiența lumii simulate poate ajuta oamenii să învețe mai repede, să păstreze cunoștințele pentru o perioadă mai lungă de timp și să fie mai implicați în formare [48]. Pe cât de mult îmbunătățesc aceste evoluții experiența utilizatorului, ele pot fi, de asemenea, perturbatoare și dezorientante pentru unii utilizatori. De aceea este important să se ia în considerare interfața cu utilizatorul și experiența utilizatorului în timp ce se implementează modificările [49].

- **Energie regenerabilă**

Tehnologiile emergente, cum ar fi sistemele de întreținere predictivă bazate pe IA, senzorii conectați și realitatea augmentată, pot accelera adoptarea surselor regenerabile, în timp ce simularea funcționării și întreținerii panourilor solare, a turbinelor eoliene sau a sistemelor hidroelectrice permite cursanților să dobândească abilități practice într-un mediu controlat [51]. La fel ca în sectorul agricol, utilizarea tehnologiilor emergente prezintă riscuri substanțiale, ceea ce face ca practicile de igienă digitală să fie un agent important în protejarea sistemelor[52]

Utilizarea tehnologiilor inovatoare, cum ar fi roboții, realitatea virtuală (RV), realitatea augmentată (RA) și simulatoarele, permite profesorilor să dezvolte competențele profesionale ale cursanților, stimulând în același timp competențele digitale și non-tehnice ale acestora. Este posibil ca aceste tehnologii să devină mai

frecvente în VET în anii următori, deoarece au avantaje în ceea ce privește flexibilitatea, costul și siguranța. [39] Predarea unei bune igiene digitale este esențială pentru integrarea tehnologiei digitale în viața noastră în moduri sigure, sănătoase, responsabile și respectuoase [9]

Unitatea 4 - Caz de bună practică în cultura igienei digitale

În unitățile anterioare, am aprofundat aspectele importante ale cultivării unei culturi robuste de igienă digitală atât în start-up-uri, cât și în instituțiile VET. Am explorat importanța monitorizării, revizuirii și îmbunătățirii continue a practicilor de igienă digitală pentru a asigura un mediu digital sigur și eficient. Aceste discuții au evidențiat rolul cultivării unei bune culturi a igienei digitale.

Acum, pe măsură ce pășim în ultima parte a modulului 3, în unitatea 4, suntem pe cale să ne axăm în aplicații din lumea reală cu exemple care prezintă cazurile practice de utilizare a principiilor de igienă digitală.

Cazuri de utilizare a igienei digitale în întreaga lume

- **Un set de instrumente specializate pentru promovarea practicilor de igienă digitală (Serbia)**

Un exemplu notabil de aplicare a bunelor practici de igienă digitală este un ghid elaborat de Share Cert, o fundație cu sediul la Belgrad, care pune accentul pe măsurile strategice de securitate cibernetică[53]. Prin clasificarea sistematică a celor mai frecvente amenințări și măsuri de securitate, acest ghid este susținut printr-o platformă deschisă în care persoanele și organizațiile pot fi informate despre cele mai presante subiecte din mediul digital și pot avea sfaturi generale despre cultura igienei digitale.

- **Campanii de sensibilizare a publicului pentru protecția drepturilor digitale (Grecia)**

O altă inițiativă importantă în ceea ce privește protecția drepturilor digitale are sediul în Grecia și se numește Homo Digitalis, o organizație neguvernamentală (ONG) care se concentrează pe dreptul la viață privată, protecția datelor cu caracter personal, interzicerea discriminării în spațiile digitale și libertatea de informare. Împreună cu cei peste 100 de membri ai săi, aceștia participă activ la studii și efectuează investigații în numele binelui public, care, în schimb, pot ajuta legiuitorii să înțeleagă mai bine aspectele legate de drepturile digitale [54].

