# Handboek voor beroepsonderwijs en -opleiding

BDA

mathemagenesis

MUĞLA SITKI KOÇMAN ÜNİVERSİTESİ

eLearning software

EduVibes

WITTENBORG University of Applied Sciences

**31 MEI 2024**

Co-funded by the European Union

GOOD START

Good Digital Hygiene for Startups

Projectnr.: 2022-1-LV01-KA220-VET-000086725 | Titel van het project: Goede digitale hygiëne voor startups

# Inhoudsopgave

# Module 1 - Digitale hygiëne voor professionals in beroepsonderwijs en -opleiding

## Unit 1 - Het belang van digitale hygiëne in het onderwijs in beroepsonderwijs en -opleiding

### Digitale hygiëne en cyberbeveiliging

Digitale hygiëne verwijst naar de praktijken en gewoonten die individuen gebruiken om hun online privacy, veiligheid en algemeen welzijn te behouden. Het omvat een breed scala aan proactieve gedragingen en maatregelen die gericht zijn op het beschermen van persoonlijke informatie, het voorkomen van online bedreigingen en het minimaliseren van risico's in verband met digitale activiteiten. Voorbeelden van digitale hygiënepraktijken zijn het gebruik van sterke wachtwoorden, het inschakelen van tweefactorauthenticatie, het regelmatig updaten van software, voorzichtig zijn met het online delen van persoonlijke informatie en het beheren van iemands digitale voetafdruk. Digitale hygiëne is een concept dat nauw verbonden is met een ander concept, namelijk cybersecurity. Vaak wordt digitale hygiëne beschouwd als een proactief element van cyberbeveiliging dat een verantwoordelijkheid is van een individu.

Cyberbeveiliging is een gespecialiseerd gebied dat zich toelegt op het beschermen van computersystemen, netwerken en gegevens tegen ongeoorloofde toegang, cyberaanvallen en andere inbreuken op de beveiliging. Het omvat de implementatie van technische maatregelen, beveiligingsprotocollen en verdedigingsstrategieën om digitale activa te beschermen en potentiële risico's van verschillende cyberdreigingen te beperken. Mensen die verantwoordelijk zijn voor cyberbeveiliging werken vaak aan het identificeren van kwetsbaarheden in systemen, het ontwikkelen van beveiligingsoplossingen, het monitoren van verdachte activiteiten en het reageren op beveiligingsincidenten om de integriteit, vertrouwelijkheid en beschikbaarheid van informatie en middelen te waarborgen. Als gevolg hiervan worden cyberbeveiligingsactiviteiten vaak uitgevoerd door professionals, in tegenstelling tot digitale hygiëne, die de verantwoordelijkheid van iedereen kan zijn.

## Digitale hygiëne in organisaties in beroepsonderwijs en -opleiding

Verschillende organisaties hebben de neiging om van hun werknemers te verwachten dat ze enkele algemene regels volgen om ervoor te zorgen dat de regels en best practices van digitale hygiëne worden nageleefd. Organisaties voor beroepsonderwijs en -opleiding hebben een aantal algemene richtlijnen die gelden voor alle organisaties die werken met mensen en hun persoonlijke informatie en met eigen diensten en producten die worden ontwikkeld, opgeslagen en gedeeld via een digitale omgeving. Ze hebben echter een aantal specifieke uitdagingen met betrekking tot het soort service dat ze leveren en de unieke aard van hun doelklanten. Opvoeders bevinden zich vaak in een situatie waarin ze hun klanten extra begeleiding moeten bieden. Dit kan betekenen dat zij tijdens het uitvoeren van de training een voorlichter van digitale hygiëne moeten zijn, bijvoorbeeld bij het verlenen van de beoogde dienst.

Er zijn verschillende redenen waarom digitale hygiëne specifiek voor organisaties in beroepsonderwijs en -opleiding als zeer belangrijk wordt beschouwd:

- **Bescherming van gevoelige informatie**

Bij het uitvoeren van hun werk hebben organisaties in beroepsonderwijs en -opleiding vaak te maken met een schat aan gevoelige informatie, waaronder studentendossiers, academische gegevens en financiële details. Een deel van deze informatie kan cruciaal zijn voor de organisatie bij het uitvoeren van learning analytics of het evalueren van de diensten die aan de klanten worden geleverd. Door een goede digitale hygiëne toe te passen, wordt deze informatie beschermd tegen ongeoorloofde toegang, datalekken en cyberdreigingen, waardoor de vertrouwelijkheid en integriteit van gevoelige gegevens wordt gewaarborgd.

- **Behoud van de institutionele reputatie**

Bij het omgaan met de gegevens die aan een organisatie voor beroepsonderwijs en -opleiding worden toevertrouwd zonder het juiste niveau van zorg, kan de organisatie onbedoeld de manier veranderen waarop haar klanten en partners ernaar kijken. Een datalek of beveiligingsincident kan aanzienlijke reputatieschade toebrengen aan een organisatie in beroepsonderwijs en -opleiding. Door prioriteit te geven aan digitale hygiënepraktijken, tonen instellingen hun toewijding aan beveiliging, betrouwbaarheid en professionaliteit, waardoor hun reputatie bij belanghebbenden, waaronder studenten, ouders, werkgevers en regelgevende instanties, wordt verbeterd.

- **Naleving van de regelgeving**

Afhankelijk van hun aard van het werk en de manier waarop ze contact maken met hun klanten, zijn organisaties in beroepsonderwijs en -opleiding onderworpen aan verschillende voorschriften en nalevingsvereisten met betrekking tot gegevensbescherming, privacy en cyberbeveiliging. Het naleven van best practices voor digitale hygiëne helpt bij het waarborgen van naleving van relevante wet- en regelgeving,

waardoor het risico op wettelijke boetes, straffen en wettelijke aansprakelijkheden in verband met niet-naleving wordt beperkt.

- **Ondersteuning bij leren en onderwijzen**

Digitale technologieën spelen een cruciale rol in het moderne onderwijs en vergemakkelijken online leren, samenwerkingsprojecten en digitale beoordelingen. Deze technologieën worden gebruikt om trainingsmateriaal te ontwikkelen, te beheren en te delen, trainingsomgevingen te organiseren, de betrokkenheid van deelnemers bij deze technologieën te beheren of gegevens te analyseren die tijdens het trainingsproces zijn verzameld. Door een veilige en betrouwbare digitale infrastructuur te onderhouden, kunnen organisaties in beroepsonderwijs en -opleiding studenten en docenten een naadloze leerervaring bieden, waardoor innovatie, creativiteit en betrokkenheid bij onderwijs- en leeractiviteiten worden bevorderd.

- **Beperking van cyberbeveiligingsrisico's**

De onderwijssector kan het doelwit zijn van cybercriminelen die misbruik willen maken van kwetsbaarheden in digitale systemen en netwerken of van het gebrek aan kennis en vaardigheden van studenten en opleiders die niet gewend zijn om betrokken te zijn bij opleidingen in een digitale omgeving. Het implementeren van digitale hygiënemaatregelen helpt cyberbeveiligingsrisico's te beperken, waaronder malware-infecties, phishing-aanvallen, ransomware-bedreigingen en ongeoorloofde toegang tot leermiddelen, waardoor de continuïteit van onderwijsdiensten en -activiteiten wordt gewaarborgd.

- **Bevordering van verantwoord digitaal burgerschap**

Voor sommige deelnemers aan het proces kan het de eerste gelegenheid zijn om betrokken te zijn bij de manier van training die wordt gegeven in een digitale omgeving of die een digitale omgeving gebruikt om trainingsmateriaal te maken, te beheren en te delen, kennisdeling en communicatie met andere deelnemers via digitale middelen uitvoert, of digitale hulpmiddelen gebruikt om administratieve taken uit te voeren tijdens de training. Organisaties in beroepsonderwijs en -opleiding hebben de verantwoordelijkheid om hun studenten en medewerkers die bij de opleiding betrokken zijn, voor te lichten over veilige en verantwoorde digitale praktijken. Door onderwijs in digitale hygiëne te integreren in het curriculum en de opleidingsprogramma's van beroepsonderwijs en -opleiding, geven instellingen leerlingen de kennis, vaardigheden en attitudes die nodig zijn om effectief door het digitale landschap te navigeren, hun online identiteit te beschermen en een positieve bijdrage te leveren aan de digitale samenleving.

- **Voorbereiding op toekomstige carrières**

In het huidige digitale tijdperk zijn digitale geletterdheid en bewustzijn van cyberbeveiliging essentiële vaardigheden voor mensen die de arbeidsmarkt betreden. Hoewel het leren van sommige vaardigheden met betrekking tot digitale hygiëne misschien niet het hoofddoel van een student is, kan deelname aan training

hen kansen bieden om die vaardigheden te verbeteren die in de toekomst nuttig kunnen blijken te zijn. De opleiders en organisatoren van opleidingen moeten zich er ook van bewust zijn dat het nodig kan zijn om tijd en middelen voor dit specifieke doel uit te trekken. Door digitale hygiënepraktijken te promoten, rusten organisaties in beroepsonderwijs en -opleiding studenten uit met de fundamentele kennis en vaardigheden die nodig zijn om digitale uitdagingen in hun toekomstige loopbaan aan te gaan, zowel in traditionele als in digitale industrieën. Hetzelfde geldt ook voor de opleiders die door deelname aan de training met behulp van digitale omgevingen en tools hun onderwijspraktijk veilig en verantwoord modern houden en mogelijk nieuwe kansen voor hun carrière tegenkomen.

Over het algemeen is digitale hygiëne belangrijk voor organisaties in beroepsonderwijs en -opleiding op bedrijfsniveau en voor individuele werknemers en hun klanten om gevoelige informatie te beschermen, de reputatie van de instelling te behouden, te voldoen aan regelgeving, leren en lesgeven te ondersteunen, cyberbeveiligingsrisico's te beperken, verantwoord digitaal burgerschap te bevorderen en studenten en tot op zekere hoogte ook hun trainers en andere werknemers voor te bereiden op succes in een digitale wereld. Door prioriteit te geven aan digitale hygiëne, kunnen organisaties voor beroepsonderwijs en -opleiding een veilige, beveiligde en bevorderlijke leeromgeving creëren die leerlingen in staat stelt te gedijen in het digitale tijdperk.