- **Un kit de reacție rapidă pentru o societate civilă din ce în ce mai digitală (globală)**

Rețelele internaționale ale echipelor de răspuns la urgențe informatice (CERT) și ale rețelei de răspuns rapid (RaReNet) au colaborat pentru a ajuta respondenții rapizi, formatorii în domeniul securității digitale și activiștii cu cunoștințe tehnice să se protejeze mai bine împotriva celor mai frecvente tipuri de urgențe digitale cu ceea ce se numește un kit digital de prim ajutor, care oferă ghidare într-o varietate de probleme

[55]. Disponibil în 13 limbi și în continuă evoluție, cu contribuții externe, trusa digitală de prim ajutor este o sursă valoroasă pentru promovarea utilizării responsabile și sigure a internetului.

- **Construirea unor instrumente reziliente pentru a ține evidența practicilor de igienă digitală pentru societatea civilă (global)**

Centrul de Reziliență Digitală este o organizație non-profit care operează în peste 20 de țări cu intenția de a stabili sisteme digitale reziliente pentru a asigura siguranța societății civile [56]. Proiectele lor includ furnizarea de servicii și instrumente, cum ar fi un instrument de crowdsourcing conceput pentru identificarea și raportarea informațiilor false, o platformă digitală pentru raportarea problemelor de securitate, un instrument de vizualizare pentru monitorizarea amenințărilor și atacurilor asupra sistemelor digitale și un instrument comunitar menit să creeze o rețea puternică de participare în cadrul CiviCERT.

- **Rețele care facilitează schimbul de conținut între echipele de răspuns la nivel global pentru a urmări practicile de igienă digitală pentru societatea civilă (Global)**

CiviCERT este o rețea care aduce CERT-uri, conținut independent pe internet și furnizori de servicii, precum și ONG-uri și persoane fizice [57]. Membrii rețelei efectuează, coordonează și sprijină răspunsul la incidentele de securitate digitală care le sunt raportate într-un mecanism de colaborare în care este nevoie de punctul de vedere al altor parteneri. CiviCERT în sine ține pasul cu bunele practici de igienă digitală, în care membrii comunică prin platforme criptate, cum ar fi o listă de corespondență criptată și o platformă de partajare a informațiilor malware, pentru a împărtăși informații despre amenințările emergente la adresa societății civile și șabloane pentru a asigura proceduri fiabile și standardizate pentru gestionarea situațiilor de urgență.

- **Încurajarea drepturilor digitale ale omului în țările în curs de dezvoltare din (Asia de Vest și Africa de Nord)**

SMEX este un ONG care pledează pentru drepturile omului în mediile digitale din Asia de Vest și Africa de Nord [58]. În ceea ce privește practicile de igienă digitală, acestea oferă sprijin utilizatorilor de internet, activiștilor și organizațiilor pentru drepturile omului pentru problemele lor de securitate cibernetică și creează programe pentru a informa publicul larg despre reglementări și legea internetului. SMEX colaborează activ, de asemenea, cu parteneri locali și internaționali pentru a promova conștientizarea și implementarea practicilor de igienă digitală, promovând un mediu online mai sigur pentru persoanele și organizațiile care pledează pentru drepturile omului în spațiul digital din Asia de Vest și Africa de Nord.

- **Un curriculum de competențe digitale pentru elevilor K-12 (America de Nord)**

Conceptul de igienă digitală este din ce în ce mai important în sistemele educaționale din întreaga lume. Una dintre organizațiile specializate în pregătirea materialelor de alfabetizare digitală specifice elevilor K-12 este Common Sense Media, o organizație independentă cu sediul în America de Nord, care își propune să ofere elevilor, părinților și profesorilor informații bazate pe date cu privire la impactul mass-media și al mediilor digitale asupra nevoilor fizice, emoționale, sociale și mentale ale copiilor [59]. Curriculum-ul lor de cetățenie

digitală, susținut de cercetare, abordează probleme importante de media și tehnologie în școli, cum ar fi: Cum să ne protejăm de agresiune? Cum să ne protejăm confidențialitatea? și Cum să navigăm prin dezinformare?