# Deel 2 - Vaardigheden en vereisten voor opleiders en opvoeders in beroepsonderwijs en -opleiding

## Rollen en verantwoordelijkheden voor organisaties in beroepsonderwijs en -opleiding

Laten we eerst beginnen met wie de rollen kunnen zijn die betrokken zijn bij de opleiding in beroepsonderwijs en -opleiding die op de hoogte moeten zijn van digitale hygiënekwesties en over de respectieve vaardigheden moeten beschikken. Afhankelijk van de situaties bij het geven van en deelnemen aan de training die wordt gegeven in digitale omgevingen en het gebruik van digitale hulpmiddelen, kunnen opleiders en opleiders in beroepsonderwijs en -opleiding te maken krijgen met verschillende indelingen van individuele taken die door deelnemers aan het proces worden uitgevoerd. Daarom kan het implementeren en beheren van digitale hygiëne in een organisatie voor beroepsonderwijs en -opleiding coördinatie en samenwerking vereisen tussen verschillende belanghebbenden met verschillende rollen en verantwoordelijkheden. Trainers kunnen de luxe hebben om te worden ondersteund door een volgroeid IT-personeel om zich te houden aan de technische aspecten van de training, of ze moeten vertrouwen op hun vaardigheden en kennis. Om die reden kunnen de vaardigheden en vereisten voor de opleiders en opvoeders van beroepsonderwijs en -opleiding variëren, afhankelijk van de organisatie waarvan zij deel uitmaken.

Er zijn verschillende typische rollen en verantwoordelijkheden voor personen die betrokken kunnen zijn bij het proces of de training in de digitale omgeving van vandaag, elk met hun eigen opdrachten en vaardigheidsvereisten:

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

De CIO of CTO houdt zich voornamelijk bezig met het ontwikkelen van en toezicht houden op de digitale hygiënestrategie, het beleid en de procedures van de organisatie. Ze nemen deel aan het bepalen van de doelen voor de organisaties met digitale hygiëne en cyberbeveiliging in het achterhoofd. Hun verantwoordelijkheden omvatten het zorgen voor afstemming van de inspanningen op het gebied van digitale hygiëne op de algemene IT- en beveiligingsdoelstellingen van de organisatie, het toewijzen van middelen en budget voor initiatieven op het gebied van digitale hygiëne en cyberbeveiligingsmaatregelen, en het bieden van leiderschap en begeleiding aan IT- en beveiligingsteams die verantwoordelijk zijn voor het implementeren van digitale hygiënepraktijken.

- **IT-beveiligingsmanager of cyberbeveiligingsfunctionaris**

Sommige organisaties hebben mogelijk een speciale functie van IT-beveiligingsmanager of een cyberbeveiligingsfunctionaris of iemand die de rol vervult als onderdeel van hun functieomschrijving. Een dergelijke rol zou cyberbeveiligingscontroles, waarborgen en risicobeheersmaatregelen ontwerpen en implementeren om systemen, netwerken en gegevens voor beroepsonderwijs en -opleiding te beschermen.

Ze zouden ook regelmatig beveiligingsbeoordelingen, audits en kwetsbaarheidsscans uitvoeren om potentiële bedreigingen en kwetsbaarheden te identificeren en te beperken, beveiligingsincidenten te monitoren, te reageren op cyberbeveiligingsincidenten en incidentresponsactiviteiten te coördineren. Af en toe ontwikkelt en levert deze rol cyberbeveiligingstrainingen en bewustmakingsprogramma's voor personeel, waardoor zij de rol van opleider in beroepsonderwijs en -opleiding op zich nemen. Soms kunnen ze ook worden uitgenodigd om studenten op te leiden om als experts goede digitale hygiënepraktijken buiten hun organisatie te promoten.

- **IT-beheerder of systeembeheerder**

IT-beheerders zijn verantwoordelijk voor het beheer van de IT-infrastructuur voor de organisatie en kunnen sommige opdrachten voor de opleiders van het beroepsonderwijs uitvoeren, soms op de achtergrond, zonder dat ze dit opmerken. Hun verantwoordelijkheden omvatten het onderhouden en beheren van VET-systemen, servers en netwerkinfrastructuur volgens digitale hygiënenormen en best practices; het beheren van gebruikersaccounts, toegangscontroles en machtigingen om veilige toegang tot middelen en gegevens voor beroepsonderwijs en -opleiding te garanderen; Het installeren, configureren en bijwerken van beveiligingssoftware, patches en firmware om te beschermen tegen bekende kwetsbaarheden en exploits die kunnen optreden bij het gebruik van digitale tools en het uitvoeren van acties tijdens de training, zoals het delen van trainingsmateriaal of communicatie tussen de deelnemers. Ze zijn ook verantwoordelijk voor het bewaken van systeemlogboeken en waarschuwingen voor verdachte activiteiten, ongeoorloofde toegangspogingen of inbreuken op de beveiliging.

- **Functionaris Gegevensbescherming (FG) of Privacy Officer**

Functionarissen voor gegevensbescherming spelen een belangrijke rol bij beroepsonderwijs en -opleiding, aangezien er op nationaal en internationaal niveau regels en voorschriften zijn die zorgvuldige aandacht vereisen voor de manier waarop beroepsonderwijsorganisaties de gevoelige gegevens van de deelnemers aan de opleiding beheren. Deze rol zorgt voor de naleving van de regelgeving inzake gegevensbescherming en de privacywetgeving met betrekking tot het verzamelen, gebruiken en opslaan van persoonsgegevens in VET-omgevingen; ontwikkelt en onderhoudt beleid, procedures en documentatie voor gegevensbescherming, met inbegrip van gegevensbeschermingseffectbeoordelingen (DPIA's) en privacyverklaringen; behandelt verzoeken om toegang van betrokkenen, privacyklachten en vragen met betrekking tot gegevensbescherming en privacypraktijken, werkt samen met IT- en juridische teams om incidenten, inbreuken en inbreuken op de privacy op het gebied van gegevensbeveiliging aan te pakken.

- **Onderwijstechnoloog of onderwijsontwerper**

Hoewel eerdere rollen in elke organisatie kunnen voorkomen, is de onderwijstechnoloog of instructieontwerper direct gerelateerd aan training en opleiding die door de organisatie worden uitgevoerd.

Hun verantwoordelijkheden omvatten het integreren van digitale hygiëneprincipes en -praktijken in het curriculum van beroepsonderwijs en -opleiding, instructiemateriaal en leeractiviteiten; het bieden van training en ondersteuning aan opvoeders en onderwijzend personeel bij het opnemen van digitale hygiëne-educatie in onderwijspraktijken, het evalueren en aanbevelen van educatieve technologische hulpmiddelen en bronnen die prioriteit geven aan beveiliging, privacy en toegankelijkheid voor lerenden in beroepsonderwijs en -opleiding.

- **Eindgebruikers (medewerkers en studenten)**

De laatste rol is vaak verdeeld in twee groepen, maar ze hebben allebei vergelijkbare verantwoordelijkheden met betrekking tot digitale hygiëne. Van eindgebruikers wordt verwacht dat ze het digitale hygiënebeleid, de richtlijnen en de beste praktijken volgen bij het gebruik van systemen, apparaten en online bronnen voor beroepsonderwijs en -opleiding. Het opleidingspersoneel van de organisatie kan door het bedrijf worden verplicht om trainings- of administratieve activiteiten uit te voeren op een specifieke manier die is vastgelegd in de regels en het beleid van de organisatie. Als zodanig kunnen zij worden verplicht om deel te nemen aan bewustmakingstrainingen en onderwijsinitiatieven op het gebied van cyberbeveiliging om hun begrip van digitale risico's en verantwoordelijkheden te vergroten en beveiligingsincidenten, verdachte activiteiten en cyberbeveiligingsproblemen te melden aan het juiste IT- of beveiligingspersoneel voor onderzoek en oplossing. Opleiders in beroepsonderwijs en -opleiding moeten zich echter bewust zijn van hun rol als begeleiders van de studenten die mogelijk begeleiding nodig hebben bij het gebruik van een digitale omgeving die hen tijdens de opleiding misschien niet bekend is.

Een persoon in een organisatie voor beroepsonderwijs en -opleiding kan tijdens de training meerdere rollen tegelijk vervullen of zich slechts op een paar verantwoordelijkheden kunnen concentreren. Hoe dan ook, door duidelijke rollen en verantwoordelijkheden te definiëren voor personen die betrokken zijn bij de implementatie en het beheer van digitale hygiëne in een organisatie voor beroepsonderwijs en -opleiding, kunnen instellingen effectief samenwerken om een cultuur van cyberbeveiligingsbewustzijn tot stand te brengen, goede digitale hygiënepraktijken te bevorderen en de vertrouwelijkheid, integriteit en beschikbaarheid van middelen en gegevens voor beroepsonderwijs en -opleiding te beschermen. Organisaties zullen echter van die personen eisen dat ze over bepaalde vaardigheden en kennis beschikken om de bovengenoemde praktijken uit te voeren.

## Kaders voor digitale vaardigheden

Er zijn bestaande competentiekaders opgesteld om de reeks vaardigheden te beschrijven die moeten beschikken over degenen die betrokken zijn bij het uitvoeren van verschillende activiteiten in een digitale omgeving. Sommige omvatten algemene digitale vaardigheden, terwijl andere specifieker zijn voor de kwesties van cyberbeveiliging en digitale hygiëne. De volgende kaders zijn nuttig bij het identificeren van

digitale hygiënevaardigheden voor opleiders en opleiders in beroepsonderwijs en -opleiding en bij het identificeren van de mogelijke opleidingsbehoeften voor de studenten die deelnemen aan onderwijs in de digitale omgeving.