- **Materiale educaționale pentru o mai bună alfabetizare digitală (America de Nord)**

Centrul de alfabetizare digitală este o organizație americană non-profit care își propune să promoveze cercetarea și crearea de materiale open-source [60] , precum și instrumente de proiectare a curriculumului, lecții, activități și evaluări care pot fi utilizate și adaptate diferitelor contexte educaționale [61]. Educația în domeniul mass-mediei este o parte importantă a practicilor de igienă digitală, iar accentul pus pe educația în domeniul mass-mediei nu numai că îmbunătățește igiena digitală, ci și cultivă o societate mai informată și mai exigentă, mai bine pregătită să se implice în complexitatea lumii digitale.

- **Luna europeană a securității cibernetice (Europa)**

În fiecare an, luna octombrie este sărbătorită ca Luna Europeană a Securității Cibernetice (ECSM), un eveniment anual important organizat de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) și Comisia Europeană [62]. Dedicat consolidării gradului de conștientizare a securității cibernetice în rândul cetățenilor și organizațiilor din UE, ECSM este una dintre numeroasele abordări multidimensionale ale UE pentru promovarea bunelor practici de igienă digitală. Pe parcursul lunii octombrie, conferințele, atelierele și webinariile creează o campanie extinsă care nu numai că crește gradul de conștientizare cu privire la securitatea cibernetică, ci împărtășește în mod activ informații actualizate și sfaturi de specialitate. Cu scopul de a promova utilizarea mai sigură a internetului, ECSM oferă sfaturi de igienă digitală. Reprezintă un efort cuprinzător și colaborativ, asemănător rețelelor globale precum CiviCERT și ONG-urilor regionale precum SMEX, jucând un rol vital în promovarea și susținerea bunelor practici de igienă digitală în întreaga Uniune Europeană.

- **Joc de securitate cibernetică pentru preșcolari (Global)**

Interland [63] este un joc interactiv creat de Google care face parte din "Be Internet Awesome" [64], un program integrat pentru promovarea practicilor de igienă digitală în rândul tinerilor cursanți. Ca joc dinamic și interactiv, Interland angajează elevii prin jocul său, oferind o abordare practică pentru predarea unora dintre aspectele esențiale ale bunelor practici de igienă digitală prin gamification[65]. Probleme complexe precum confidențialitatea, phishingul, hacking-ul și hărțuirea cibernetică sunt traduse elevilor mai tineri în animații colorate care sunt potrivite pentru nivelul lor de competență [66]. În general, Interland reprezintă un exemplu demn de remarcat al insuflării bunelor practici de igienă digitală de la o vârstă fragedă prin utilizarea tehnologiei.

În această unitate, am discutat despre implementarea și importanța bunelor practici de igienă digitală. Am analizat subiecte precum dezvoltarea unei culturi de igienă digitală în organizația dvs. la diferite niveluri de

management, explorarea metodelor de îmbunătățire continuă a acestor practici, informarea cu privire la oportunitățile viitoare de recoltare și provocările de depășit și apoi explorarea studiilor de caz din întreaga lume.

Consultați celelalte module ale acestui ghid pentru sfaturi și strategii suplimentare privind bunele practici de igienă digitală și vizitați site-ul web al Good Digital Hygiene for Startups.

Resurse

Unitatea 1 - Construirea unei culturi digitale de igienă în startup-uri și instituții VET

[1] Boulet, C. (2006). Digital Hygiene: Clean Living on a Dirty Network. *Interface: The Journal of Education, Community, and Values 6(3).* Retrieved from: Digital Hygiene: Clean Living on a Dirty Network (core.ac.uk) [Access Date 05.12.2023]

[2] Groysberg, B., Lee, J., Price, J., & Cheng, J. Y.-J. (2018, January-February). The leader's guide to corporate culture. *Harvard Business Review.* Retrieved from: The Leader's Guide to Corporate Culture (hbr.org) [Access Date 05.12.2023]

[3] Trevors, M. (2017). Cyber hygiene: 11 essential practices. Software Engineering Institute Blog. Retrieved from https://insights.sei.cmu.edu/blog/cyber-hygiene-11-essential-practices/ [Access Date 05.12.2023]

[4] Ly, B. The Interplay of Digital Transformational Leadership, Organizational Agility, and Digital Transformation. J Knowl Econ (2023). https://doi.org/10.1007/s13132-023-01377-8

[5] Harvard Business School Online. (n.d.). *How to Become a More Effective Leader.* Harvard Business School Publishing. Retrieved from https://info.email.online.hbs.edu/leadership-ebook

[6] Cortellazzo, L., Bruni, E., & Zampieri, R. (2019). The role of leadership in a digitalized world: A review. *Frontiers in Psychology,* 10, 1938. https://doi.org/10.3389/fpsyg.2019.01938

[7] Cisco. (n.d.) Cisco Learning Network Store. Retrieved from https://learningnetworkstore.cisco.com/

[Access Date 06.12.2023]

[8] European Union Agency for Cybersecurity (ENISA). (n.d.). Online training material for cybersecurity specialists: Technical and operational. ENISA. Retrieved from https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#identification_handling [Access Date 06.12.2023]

[9] Sklar, A. (2017). Sound, smart, and safe: A plea for teaching good digital hygiene. *LEARNing Landscapes Journal*, 10(2). https://doi.org/10.36510/learnland.v10i2.799 [Access Date 06.12.2023]

[10] Glazer, K. (2017, March 22). A quick guide to good digital hygiene. *Literacy Now*. Retrieved from https://www.literacyworldwide.org/blog/literacy-now/2017/03/22/a-quick-guide-to-good-digital-hygiene

[Access Date 06.12.2023]

[11] Documenting Digital Attacks (n.d). Digital First Aid. Retrieved from https://digitalfirstaid.org/documentation/

[12] Saraf, A. (2021, May 14). Three steps to healthy digital hygiene. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2021/05/14/three-steps-to-healthy-digital-hygiene/

[Access Date 11.12.2023]

[13] Kaspersky. (n.d.). Cyber hygiene habits: 11 ways to improve your security. Retrieved from https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

[14] Cybersecurity and Infrastructure Security Agency (CISA). (2022). 4 things you can do to keep yourself cyber safe. Retrieved from https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe [Access Date 11.12.2023]

[15] CHAYN. (2018). *Do it Yourself Online Safety.* Retrieved from https://chayn.gitbook.io/diy-online-safety/english [Access Date 07.12.2023]

[16] Torbet, G. (2019, February 3). Social media sites can predict your behavior even if you don't use them. *Digital Trends.* Retrieved from https://www.digitaltrends.com/social-media/social-media-privacy-friends-prediction/

[17] Toth.R., & Trifonova, T. (2021). Somebody's Watching Me: Smartphone Use Tracking and Reactivity. *Computers in Human Behavior Reports, 4*, *100142*, https://doi.org/10.1016/j.chbr.2021.100142

[Access Date 07.12.2023]

[18] Brooks, T. (2021, July 29). Why You Should Update Your Web Browser. *How-To Geek.* Retrieved from https://www.howtogeek.com/725165/why-you-should-update-your-web-browser/ [Access Date 08.12.2023]

[19] Barrons, M. (2016, September 12). How to Create Secure Passwords You Won't Forget. *InfoWare Group Blog.* Retrieved from https://infowaregroup.com/blog/how-to-create-secure-passwords-you-won't-forget [Access Date 08.12.2023]

Unitatea 2 - Monitorizarea, revizuirea și îmbunătățirea continuă a practicilor de igienă digitală

[20] Scott, M. (2023, December 8). Europe's plan to tame Big Tech: A new legal framework. *The New York Times*. Retrieved from E.U. Agrees on AI Act, Landmark Regulation for Artificial Intelligence - The New York Times (nytimes.com)

[21] Rehak, D., & Grasseova, M., (2011). The Ways of Assessing the Security of Organization Information Systems through SWOT Analysis. In M. Alshawi & M. Arif (Eds.), *Cases on E-Readiness and Information*

Systems Management in Organizations: Tools for Maximizing Strategic Alignment (1st ed., pp. 162-184). IGI Global. https://doi.org/10.4018/978-1-61350-311-9