- **Digitaal competentiekader voor burgers (DigComp) [1]**

Het DigComp 2.2-framework, ontwikkeld door de Europese Commissie, is de nieuwste versie van het Digital Competence Framework for Citizens. Het definieert de belangrijkste componenten van digitale competentie op vijf gebieden: informatie- en datageletterdheid, communicatie en samenwerking, creatie van digitale inhoud, veiligheid en probleemoplossing. Elk gebied is verder onderverdeeld in specifieke competenties die de vaardigheden en kennis beschrijven die nodig zijn om bekwaam te zijn in digitale omgevingen.

Dit kader dient als leidraad voor individuen om hun digitale vaardigheden te beoordelen en te verbeteren, en voor opvoeders en beleidsmakers om curricula en beleid te ontwerpen die digitaal onderwijs en digitale opleiding ondersteunen. DigComp 2.2 introduceert ook vaardigheidsniveaus en gebruiksvoorbeelden, waardoor het praktisch is voor verschillende educatieve en professionele omgevingen. Het raamwerk benadrukt het belang van effectief en kritisch kunnen opereren in een digitale samenleving.

- **Europees kader voor e-competentie (E-CF) [2]**

Het European e-Competence Framework (e-CF) is een gestandaardiseerd kader om de competenties, vaardigheden en vaardigheidsniveaus van professionals op het gebied van informatie- en communicatietechnologie (ICT) te beschrijven en dat is ontwikkeld om de groei en mobiliteit van ICT-professionals te ondersteunen. Het raamwerk bestaat uit vijf competentiegebieden die verband houden met ICT, zoals Plan, Build, Run, Enable en Manage. Het bevat in totaal 41 competenties en omvat vaardigheidsniveaus die de kennis, vaardigheden en autonomie op elk niveau beschrijven, variërend van Foundation tot Expert. Het bevat ook voorbeelden van kennis en vaardigheden met betrekking tot de competenties.

De e-CF is bedoeld om organisaties, HR-managers, trainers en opvoeders te helpen bij het ontwikkelen van functies en carrièrepaden voor ICT-professionals, het verbeteren van het personeelsbeheer en het bevorderen van professionele ontwikkeling in de ICT-sector. Het dient ook als een instrument voor beleidsontwikkeling, onderwijs en opleiding op elkaar af te stemmen binnen de digitale markt van Europa.

- **Europees kader voor cyberbeveiligingsvaardigheden (ECSF) [3]**

Het European Cybersecurity Skills Framework (ECSF) is ontworpen om vaardigheden, rollen en competenties op het gebied van cyberbeveiliging in heel Europa te harmoniseren en te standaardiseren. Het dient als een basisstructuur voor het ontwikkelen en beoordelen van cyberbeveiligingsvaardigheden, gericht op het aanpakken van de lacunes in cyberbeveiligingsvaardigheden en het verbeteren van de

cyberbeveiligingshouding van organisaties en landen. De ECSF categoriseert cyberbeveiligingsvaardigheden in verschillende gebieden, waarbij specifieke rollen en competenties worden beschreven die vereist zijn op het gebied van cyberbeveiliging. Het schetst de belangrijkste cyberbeveiligingsrollen die doorgaans nodig zijn voor organisaties, specifieke vaardigheden en capaciteiten die nodig zijn om effectief te presteren in deze rollen, en vaardigheidsniveaus of expertiseniveaus, van beginner tot expert, die vereist zijn voor elke competentie.

Dit kader is nuttig voor verschillende belanghebbenden, waaronder onderwijsinstellingen, bedrijven en beleidsmakers, om curricula, trainingsprogramma's en loopbaantrajecten in cyberbeveiliging te ontwikkelen. Het ondersteunt het creëren van duidelijke loopbaanstructuren op het gebied van cyberbeveiliging, waardoor het gemakkelijker wordt om tekorten aan vaardigheden op te sporen en effectief aan te pakken.

- **Kader voor digitale competenties voor opvoeders (DigCompEdu) [4]**

Het DigCompEdu-framework beschrijft de vereisten voor de ontwikkeling van digitale competenties van docenten. Het is specifiek op maat gemaakt voor leerkrachten op alle onderwijsniveaus, van kleuteronderwijs tot hoger onderwijs en volwassenenonderwijs, en het richt zich op het verbeteren van de digitale vaardigheden die nodig zijn voor effectief lesgeven in steeds digitalere leeromgevingen. Het raamwerk is gestructureerd rond zes competentiegebieden van professionele betrokkenheid (Digitale technologieën gebruiken voor communicatie, samenwerking en professionele ontwikkeling.), digitale bronnen (Digitale bronnen creëren en wijzigen en effectief beheren.), onderwijzen en leren (Digitale technologieën inzetten voor het voorbereiden, implementeren en beheren van het onderwijs- en leerproces.), beoordeling (Digitale technologieën gebruiken voor beoordeling van, voor en als leren.), empowerment van lerenden (digitale hulpmiddelen gebruiken om inclusie, personalisatie en actieve betrokkenheid van lerenden te verbeteren.), het bevorderen van de digitale competentie van lerenden (strategische bevordering van de digitale vaardigheden van lerenden en veilig en verantwoord gebruik van digitale hulpmiddelen.). Bovendien identificeert het DigCompEdu-raamwerk 22 individuele competenties en vaardigheidsniveaus die variëren van 'nieuwkomer' tot 'pionier', en biedt het een pad voor de ontwikkeling van docenten in hun digitale praktijken.

Dit kader dient als leidraad voor docenten om hun digitale competenties te beoordelen en te verbeteren en ondersteunt onderwijsinstellingen bij het ontwerpen van trainingsprogramma's en -beleid dat is afgestemd op de hedendaagse onderwijsbehoeften.

De hierboven genoemde kaders zijn weliswaar algemeen voor het identificeren van de behoeften van personen en organisaties die deelnemen aan een praktijk in de digitale omgeving, maar bieden een gestructureerd beeld van de reikwijdte van de vaardigheden die van opleiders en opvoeders in beroepsonderwijs en -opleiding worden verlangd.

## Vaardigheden voor opleiders en opvoeders in beroepsonderwijs en -opleiding

Tot op zekere hoogte verschillen opleiders en opleiders in beroepsonderwijs en -opleiding niet van andere deelnemers aan de digitale omgeving. Om die reden zijn de vaardigheden die ze nodig hebben om zich te houden aan goede digitale hygiënepraktijken vaardigheden die iedereen zou moeten bezitten. Deze vaardigheden omvatten een reeks technische, gedrags- en cognitieve vaardigheden. Ze zijn ook een subset van vaardigheden die kunnen worden aangeduid als moderne of toekomstige vaardigheden en op basis van de recente ontwikkeling van de digitale omgeving zijn dit dezelfde vaardigheden die zijn benadrukt als vaardigheden die cruciaal zijn voor organisaties of de nabije toekomst, zoals het gebruik van cloudtechnologieën, het analyseren van big data en het gebruik van kunstmatige-intelligentietools om de werkproductiviteit en efficiëntie te verbeteren [5,6].

De aard van hun werk vereist echter dat opleiders en opleiders in beroepsonderwijs en -opleiding meer aandacht besteden aan de manier waarop zij met gegevens omgaan en omgaan met andere deelnemers aan het opleidingsproces. Hier zijn enkele belangrijke vaardigheden die nodig zijn voor opleiders en opvoeders in beroepsonderwijs en -opleiding met betrekking tot goede digitale hygiëne:

- **Algemeen bewustzijn van cyberbeveiliging**

De vaardigheid omvat het begrijpen van veelvoorkomende online bedreigingen zoals malware, phishing en social engineering-aanvallen, en weten hoe u deze kunt herkennen en erop kunt reageren; weten hoe u veilig op internet kunt surfen, inclusief het vermijden van verdachte websites, het gebruik van beveiligde verbindingen (HTTPS) en voorzichtig zijn bij het downloaden van bestanden of het klikken op links.

- **Gegevensbescherming en privacy**

De vaardigheid omvat het kunnen versleutelen van gevoelige gegevens, zowel tijdens het transport als in rust, en weten hoe gegevens veilig kunnen worden verwijderd of verwijderd wanneer dat nodig is; en begrijpen hoe u privacy-instellingen op verschillende online platforms en apparaten kunt configureren om het delen van persoonlijke informatie te beheren.

- **Apparaatbeveiliging en -beheer**

Deze vaardigheid omvat de praktijk van het regelmatig bijwerken van software, besturingssystemen en applicaties om beveiligingsproblemen te patchen en te beschermen tegen bekende exploits; de mogelijkheid om sterke, unieke wachtwoorden voor verschillende accounts te maken en wachtwoordbeheertools effectief te gebruiken om wachtwoorden veilig op te slaan en te beheren; De praktijk van het inschakelen en beheren van multi-factor authenticatie, indien beschikbaar, om een extra beveiligingslaag toe te voegen aan online accounts.

- **Veilige digitale communicatie**

Deze vaardigheid omvat het oefenen van veilige communicatiepraktijken, zoals het gebruik van versleutelde e-maildiensten of het selecteren en gebruiken van beveiligde berichten-apps bij het delen van vertrouwelijke informatie of het communiceren met studenten, collega's, collega's of partners buiten de organisatie voor beroepsonderwijs en -opleiding; het naleven van richtlijnen voor het identificeren en vermijden van phishing-e-mails, oplichting en andere social engineering-tactieken die VET-systemen in gevaar kunnen brengen of tot datalekken kunnen leiden.

- **Beheer van digitale voetafdruk**

Deze vaardigheid omvat het begrijpen van de implicaties van iemands digitale voetafdruk en het nemen van stappen om de blootstelling van persoonlijke informatie online te minimaliseren; het adviseren van deelnemers aan de training om hetzelfde te doen.

- **Kritisch denken**

Deze vaardigheid omvat het ontwikkelen en toepassen van kritische denkvaardigheden om de geloofwaardigheid van online bronnen te evalueren, verkeerde informatie en oplichting te identificeren en weloverwogen beslissingen te nemen over online activiteiten bij het uitvoeren of voorbereiden van de training.