[22] Gleason, Benjamin & von Gillern, Sam. (2018). Digital citizenship with social media: Participatory practices of teaching and learning in secondary education. Educational Technology and Society. 21. 200-212. https://www.researchgate.net/publication/322733013_Digital_citizenship_with_social_media_Participatory_practices_of_teaching_and_learning_in_secondary_education [Access Date 20.12.2023]

[23] Lewin, C., Niederhauser, D., Johnson, Q., Saito, T., Sakamoto, A., & Sherman, R. (2021). Safe and Responsible Internet Use in a Connected World: Promoting Cyber-Wellness. *Canadian Journal of Learning and Technology, 47*(4), Special Issue.

Unitatea 3 - Viitorul igienei digitale: provocări și oportunități

[24] Metz, C. (2023). What's the Future of AI? *The New York Times.* Retrieved from https://www.nytimes.com/2023/03/31/technology/ai-chatbots-benefits-dangers.html?searchResultPosition=1

[25] Gleason, Benjamin & von Gillern, Sam. (2023). Tinkering With ChatGPT, Workers Wonder: Will This Take My Job? *The New York Times.* Retrieved from https://www.nytimes.com/2023/03/28/business/economy/jobs-ai-artificial-intelligence-chatgpt.html

[26] Banholzer, M., Fletcher, B., LaBerge, L., & McClain, J. (2023, August 31). Companies with Innovative Cultures Have a Big Edge with Generative AI. *McKinsey & Company.* Retrieved from https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/companies-with-innovative-cultures-have-a-big-edge-with-generative-ai [Access Date 21.12.2023]

[27] Chng, E., Tan, A.L. & Tan, S.C. Examining the Use of Emerging Technologies in Schools: a Review of Artificial Intelligence and Immersive Technologies in STEM Education. Journal for STEM Educ Res 6, 385–407 (2023). https://doi.org/10.1007/s41979-023-00092-y [Access Date 21.12.2023]

[28] Spatharou, A., Hieronimus, S., & Jenkins, J. (2020, March 10). Transforming healthcare with AI: The impact on the workforce and organizations. *McKinsey & Company.* Retrieved from https://www.mckinsey.com/industries/healthcare/our-insights/transforming-healthcare-with-ai

[29] Kopp, W., & Thomsen, B. S. (2023, May 1). How AI can accelerate students' holistic development and make teaching more fulfilling. *World Economic Forum.* Retrieved from

https://www.weforum.org/agenda/2023/05/ai-accelerate-students-holistic-development-teaching-fulfilling/

[30] Pappas, C., (2016, January 7). The Top 8 Benefits Of Using Learning Management Systems. *Elearning Industry.* Retrieved from https://elearningindustry.com/top-8-benefits-of-using-learning-management-systems

[31] Seo, K., Tang, J., Roll, I. *et al.* The impact of artificial intelligence on learner–instructor interaction in online learning. *International Journal of Educational Technology in Higher Education* 18, 54 (2021). https://doi.org/10.1186/s41239-021-00292-9

[32] Yadav, N. R., & Deshmukh, S. S. (2023). Proceedings of the International Conference on Applications of Machine Intelligence and Data Analytics. In *Proceedings of the International Conference on Applications of Machine Intelligence and Data Analytics (ICAMIDA 2022)* Retrieved from https://www.atlantis-press.com/article/125986295.pdf

[33] Duball, J. (2020). Shift to Online Learning Ignites Student Privacy Concerns. *International Association of Privacy Professionals (IAPP).* Retrieved from https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns/

[34] United States International Trade Administration. (n.d.). European Union - Data Privacy and Protection. Retrieved from https://www.trade.gov/european-union-data-privacy-and-protection

[35] Gonzalez, G. (2018, October 10). Amazon Abandons AI Recruiting Tool That Showed Bias Against Women. *Inc.* Retrieved from https://www.inc.com/guadalupe-gonzalez/amazon-artificial-intelligence-ai-hiring-tool-hr.html