- **Continu leren**

Deze vaardigheid omvat deelname aan de algemene praktijk van het verbeteren van iemands vaardigheid; het aanleren van nieuwe instrumenten en benaderingen voor opleiding in een digitale omgeving of het gebruik van moderne digitale hulpmiddelen; en op de hoogte blijven van evoluerende cyberbeveiligingsbedreigingen, privacykwesties en best practices door middel van voortdurende opleiding en training.

- **Digitaal burgerschap en ethiek**

Deze vaardigheid omvat het beoefenen van verantwoordelijk digitaal burgerschap bij het uitvoeren van beroepsopleidingen door zich te houden aan de regelgeving en de rechten van andere personen en organisaties te respecteren; het bevorderen van verantwoord digitaal burgerschap onder studenten door ethisch gedrag, respectvolle communicatie en digitale etiquette aan te leren in online omgevingen; het bevorderen van analytische denkvaardigheden om studenten te helpen de geloofwaardigheid van online informatie te beoordelen, digitale risico's te herkennen en weloverwogen beslissingen te nemen over hun online activiteiten; het beschermen van de digitale reputatie van personen en organisaties die deelnemen aan het proces.

Deze vaardigheden kunnen worden verwezen naar het eerder beschreven DigCompEdu-framework, maar ze komen mogelijk niet rechtstreeks overeen met individuele competenties die in die frameworks zijn opgenomen. In plaats daarvan zijn er elementen in de beschrijvingen van de competentiegebieden in het kader die overeenkomen met de vaardigheden die nuttig zijn voor opleiders en opvoeders in beroepsonderwijs en -opleiding.

*Tafel 1. Koppeling van voorgestelde vaardigheden van opleiders in beroepsonderwijs en -opleiding aan de competentiegebieden van DigCompEdu.*

| Vaardigheid van VET Trainer | Competentiegebied DigCompEDU |
|---|---|
| **Algemeen bewustzijn van cyberbeveiliging** | • Leerlingen mondiger maken<br>• Bevordering van de digitale competentie van lerenden |
| **Gegevensbescherming en privacy** | • Digitale bronnen<br>• Bevordering van de digitale competentie van lerenden |
| **Apparaatbeveiliging en -beheer** | • Onderwijzen en leren<br>• Bevordering van de digitale competentie van lerenden |
| **Veilige digitale communicatie** | • Professionele betrokkenheid<br>• Beoordeling |
| **Beheer van digitale voetafdruk** | • Digitale bronnen<br>• Bevordering van de digitale competentie van lerenden |
| **Kritisch denken** | • Onderwijzen en leren<br>• Bevordering van de digitale competentie van lerenden |
| **Continu leren** | • Professionele betrokkenheid<br>• Bevordering van de digitale competentie van lerenden |
| **Digitaal burgerschap en ethiek** | • Leerlingen mondiger maken<br>• Bevordering van de digitale competentie van lerenden |

De vaardigheden bieden de opleiders en opvoeders van beroepsonderwijs en -opleiding de middelen om deel te nemen aan educatieve activiteiten en zich te houden aan de beste praktijken op het gebied van digitale hygiëne. Een nuchtere referentie van enkele van de beste praktijken is beschikbaar als een spiekbriefje voor digitale hygiëne [7]. Het beschrijft 12 principes van een veilig digitaal leven die allemaal enige kennis van de digitale wereld vereisen, waaronder:

- het up-to-date houden van uw werkende software, antivirus, firewall, enz.,
- het gebruik van veilige wachtwoorden, het veilig beheren ervan en het gebruik van multi-factor authenticatie,
- voorzichtig zijn bij het downloaden van software,

- op de hoogte zijn van phishing en andere verdachte pogingen om uw vermogen in gevaar te brengen,
- het beperken van uw digitale en sociale voetafdruk,
- het aannemen van een algemene "security first"-mentaliteit bij het omgaan met informatie in de digitale omgeving.

In opleiding en onderwijs in beroepsonderwijs en -opleiding is het verwerven en oefenen van digitale hygiënevaardigheden belangrijk om een veilige omgeving voor informatie-uitwisseling te bieden.

# Unit 3 - Digitale hygiëne aanpassen in het curriculum en de opleiding van beroepsonderwijs en -opleiding

Onderwerpen op het gebied van digitale hygiëne zouden een dagelijks onderdeel moeten zijn van de opleiding in beroepsonderwijs en -opleiding. Opleiders en opleiders in beroepsonderwijs en -opleiding moeten de richtsnoeren voor goede digitale hygiëne volgen bij het plannen en beheren van de opleiding waarbij het gebruik van digitale hulpmiddelen wordt toegepast als onderdeel van de opleidingsomgeving; het produceren en distribueren van opleidingsmateriaal; het organiseren van peer-to-peer en trainer-to-student communicatie; het analyseren van de trainingsresultaten; en het uitvoeren van administratieve procedures en het plannen van de verbetering van het opleidingsproces.

Bovendien moeten opleiders in beroepsonderwijs en -opleiding zich ervan bewust zijn dat, hoewel het onderwerp van de opleiding misschien geen onderwerpen zijn die verband houden met de digitale wereld, een deel van deze informatie nodig kan zijn om de doeltreffendheid van de gegeven opleiding te vergroten. Trainers moeten zich bewust blijven van de mogelijke achtergronden van hun studenten en het schema van de training aanpassen door tijd en moeite te reserveren voor de uitleg en demonstratie van enkele trainingspraktijken die zullen leiden tot een betere digitale hygiëne voor hun studenten.

Natuurlijk kunnen digitale hygiëne en andere gerelateerde onderwerpen soms het eigenlijke hoofdonderwerp van de training zijn. In die gevallen kunnen opleiders en opleiders in beroepsonderwijs en -opleiding hun studenten begeleiden terwijl ze nieuwe kennis opdoen en nieuwe vaardigheden verwerven met betrekking tot digitale hygiëne.

Digitale hygiëne vanuit het perspectief van opleiders in beroepsonderwijs en -opleiding kan worden gezien als de praktijk van het onderhouden en waarborgen van veilige en productieve digitale activiteiten tijdens de opleiding die wordt gegeven, ongeacht het onderwerp van de opleiding. Voor verschillende aspecten van beroepsonderwijs en onderwijs kan het gebruik van een digitale omgeving nodig zijn om de opleidingsresultaten te verbeteren en de tevredenheid van de studenten die aan de opleiding deelnemen te vergroten. Trainers moeten zich bewust zijn van de invloed van het gebruik van digitale hulpmiddelen op het opleidingsproces en proberen een aantal aspecten die verband houden met digitale hygiëne in de opleiding zelf te integreren. Hier zijn enkele van de opties om het trainingsproces te verbeteren:

- **Onderwerpen en cursusmodules over digitale veiligheid**

Bij het aanbieden van trainingsinhoud, het voorstellen om een specifieke trainingsactiviteit te starten of het verplichten van de studenten om een administratieve activiteit uit te voeren die verband houdt met training, introduceer dan wat advies in de vorm van kleinere trainingsonderwerpen of uitgebreidere modules die studenten leren over de basisprincipes van cyberbeveiliging, zoals wachtwoordbeheer, het herkennen van

phishing-pogingen en het beveiligen van persoons- en werkplekgegevens. Indien beschikbaar, stem deze onderwerpen af op de specifieke industrieën, werkgebieden, werkrollen of activiteiten die studenten hebben die verband houden met het huidige werk van de student of de verwachte baan of toekomstige functie die ze voorbereiden om te betreden, waardoor de informatie relevant en toepasbaar wordt.

- **Praktische workshops, individueel en groepswerk**

Bij het uitvoeren van praktijkopdrachten tijdens de opleiding, zoals bijvoorbeeld praktijkworkshops of individuele of groepswerkopdrachten, implementeer workshops waar studenten kunnen oefenen met het opzetten van beveiligde netwerken, het gebruik van VPN's, het installeren en beheren van beveiligingssoftware en het uitvoeren van regelmatige beveiligingscontroles; Of laat ze ervaren hoe sommige van de fouten waarvan ze zich misschien niet bewust zijn, presteren in een veilige leeromgeving, mogelijk tot problemen kunnen leiden. Een hands-on aanpak en mogelijkheden voor vallen en opstaan helpen de theoretische kennis te verstevigen door praktische toepassing.

- **Ethiek en naleving**

Neem tijdens de training discussies op en bied begeleiding over ethisch gedrag online en de juridische implicaties van digitale acties als de theoretische trainingsonderwerpen of praktische opdrachten implicaties hebben voor bepaald gedrag. Dit kan betrekking hebben op onderwerpen als gegevensprivacywetten die relevant zijn voor het onderwerp van de training of de rollen en het professionele gedrag van de studenten, ethisch hacken en het belang van het onderhouden van een professionele online aanwezigheid.

- **Beheer van digitale voetafdruk**

Leer studenten over het beheren van hun digitale voetafdrukken en benadruk de langetermijneffecten van online activiteiten op de persoonlijke en professionele reputatie. Training kan bestaan uit het effectief gebruiken van sociale media, het beheren van digitale inhoud en het begrijpen van de gevolgen van online berichten. Leer studenten hoe digitale tools die voor werk worden gebruikt ook een digitale voetafdruk kunnen creëren en hoe de studenten hun werkresultaten en de resultaten van anderen die tijdens de samenwerking worden verworven, moeten beheren.

- **Continu leren**

Houd er rekening mee dat moderne digitale landschappen voortdurend veranderen. Op basis van hun rol en het werk waar ze vandaan komen of verwachten lid te worden, kunnen studenten nieuwe kennis nodig hebben over onderwerpen die verband houden met het gebruik van nieuwe digitale tools. Het is belangrijk om op de hoogte te blijven van de nieuwste technologieën en op de hoogte te zijn van de nieuwste bedreigingen die van invloed kunnen zijn op de studenten die het onderwerp van de training leren. Het vergroten van het bewustzijn van nieuwe opties in de digitale omgeving en het introduceren van nieuwe tools bij de studenten kan leiden tot een hogere waargenomen kwaliteit van de training en het verbeteren

van de kennis en vaardigheden van de studenten. Het zoeken naar mogelijkheden voor continu leren en certificering in digitale beveiligingspraktijken kan een integraal onderdeel van het curriculum worden, ongeacht de belangrijkste trainingsonderwerpen.