[36] Gatzemeier, S. (2021, June 18). AI Bias: Where Does It Come From and What Can We Do About It? *UC Berkeley School of Information Blog.* Retrieved from https://blogs.ischool.berkeley.edu/w231/2021/06/18/ai-bias-where-does-it-come-from-and-what-can-we-do-about-it/

[37] Akgun, S., Greenhow, C. Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI Ethics* 2, 431–440 (2022). Retrieved from https://doi.org/10.1007/s43681-021-00096-7

[38] Polluveer, K. (2023). Innovation Policy. *European Parliament Fact Sheet.* Retrieved from https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/en/FTU_2.4.6.pdf

[39] OECD (2021), Teachers and Leaders in Vocational Education and Training, OECD Reviews of Vocational Education and Training, OECD Publishing, Paris, https://doi.org/10.1787/59d4fbb1-en

4. Promoting innovative pedagogical approaches in vocational education and training | Teachers and Leaders in Vocational Education and Training | OECD iLibrary (OECD-ilibrary.org)

[40] eduLAB Pty Ltd. (2020, August 12). eduLAB Introduction Video. *Vimeo.* Retrieved from https://vimeo.com/447337687

[41] N.d. (2022, March 27). 7 Technology Innovations That Will Impact Cybersecurity in 2022 and Beyond. *Cloud Security Alliance Blog.* Retrieved from 7 Technology Innovations That Will Impact Cybersecurity in 2022 | CSA (cloudsecurityalliance.org)

[42] World Economic Forum. (2021, March). Artificial Intelligence for Agricultural Innovation. *Community Paper.* Retrieved from WEF_Artificial_Intelligence_for_Agriculture_Innovation_2021.pdf (weforum.org)

[43] BIS Research. (2021, October 7). The Increasing Adoption of Augmented Reality (AR) in Agriculture. Retrieved from https://blog.marketresearch.com/the-increasing-adoption-of-augmented-reality-ar-in-agriculture

[44] BIS Research. (2021, October 7). The Increasing Adoption of Augmented Reality (AR) in Agriculture. Retrieved from https://eos.com/blog/smart-farming/

[45] Tzachor, A., Devare, M., King, B., et al. (2022). Responsible artificial intelligence in agriculture requires a systemic understanding of risks and externalities. *Nature Machine Intelligence, 4*, 104–109. https://doi.org/10.1038/s42256-022-00440-4

[46] Bettencourt, J. (2023, November 16). How the hospitality industry is using AR, and VR for the guest experience. *Hotel Management.* Retrieved from https://www.hotelmanagement.net/tech/how-hospitality-industry-using-ar-vr-guest-experience

[47] Kover, A. (2020, March 10). A new perspective on hospitality: How Hilton uses VR to teach empathy. *Facebook Reality Labs Tech Blog.* Retrieved from https://tech.facebook.com/reality-labs/2020/3/a-new-perspective-on-hospitality-how-hilton-uses-vr-to-teach-empathy/

[48] Guenther, D. (2021, September 9). Virtual Reality training prepares hospitality workers for the next era of travel. *Medium.* Retrieved from https://medium.com/@DanielGuenther/virtual-reality-training-prepares-hospitality-workers-for-the-next-era-of-travel-7a8d5d3b8be5

[49] Pencarelli, T. The digital revolution in the travel and tourism industry. *Inf Technol Tourism* 22, 455–476 (2020). Retrieved from https://doi.org/10.1007/s40558-019-00160-3

[50] Amon, C., Slaughter, A., & Motyka, M. (2018, September). Global renewable energy trends. *Deloitte.* Retrieved from https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/global-renewable-energy-trends.html

[51] Travelers. (n.d.). Predictive Maintenance at Solar and Wind Installations. Retrieved from https://www.travelers.com/resources/business-industries/energy/predictive-maintenance-at-solar-and-wind-installations

[52] Victor, D. G. (2019, January 10). How artificial intelligence will affect the future of energy and climate. *Brookings Institution.* Retrieved from https://www.brookings.edu/articles/how-artificial-intelligence-will-affect-the-future-of-energy-and-climate/