- **Beoordeling en certificering**

Assessments maken deel uit van trainingen. Afhankelijk van het onderwerp en de doelen van de training kunnen assessments meer of minder formeel zijn en kunnen ze het gebruik van digitale hulpmiddelen omvatten om de assessment uit te voeren en om de assessmentresultaten te verzamelen en te analyseren. Het is een goede gewoonte om ervoor te zorgen dat de studenten op de hoogte zijn van het juiste gebruik van beoordelingsinstrumenten. De inhoud van de assessments kan bestaan uit het toetsen van de kennis en vaardigheden die specifiek zijn opgedaan op het gebied van digitale hygiëne en de kennis van algemene onderwerpen. Beoordeling en certificeringen kunnen worden gebruikt om studenten te stimuleren en de vorm waarin de resultaten worden gepresenteerd, kan extra nadenken over de digitale omgeving vereisen. De studenten kunnen hulp nodig hebben bij het verkrijgen en verwerken van hun nieuwe certificeringsinformatie of het gebruik van hun nieuwe kwalificaties om hun inzetbaarheid te vergroten.

Het is u misschien opgevallen dat sommige opties voor de verbetering van de opleiding in beroepsonderwijs en -opleiding op het gebied van digitale hygiëne overeenkomen met eerder geïdentificeerde vaardigheden. Al deze elementen kunnen worden opgenomen in programma's voor beroepsonderwijs en -opleiding en vanuit twee verschillende perspectieven worden bekeken: welke digitale hygiënevaardigheden moeten worden gebruikt als onderdeel van de training en vereisen extra aandacht tijdens de training; En wat zijn de extra mogelijkheden om de kennis en vaardigheden op het gebied van digitale hygiëne tijdens de training te verbeteren, naast de hoofdonderwerpen. Het aanpakken van deze elementen kan de kwaliteit van de training verbeteren en de studenten extra voordelen bieden in hun werkomgeving die sterk afhankelijk is van de opties van de digitale wereld.

Vanuit praktisch oogpunt betekent dit dat opleiders en opleiders in beroepsonderwijs en -opleiding: veilige leeromgevingen en -instrumenten moeten introduceren die specifiek voor opleiding zijn bestemd, richtsnoeren moeten opstellen voor het omgaan met opleidingsmateriaal, communicatiemiddelen moeten gebruiken en communicatie moeten uitvoeren met het oog op de bescherming van persoonsgegevens en bedrijfseigen informatie, gegevens over het opleidingsproces en de resultaten moeten beheren, die vaak gevoelige informatie bevatten;  en volg en geef het algemene advies dat het naleven van goede digitale hygiënepraktijken vergemakkelijkt.

# Unit 4 – Voorbeeld van goede praktijken – Digitale hygiëne voor beroepsonderwijs en -opleiding

Laten we eens kijken naar een voorbeeld van een goede praktijk van hoe digitale hygiëne kan worden geïntroduceerd in de organisatie van beroepsonderwijs en -opleiding voor de veiligheid van de organisatie en het gebruik van opleiders in beroepsonderwijs en -opleiding en de studenten die deelnemen aan de opleiding.

## Beschrijving van de situatie

Een bedrijf voor beroepsonderwijs en -opleiding wil online training bieden aan hun studenten om kostbare en tijdrovende reizen te vermijden en om de studenten het gemak te bieden om de training vanuit hun veilige fysieke omgeving bij te wonen. Het bedrijf voor beroepsonderwijs en -opleiding heeft een staf van interne en externe trainers die verschillende eerdere ervaringen hebben met het geven van online training en mogelijk verschillende kennis en vaardigheden hebben met betrekking tot het geven van dergelijke trainingen. Het bedrijf heeft ook interne medewerkers die administratieve activiteiten uitvoeren met betrekking tot training en omgaan met informatie die soms gevoelig is en moet worden aangepakt door de nalevingsregels en -richtlijnen. Doorgaans wordt van de trainers verwacht dat ze de Microsoft Teams-omgeving gebruiken voor het geven van de training, het delen van het trainingsmateriaal en het communiceren met de studenten, terwijl intern ondersteunend personeel Microsoft Teams en e-mail gebruikt voor het beheren van studenten voor, tijdens en na de training en een soort documentopslagsysteem voor het beheren en delen van trainingsmateriaal.

De zaken waar het mbo-bedrijf zich zorgen over maakt zijn:

- verkeerd gebruik van persoonlijke informatie door een van de deelnemers aan de training,
- zorgvuldig gebruik van bedrijfseigen informatie van het bedrijf en de externe partners,
- het beperken van de toegang tot de training tot alleen het beoogde publiek,
- het bieden van een rijke ervaring voor de studenten,
- het behouden van een bepaald niveau van reputatie als een goede aanbieder van trainingsdiensten in de markt.

Laten we eens kijken hoe digitale hygiëneproblemen in deze situatie kunnen worden aangepakt.

## De oplossing

Dit soort situaties is complex en vereist dat er aandacht wordt besteed aan verschillende aspecten die verband houden met digitale hygiëne:

- het organiseren van de inrichting van de Microsoft Teams omgeving en het beheren van gebruikers tijdens de training,
- opleiding van de opleiders die de opleiding geven;
- het uitvoeren van de eigenlijke trainingssessies met de betrokkenheid van studenten en opleiders;
- omgaan met het trainingsmateriaal dat tijdens de training wordt gebruikt,
- het organiseren van de communicatie tussen de trainer en de studenten en tussen de studenten onderling,
- het uitvoeren van evaluaties van de training en het verzamelen van feedback.

Hierna volgt een meer gedetailleerde beschrijving van goede praktijken voor elk van deze aspecten.

### *Installatie- en aanmeldingsbeheer*

**Teams Voor Onderwijs:** Er is een Teams-omgeving opgezet die los staat van de Teams-omgeving en die wordt gebruikt voor de dagelijkse communicatie en kennisdeling door de medewerkers van de mbo-organisatie. Microsoft Teams voor het onderwijs is beschikbaar voor organisaties in beroepsonderwijs en -opleiding die voldoen aan de vereisten van officiële onderwijsorganisaties en biedt extra functies die nuttig zijn voor het geven van de training.

**Single Sign-On (SSO):** Implementatie van SSO met behulp van een gemeenschappelijk authenticatieplatform (zoals Active Directory) werd uitgevoerd om de toegang tot Microsoft Teams, applicaties die worden gebruikt binnen de Microsoft Teams-omgeving en andere tools die centraal en met goedkeuring van de VET-organisatie worden gebruikt, te stroomlijnen tijdens de training werd uitgevoerd.

**Toegangsbeheer op basis van rollen:** Rollen en machtigingen binnen Teams op basis van de positie van de gebruiker zijn toegewezen. Concreet kregen 4 rollen toegewezen, elk met hun eigen rechten in de Teams-omgeving: systeembeheerder, trainingsbeheerder (de persoon die trainingssessies organiseert vóór de training en daarna de trainingsresultaten analyseert), trainer (de persoon die de training en praktijkopdrachten uitvoert en het trainingsmateriaal tijdens de training hanteert) en student, die zorgt voor de juiste toegang tot functies en informatie.

**Veilige authenticatiepraktijken:** Waar nodig werden de gebruikers aan wie meer rechten kregen toegewezen bij het openen van gevoelige informatie, getraind in het gebruik van multi-factor authenticatie (MFA) en sterke wachtwoorden om de beveiliging te verbeteren.

### *Opleiding van de trainers*

**Microsoft Teams-trainingsworkshops:** Speciale workshops voor trainers over het effectief gebruiken van Microsoft Teams werden gepland en uitgevoerd en interne en externe trainers werden uitgenodigd om deel

te nemen aan het ontvangen van richtlijnen voor veilig gedrag in een Teams-omgeving. De training omvatte het maken en beheren van teams en kanalen, het plannen van vergaderingen en het gebruik van samenwerkingsfuncties zoals gedeelde bestanden en chat.

**Training met geavanceerde functies:** Trainers kregen aanvullende training over geavanceerde functies zoals breakout rooms, live-evenementen en het integreren van apps van derden die de trainingservaring kunnen verbeteren en de kans om deze functies te oefenen als praktische opdrachten tijdens de training werd aangeboden.

**Doorlopende ondersteuning:** Voor de trainers die het pand nodig hadden, werden volledig ingerichte fysieke trainingsruimtes aangeboden met beveiligde verbindingen met internet. Voor de opleiders die van plan waren hun gebouwen te gebruiken, werden richtlijnen gegeven voor het veilig uitvoeren van de training. De contactgegevens van speciaal IT-ondersteunend personeel zijn opgezet om trainers te helpen in geval van technische problemen.

### *Het geven van trainingssessies*

**Sessieplanning:** Interne trainingsbeheerders en trainers werden getraind in het gebruik van een agenda om sessies te plannen, herinneringen in te stellen en vooraf een agenda te verstrekken in de uitnodiging voor de vergadering. Er werden geautomatiseerde uitnodigingen opgezet voor de studenten om de risico's van deelname aan de verkeerde trainingssessies te minimaliseren.

**Interactieve functies:** Alle trainers werd geadviseerd om tijdens sessies extra Teams-functies te gebruiken, zoals peilingen, quizzen en whiteboards, om studenten te betrekken en het leren waar mogelijk te verbeteren. Het gebruik van extra tools en functies was toegestaan, maar de trainers werd geadviseerd om de studenten te begeleiden bij het gebruik ervan voor aanvullende informatie of praktische opdrachten.

**Opnamesessies:** Het opnemen van trainingssessies was ernstig beperkt vanwege de AVG en werd alleen uitgevoerd met uitdrukkelijke toestemming van alle studenten. Bij het maken van de opnames werden de opnames veilig opgeslagen en waren ze alleen toegankelijk voor degenen die de trainingssessies bijwoonden, en alleen voor een beperkte tijd. Hoewel opnames in het algemeen als nuttig worden beschouwd voor studenten bij het later bekijken van de trainingsinhoud, moet een organisatie voor beroepsonderwijs en -opleiding zich bewust zijn van de risico's die hieraan verbonden zijn.

**Breakout Rooms:** Breakout rooms voor groepsactiviteiten of discussies werden opgezet door de trainingsbeheerder, er werden toegangsrechten gegeven en er werd een passende training gegeven voor de trainers, zodat trainers van de ene naar de andere ruimte konden springen om de voortgang van de training te begeleiden en te volgen.

### *Omgaan met trainingsmateriaal*

**Bestanden en bronnen delen:** Al het trainingsmateriaal dat tijdens de training werd gebruikt, werd opgeslagen op beveiligde servers. De elektronische sleutels van het trainingsmateriaal of de daadwerkelijke kopieën van het trainingsmateriaal werden beheerd door een toegewijde trainingsbeheerder. Voor minder gevoelige materialen werd de omgeving van Teams zelf gebruikt.

**Collaborative Editing:** Bij het samenwerken aan documenten of presentaties in real-time tijdens de praktijkopdrachten werden de trainers en studenten geadviseerd om officiële software zoals Office 365-integratie te gebruiken en er rekening mee te houden dat de informatie niet te veel wordt gedeeld.

**Versiebeheer:** Versiebeheer van interne documenten die deel uitmaakten van trainingsmateriaal werd geïntroduceerd binnen de VET-organisatie. Alle opleiders werd geadviseerd om de rol van deskundigen voor extern opleidingsmateriaal op zich te nemen en werden aangemoedigd om de interne opleidingsbeheerders te raadplegen voor versies van opleidingsmateriaal, studentenhandleidingen en praktijktests, indien van toepassing, om de reputatieschade van de organisatie voor beroepsonderwijs en -opleiding te beperken door het niet verstrekken van actuele versies van opleidingsmateriaal.

### *Communicatie tussen studenten en opleiders*

**Regelmatige updates:** Teams-chat werd gebruikt om aankondigingen te doen, updates te delen en feedback te geven over trainingssessies.

**Speciale kanalen:** Er werden kanalen gecreëerd voor specifieke trainingssessies en individuele groepen studenten, waardoor gerichte discussies en het delen van bronnen mogelijk werden.

**Privéchats:** Extra privéchats tussen de trainer en de studenten waren beperkt tot alleen situaties waarin beide partijen overeenkwamen om extra communicatie te organiseren en de uitwisseling van de contactgegevens centraal te organiseren.

### *Evaluatie en feedback*

**Feedbackformulieren:** Het gebruik van Microsoft Forms of speciale software die intern door de organisatie voor beroepsonderwijs en -opleiding is ontwikkeld om feedback op trainingssessies te verzamelen, werd afgedwongen. Links naar de software die voor feedback werd gebruikt, werden verspreid via een Teams-omgeving, zodat alleen het beoogde publiek kon deelnemen aan feedback. De toegang tot de informatie in de feedbackformulieren was beperkt tot de interne opleidingsbeheerders van de organisatie voor beroepsonderwijs en -opleiding.

**Prestaties bijhouden:** Opdrachtfuncties binnen Teams om taken te geven, werk te verzamelen en beoordeelde feedback te geven, werden gebruikt.

Deze opzet van zowel de technische omgeving als de procedures en rollen die bij het proces betrokken zijn, zorgt voor een uitgebreide, veilige en interactieve trainingsomgeving met behulp van Microsoft Teams, die voldoet aan de behoeften van zowel trainers als studenten, terwijl een hoge standaard van digitale hygiëne en efficiëntie behouden blijft.

# Bronnen


1. Vuorikari, R., Kluzer, S. and Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.
2. European e-Competence Framework, https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf, [accessed April 15, 2024].
3. European Union Agency for Cybersecurity (ENISA). European Cybersecurity Skills Framework Role Profiles, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles [accessed April 15, 2024].
4. Punie, Y., editor(s), Redecker, C., European Framework for the Digital Competence of Educators: DigCompEdu, EUR 28775 EN, Publications Office of the European Union, Luxembourg, 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. World Economic Forum, “Future of Jobs Report 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. Digital Hygiene Cheat Sheet. https://digitalhygiene.net/ [accessed April 15, 2024].

# Module 2 - Digitale hygiëne Curriculum op maat voor beroepsonderwijs en -opleiding

## Introductie

Digitale hygiëne heeft een veel grotere en belangrijkere rol gespeeld in ons dagelijks leven. Met de snelle groei van digitalisering en de uitbreiding ervan naar alle sferen van menselijke activiteit, is er een dringende behoefte ontstaan om ervoor te zorgen dat onze digitale omgevingen veilig zijn. Een van de belangrijkste en fundamentele waarborgen in dit verband is het waarborgen van een goede digitale hygiëne. Dit geldt met name gezien de groeiende cyberdreigingen waarmee organisaties worden geconfronteerd. Digitale hygiëne richt zich in de eerste plaats op het handhaven van een gezonde en veilige digitale aanwezigheid, en dit is steeds relevanter geworden naarmate meer organisaties hun activiteiten online verplaatsen. Deze module is ontworpen om een robuust curriculum te bieden dat studenten op beroepsniveau kan opleiden in het ontwikkelen, beoordelen en onderhouden van goede digitale hygiënepraktijken.

Door dit programma te volgen, kan de student de vereiste analytische en praktische basisvaardigheden verwerven om effectief te beoordelen, te onderhouden en waar nodig in te grijpen om digitale hygiëne binnen een organisatorische omgeving te waarborgen. Dit is een echt relevant programma vanwege de grote vraag in de markt naar professionals met vaardigheden op dit gebied. Dit ontwikkelingsprogramma is gebenchmarkt aan de hand van best practices binnen dit domein. De focus van dit programma op startups en MKB-professionals vormde de basis voor de keuze van modules en structuur. De essentie is om vaardigheid op dat niveau op te bouwen, wat betekent dat het programma is ontworpen en gestructureerd om toegankelijk te zijn voor degenen die het op parttime of fulltime basis willen volgen. Het programma is ook ontworpen om hands-on en praktijkgericht te zijn met een korte doorlooptijd. Het is echter ook ontworpen om studenten in staat te stellen in hun eigen tempo te gaan.

## Unit 1 – Overzicht van het curriculum

Dit handboek is geschreven om studenten die momenteel zijn ingeschreven of op het punt staan zich in te schrijven voor het programma Beroepsonderwijs en -opleiding (VET) in digitale hygiëne, evenals instructeurs, relevante informatie te verstrekken met betrekking tot het doel, de planning, de structuur en de beoordeling

van het programma. In het besef dat niet alle organisaties hetzelfde zijn en hetzelfde niveau van digitale hygiënevaardigheden vereisen, zijn deze module en de verschillende onderdelen modulair opgebouwd. Hierdoor kunnen personen die bekwaam zijn in bepaalde gebieden zich concentreren op of overstappen naar andere modules naarmate hun behoeften evolueren. Het uiteindelijke doel van dit programma is om een robuuste basis te leggen op het gebied van digitale hygiëne, waardoor zowel studenten als docenten cyberrisico's effectief kunnen beheren en beperken. Dit curriculum is ook ontworpen om substantiële delen van de professionele cyberbeveiligingscertificeringen op basisniveau te dekken, zoals GIAC Security Essentials (GSEC) en de CompTIA Security+. Het biedt daarom een meerwaarde en een verhoogde stimulans voor studenten om deel te nemen aan dit programma.

## Doel en doelstellingen van het programma van de module

De kerndoelstellingen van de module Digitale Hygiëne zijn ontworpen om de cyberbeveiliging van organisaties te verbeteren door deelnemers in staat te stellen om:

- Beoordeel cyberbeveiligingsbedreigingen waarmee organisaties worden geconfronteerd.
- Beoordeel en implementeer de basisbeveiliging van het netwerk.
- Weten hoe u basisversleutelingsprotocollen implementeert en onderhoudt.
- Beoordeel en implementeer gegevensbeheer en beveiligingsprotocollen.
- Beoordeel en pas de basisbeveiligingsprotocollen voor hardware en software toe.
- Beheer de beveiliging in de mobiele omgeving.

## Vakdidactiek

Het programma maakt gebruik van een mix van theoretische instructie en praktische toepassing. Het maakt gebruik van casestudy's, hands-on labsessies en interactieve workshops om ervoor te zorgen dat leerlingen de concepten die ze leren kunnen toepassen in real-world scenario's. Deze aanpak vergroot niet alleen het begrip, maar zorgt er ook voor dat afgestudeerden klaar zijn voor een baan en in staat zijn om onmiddellijk na voltooiing van het programma uitgebreide digitale hygiënepraktijken te implementeren.

## Evaluatie en continue verbetering

De beoordeling binnen het programma Digitale Hygiëne is zowel rigoureus als continu, waarbij gebruik wordt gemaakt van verschillende methoden om de kennis en vaardigheden van de deelnemer te evalueren. Deze omvatten quizzen, praktijkexamens, projectgebaseerde beoordelingen en een sluitstukproject dat het geheel van het leren van de deelnemers omvat. Feedbackmechanismen zijn een integraal onderdeel van het curriculum en bieden deelnemers tijdig inzicht in hun voortgang en verbeterpunten. Bovendien wordt het curriculum zelf regelmatig bijgewerkt om aan te sluiten bij de nieuwste informatie over cyberdreigingen en

technologische ontwikkelingen, waardoor relevantie en doeltreffendheid worden gewaarborgd bij het aanpakken van hedendaagse cyberbeveiligingsuitdagingen.