[9] Sklar, A. (2017). Sound, smart, and safe: A plea for teaching good digital hygiene. *LEARNing Landscapes Journal*, 10(2). https://doi.org/10.36510/learnland.v10i2.799 [Access Date 06.12.2023]

Unitatea 4 - Caz de bună practică în cultura igienei digitale

[53] ShareCert Toolkit. (n.d.). Retrieved from Cybersecurity Toolkit

[54] Homo Digitalis. (2022, July 13). A big success for Homo Digitalis: The Hellenic DPA fines CLEARVIEW AI with €20 million. Retrieved from https://homodigitalis.gr/en/posts/12155/

[55] Digital First Aid. (n.d.). Retrieved from Digital First Aid Kit

[56] Digiresilience. (n.d.). Retrieved from Center for Digital Resilience

[57] CivicERT. (n.d.). Retrieved from CiviCERT

[58] SMEX. (n.d.). Retrieved from SMEX

[59] Common Sense Media. (n.d.). Digital Literacy and Citizenship. Retrieved from https://www.commonsensemedia.org/what-we-stand-for/digital-literacy-and-citizenship

[60] Center for Media Literacy. (2005). Five Key Questions of Media Literacy. Retrieved from https://www.medialit.org/sites/default/files/14B_CCKQPoster+5essays.pdf

[61] Center for Media Literacy. (n.d.). Retrieved from https://www.medialit.org/https://www.medialit.org/

[62] European Cyber Security Month. (n.d.). Retrieved from https://cybersecuritymonth.eu/

[63] Google. (2023). Be Internet Awesome: Interland. Retrieved from https://beinternetawesome.withgoogle.com/en_us/interland/

[64] Google. (2023). Be Internet Awesome: Interland. Retrieved from https://beinternetawesome.withgoogle.com/en_us

[65] Bogardus Cortez, M. (2018, April 17). The Digital Citizenship Curriculum: Digital Literacy, Cyber Hygiene and More. *EdTech Magazine.* Retrieved from How to Design Your Digital Citizenship Curriculum - EdTech (edtechmagazine.com)

[66] Bogardus Cortez, M. (2014, July 24). Digital Citizenship Game by Google & ITSE Aims to Educate. *EdTech Magazine.* Retrieved from Digital Citizenship Game by Google & ITSE Aims to Educate | EdTech Magazine

---

[12*] Durbin, S. (2019). The top 3 global cybersecurity threats of 2020. *Dark Reading.* Retrieved from **https://www.darkreading.com/vulnerabilities-threats/crystal-ball-the-top-3-global-cybersecurity-threats-for-2020** [Access Date 06.12.2023]

[13*] Ponemon, L., & Beri, S. (2014). *Data Breach: The Cloud Multiplier Effect.* Retrieved from **https://www.slideshare.net/Netskope/data-breach-the-cloud-multiplier-effect** [Access Date 06.12.2023]

[14*] Hadlington, L. (2017). Human factors in cybersecurity: examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. *Heliyon, 3*. **https://doi.org/10.1016/j.heliyon.2017.e00346**

[15*] Telefonica Tech. (2022, November 10). Human Factors in Cybersecurity: Protect Yourself. *Telefonica Tech Blog.* Retrieved from **https://telefonicatech.com/en/blog/human-factors-in-cybersecurity** [Access Date 11.12.2023]

[XXXXX] Irwin, L. (2020, June). *5 ways to detect a phishing email – with examples*. ITGovernance. https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishing-email [Access Date 08.12.2023]

[XXXXXXX] Federal Trade Commission Consumer Information (2019, May). *How To Recognize and Avoid Phishing Scams.* https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams [Access Date 08.12.2023]

[XX] DCAF (Geneva Centre for Security Sector Governance), Babić, V., & Bratić, A. (2022, October). *Guidebook on Staying Safe Online: Cyber Hygiene for Public Institutions and SMEs.* Retrieved from **https://www.dcaf.ch/sites/default/files/publications/documents/GuidebookStayingSafeOnline_CyberHygiene_EN_web_Jan2023.pdf** [Access Date 06.12.2023]