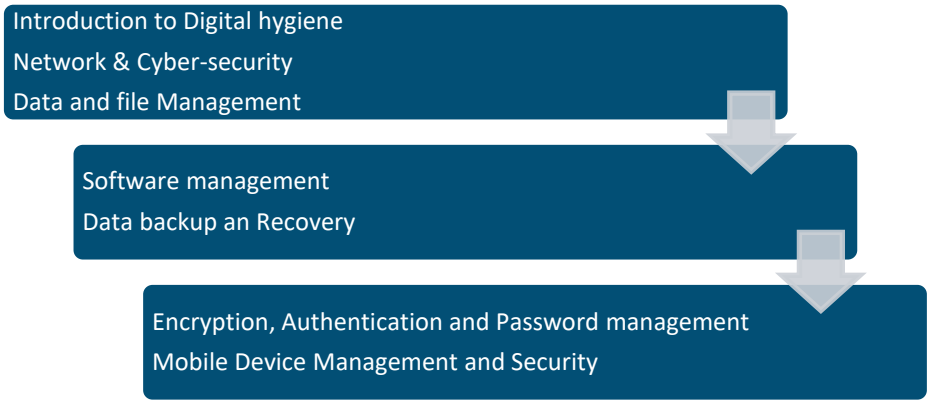
## Conclusie

Het programma Digitale Hygiëne van de instelling voor beroepsonderwijs en -opleiding is niet alleen bedoeld om essentiële kennis en vaardigheden op het gebied van cyberbeveiliging bij te brengen, maar ook om de deelnemers een proactieve en geïnformeerde cyberbeveiligingscultuur bij te brengen. Aan het einde van het programma zijn de deelnemers niet alleen afgestudeerden; Het zijn mondige digitale burgers, uitgerust om aanzienlijk bij te dragen aan de cyberbeveiliging van hun organisaties. Dit uitgebreide programma is een hoeksteen in het voorbereiden van de volgende generatie cyberbeveiligingsprofessionals, klaar om de dynamische uitdagingen van het digitale tijdperk aan te gaan.

# Unit 2 – Belangrijkste leergebieden

## Overzicht van het curriculum

| Code | Leergebieden/vakken |
|---|---|
| D21 | Inleiding tot digitale hygiëne |
| D22 | Netwerk en cyberbeveiliging |
| D23 | Gegevens- en bestandsbeheer |
| D24 | Softwarebeheer |
| D25 | Back-up en herstel van gegevens |
| D26 | Versleuteling, verificatie en wachtwoordbeheer |
| D27 | Beheer en beveiliging van mobiele apparaten |




## Inleiding tot digitale hygiëne

Dit onderwerp is bedoeld om de studenten een uitgebreid overzicht te geven van digitale hygiëne. Dit overzicht biedt zowel een conceptueel overzicht van de inhoud als een deel van de praktische uitwerking bij het bekijken van het programma vanuit een integratief perspectief. De primaire focus zal liggen op het introduceren van de verschillende gebieden van digitale hygiëne en hoe de verschillende vakgebieden met elkaar verbonden zijn en met elkaar in verband staan. Het zal een voorlopig overzicht geven van de basisprincipes en praktijken van digitale hygiëne en hoe de verschillende componenten in elkaar passen. Deze eenheid biedt de fundamentele kennis en het begrip waarop de andere componentgebieden kunnen worden gebouwd.

### *De belangrijkste onderwerpen die in dit onderwerp aan bod komen*

- Inzicht in digitale hygiëne: een verkenning van wat digitale hygiëne is en waarom het van cruciaal belang is in het huidige digitale tijdperk.
- Essentiële digitale hygiëne: Kernpraktijken en protocollen die de integriteit en veiligheid van gegevens en systemen waarborgen.
- De veiligheidsimplicaties van digitale hygiëne: Een gedetailleerd overzicht van hoe effectieve digitale hygiëne verschillende cyberdreigingen kan beperken.
- Basisprincipes van implementatie van digitale hygiëne: Praktische stappen voor het instellen van digitale hygiënemaatregelen binnen persoonlijke en organisatorische contexten.
- Naleving van cyberbeveiliging: een overzicht van de basisbeleidslijnen, voorschriften en nalevingsvereisten van de lidstaten en de EU op het gebied van cyberbeveiliging

### *Onderwerp Leerresultaten*

Aan het einde van dit vak zijn studenten in staat om:

- Definieer digitale hygiëne en begrijp de kritieke componenten ervan.
- Identificeer potentiële cyberdreigingen en begrijp de rol van digitale hygiëne bij de bescherming tegen deze bedreigingen.
- Implementeer digitale basishygiënepraktijken op verschillende platforms en apparaten.
- Communiceer het belang van digitale hygiëne aan collega's en leidinggevenden en pleit voor best practices binnen hun organisaties.
- Inzicht in de basisvereisten voor cyberbeveiliging

### *Lesmethoden*

Een mix van lezingen, interactieve workshops en casestudy's zal worden gebruikt om studenten een robuuste leerervaring te bieden. Elke sessie is bedoeld om theoretische kennis in evenwicht te brengen met praktische toepassing, zodat studenten wat ze leren kunnen vertalen in bruikbare strategieën op hun werkplek.

### *Aanbevolen literatuur*


- Brooks, C.J., Grow, C., Craig, P., Short, D., (2018), Cybersecurity Essentials.
    - This book provides a thorough introduction to the domain of cybersecurity and is especially useful for entry-level cybersecurity certifications.
- Paula, D., Cruz, M., (2023), Cybersecurity Essentials Made Easy: A No-Nonsense Guide to Cyber Security for Beginners.
    - This book is an essential read for understanding cybersecurity challenges and how to mitigate against them. It is especially relevant to new startup SME owners and students looking to seek to understand online safety.
- Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
    - This reference provides an accessible overview of the key concepts and challenges in cybersecurity, making it an excellent resource for students starting their journey in understanding cyber threats and protection mechanisms.
- Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

- Bruce Schneier's book is crucial for understanding the landscape of data privacy and security, offering insights into how personal data is collected and used, and the importance of robust data management practices.

Deze bronnen zijn geselecteerd om theoretische kennis en praktische vaardigheden op het gebied van netwerk- en cyberbeveiliging te bieden, het curriculum te ondersteunen en de onderwijservaring van studenten in beroepsonderwijs en -opleiding op het gebied van digitale hygiëne te verbeteren.

## Netwerk en cyberbeveiliging

Dit onderwerp is erop gericht de studenten de nodige vaardigheden bij te brengen om netwerkbedreigingen te identificeren, te beoordelen en te neutraliseren. Een van de belangrijkste uitdagingen waarmee organisaties in de huidige operationele omgevingen worden geconfronteerd, is het waarborgen van netwerkbeveiliging. Aangezien de meeste netwerken zijn verbonden met internet, worden ze vaak blootgesteld aan kwaadwillende actoren die kunnen proberen netwerkkwetsbaarheden te misbruiken om op ongeoorloofde wijze toegang te krijgen tot het netwerk. Om dit te bereiken wordt de student geïnstrueerd in belangrijke netwerkconcepten, gemeenschappelijke protocollen, poorten, LAN, WAN en cloudsystemen.

### *De belangrijkste onderwerpen die in dit onderwerp aan bod komen*

- Inleiding tot cyberbeveiliging
- Analyse van kwetsbaarheden
- Dreigings- en risicobeoordeling
- Netwerkbeveiligingsprotocollen – Firewalls, antivirus.
- Veelvoorkomende cyberaanvallen
- Gemeenschappelijke cyberbeveiligingstools
- Ethiek in cyberbeveiliging

### *Leerresultaten*

- Identificeer belangrijke netwerkconcepten: Studenten zullen in staat zijn om de fundamentele aspecten van netwerken, waaronder LAN-, WAN- en cloudsystemen, te beschrijven en hun rol in de organisatorische infrastructuur te begrijpen.
- Beoordeel netwerkkwetsbaarheden: Leerlingen zullen de vaardigheden verwerven om kwetsbaarheidsanalyses uit te voeren op verschillende netwerksystemen om mogelijke zwakke punten in de beveiliging te identificeren.
- Implementeer beveiligingsmaatregelen: Studenten zullen bedreven zijn in het opzetten en beheren van netwerkbeveiligingsprotocollen zoals firewalls en antivirussystemen om te beschermen tegen cyberdreigingen.
- Voer dreigings- en risicobeoordelingen uit: Voorzie studenten van de mogelijkheid om risico's in verband met cyberbeveiligingsbedreigingen voor netwerksystemen te beoordelen en te prioriteren.
- Begrijp ethische implicaties: Studenten zullen de ethische overwegingen in cyberbeveiliging onderzoeken en de verantwoordelijkheden begrijpen van het beschermen van gegevens en systemen tegen ongeoorloofde toegang.

### *Lesmethoden*

- Interactieve lezingen: Gericht op het introduceren van fundamentele en geavanceerde netwerkconcepten, beveiligingsprotocollen en ethische kwesties in cyberbeveiliging.
- Hands-On Labs: Praktijksessies in computerlokalen waar studenten echte en gesimuleerde netwerkomgevingen kunnen gebruiken om beveiligingsmaatregelen en -tools toe te passen.
- Analyse van casestudy's: Bespreking en analyse van real-world cyberbeveiligingsincidenten om dreigingsmechanismen en effectieve tegenmaatregelen te begrijpen.
- Groepsprojecten: Teams van studenten beoordelen een hypothetische netwerkopstelling op kwetsbaarheden en stellen een uitgebreide beveiligingsstrategie voor.
- Gastsprekerssessies: Cybersecurity-professionals worden uitgenodigd om inzichten en ervaringen te delen, waarbij de nadruk wordt gelegd op de huidige uitdagingen en opkomende technologieën.

### *Aanbevolen literatuur*

- Stewart, J. M., Chapple, M., & Gibson, D. (2020). *CompTIA Security+ Guide to Network Security Fundamentals* (7th ed.). Cengage Learning.
    - This guide covers a broad range of foundational topics in network security, suitable for students beginning their journey in cybersecurity.
- Marsh, N., (2023), Cybersecurity: A Fat-Free Guide to Network Security Best Practices (Fat-Free Technology Guides). This book provides a comprehensive insight into cyber threats and critical network security issues.
- Whitman, M. E., & Mattord, H. J. (2018). *Principles of Information Security* (6th ed.). Cengage Learning.
    - A comprehensive resource that provides an in-depth look at the principles of information security, including detailed discussions on vulnerability analysis, threat, and risk assessment.
- Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson. Stallings' text provides comprehensive coverage of network security protocols and standards, ideal for students needing a detailed understanding of the technical aspects of securing networks.
- Computer & Internet Security: A Hands-on Approach 3rd ed. Edition by Wenliang Du

Deze academische bronnen zullen het curriculum ondersteunen door zowel theoretische kaders als praktische inzichten te bieden in het beheren en beveiligen van netwerkomgevingen, in lijn met de geschetste leerresultaten en onderwijsstrategieën.

## Gegevens- en bestandsbeheer

Gegevens zijn, zoals eerder vermeld, een van de meest waardevolle activa die organisaties bezitten. Het beheer van dit vermogen heeft dan ook een steeds belangrijkere rol gekregen binnen de organisatie. Dit is vooral belangrijk vanwege de toenemende bezorgdheid over de veiligheid in de cyberomgeving. Goed gegevensbeheer is cruciaal geworden voor effectieve cyberbeveiliging, vooral bij het vastleggen, organiseren en verspreiden van gevoelige informatie. Gegevensbeheer verwijst naar de principes en praktijken die worden toegepast bij het beheer en de bescherming van gegevens. In het kader van cyberbeveiliging houdt gegevensbeheer zich ook bezig met de bescherming van gegevens tegen geautoriseerde toegang, wijziging en overdracht. In de huidige omgeving waar enorme hoeveelheden gegevens worden verzameld, geanalyseerd en verspreid, hebben de aspecten van beveiligingsbeheer aan belang gewonnen. Daarom is er een verhoogde behoefte aan professionals die bedreven zijn in gegevensbeheer.

### *De belangrijkste onderwerpen die in dit onderwerp aan bod komen*

- Gegevensbeheer
- Classificatie van gegevens
- Versleuteling in gegevensbeheer
- Gegevensbewaking en -audit
- Back-up en herstel van gegevens
- Gegevensintegriteit en privacy
- Toegangscontrole en authenticatie

### *Leerresultaten*

- Begrijp Data Governance: Studenten zullen de fundamentele concepten van data governance en de rol ervan in de organisatorische context begrijpen.
- Gegevens classificeren: Leerlingen kunnen gegevens classificeren op basis van gevoeligheid en belang, waarbij passende beveiligingsmaatregelen worden toegepast op verschillende soorten gegevens.
- Implementeer gegevensversleuteling: Studenten zullen coderingstechnieken begrijpen en toepassen om de integriteit en vertrouwelijkheid van gegevens tijdens opslag en overdracht te beschermen.
- Voer gegevensaudits uit: Rust studenten uit met de vaardigheden om regelmatig gegevensmonitoring en audits uit te voeren om ervoor te zorgen dat het beveiligingsbeleid en de beveiligingsvoorschriften worden nageleefd.
- Gegevensherstel beheren: Studenten leren strategieën voor gegevensback-up en -herstel om de beschikbaarheid en continuïteit van gegevens te garanderen in geval van gegevensverlies of systeemstoringen.
- Zorg voor gegevensintegriteit en privacy: Leerlingen zullen methoden begrijpen om de gegevensintegriteit te behouden en privacy-instellingen te beheren om gebruikersgegevens te beschermen tegen ongeoorloofde toegang.
- Toegangscontroles toepassen: Studenten zullen in staat zijn om robuuste toegangscontroles en authenticatiemethoden te implementeren om de toegang tot gegevens te beschermen.

### *Aanbevolen literatuur*


- Ladley J., (2019)., Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program 2nd Edition. This book provides a comprehensive view of data governance and security.
- Talabis, M., & Martin, J. (2015). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis. Syngress.
    - This book provides practical tools and techniques for assessing information security risks, including those associated with data management.
- Bertino, E., & Sandhu, R. (2017). Data Privacy and Security. Springer.
    - A comprehensive overview of data privacy and security techniques, this text is crucial for understanding the complexities of protecting sensitive data in various environments.
- Swanson, M., & Guttman, B. (2016). Generally Accepted Principles and Practices for Securing Information Technology Systems. National Institute of Standards and Technology.
    - This government publication offers guidelines and best practices for securing IT systems, including detailed sections on data management and security controls.

Deze academische bronnen zullen het onderwijskader verbeteren door theoretische kennis en praktische toepassingsvoorbeelden te bieden, waardoor studenten bekwaam kunnen worden in het effectief beheren en beveiligen van organisatiegegevens.

## Softwarebeheer

Softwarebeheer is een cruciaal onderdeel van cyberbeveiliging. Softwarebeheer omvat het systematische proces van planning, het implementeren van een systematisch proces van planning, implementatie, monitoring en onderhoud van software gedurende de levenscyclus. Het omvat taken zoals versiebeheer, patchbeheer, licenties en beveiligingsupdates. Effectief softwarebeheer zorgt voor optimale prestaties, beveiliging en naleving, terwijl risico's en kwetsbaarheden tot een minimum worden beperkt. Moderne organisaties worden geconfronteerd met verschillende uitdagingen op het gebied van softwarebeveiliging, zoals slecht wachtwoordbeleid, onveilige API-niet-gepatchte kwetsbaarheden, phishing en datalekken om er maar een paar te noemen. Het is daarom absoluut noodzakelijk dat ze opgeleid personeel hebben dat is opgeleid om de software van de organisatie effectief te beheren en inbreuken op de softwarebeveiliging te voorkomen. Deze module biedt de student praktische basiskennis over hoe de software van de organisatie effectief kan worden beheerd en het risico op een inbreuk op de beveiliging kan worden geminimaliseerd.

### *De belangrijkste onderwerpen die in dit onderwerp aan bod komen*

- Beveiliging van applicaties
- Testen en controleren van software
- Gebruikerstoegang en -rechten beheren
- Implementeren van reguliere updateprotocollen
- Beveiligingsmaatregelen voor eindpunten

### *Leerresultaten*

- Master Application Security: Studenten begrijpen de basisprincipes van het beveiligen van applicaties van ontwerp tot implementatie, inclusief veelvoorkomende kwetsbaarheden en mitigatiestrategieën.
- Voer softwaretests en audits uit: Leerlingen zullen vaardigheid verwerven in verschillende methoden voor het testen en auditen van software om beveiligingsproblemen te identificeren en op te lossen.
- Gebruikerstoegang beheren: Studenten leren gebruikerstoegang en privileges effectief te beheren om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot kritieke softwarebronnen.
- Implementeer updateprotocollen: Rust studenten uit met de kennis om regelmatig software-updateprotocollen op te stellen en te onderhouden om kwetsbaarheden te beperken.
- Verbeter de beveiliging van eindpunten: Studenten zullen eindpuntbeveiligingsmaatregelen begrijpen om de organisatie-infrastructuur te beschermen tegen bedreigingen zoals malware en ransomware.

### *Aanbevolen literatuur*

- Du, W., (2022), Computer Security: A hands-on approach, 3rd edition. This book investigates software management, vulnerabilities, and mitigation activities.
- Allen, J. H., Barnum, S., Ellison, R., McGraw, G., & Viega, J. (2008). Software Security Engineering: A Guide for Project Managers. Addison-Wesley Professional.
    - This book offers a comprehensive guide to integrating security practices into software development, making it essential for understanding application security and lifecycle management.
- 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.
    - Provides insights into managing user access and privileges by identifying key stakeholders and their needs, crucial for effective software management.
- Lindqvist, U., & Neumann, P. G. (2017). The Future of Cybersecurity: Challenges and Opportunities. IEEE Security & Privacy.
    - This article discusses future challenges and opportunities in cybersecurity, including the importance of continuous software updates and endpoint security measures.

Deze bronnen zullen het curriculum ondersteunen door een solide theoretische basis en praktische inzichten in softwarebeheer te bieden, zodat studenten goed zijn toegerust om softwarebeveiligingsuitdagingen in moderne organisatorische omgevingen aan te pakken.

## Back-up en herstel van gegevens

Deze module is ontworpen om de studenten een uitgebreid begrip te geven van het back-up- en herstelproces en hoe dit kan worden geïmplementeerd. Alle moderne organisaties moeten beschikken over het juiste back-up- en herstelbeleid, protocollen en systemen. De meeste huidige organisaties zijn datagedreven en hechten daarom veel waarde aan het beheer van hun gegevens en informatiebronnen. In principe slaan de meeste organisaties, met name KMO's, hun gegevens op in een gecentraliseerde, lokale of clouddatabase. Cloudgebaseerde systemen zijn geavanceerder en veiliger geworden, met zeer geavanceerde beheercontroles, waardoor ze minder vatbaar zijn voor de traditionele problemen van vernietiging van de fysieke opslagsystemen. Ze zijn echter nog steeds vatbaar voor menselijke fouten, verkeerde configuraties en datalekken, daarom is het belangrijk dat het IT-personeel dat toezicht houdt op dergelijke systemen bekend is met de betrokken technologieën, protocollen en processen. De module is ontworpen om deze kennis aan de student te bieden.

### *De belangrijkste onderwerpen die in dit onderwerp aan bod komen*

- Bestandsbeheer
- Back-up- en herstelprotocollen
- Soorten back-ups
- Back-upservices en -apparaten

### *Leerresultaten*

- Begrijp bestandsbeheer: Studenten leren de principes van effectief bestandsbeheer, cruciaal voor het organiseren van gegevens voor back-updoeleinden.
- Beheers back-up- en herstelprotocollen: Leerlingen zullen verschillende back-up- en herstelprotocollen begrijpen en hoe ze deze effectief kunnen toepassen in verschillende scenario's.
- Identificeer back-uptypen: Studenten kunnen onderscheid maken tussen verschillende soorten back-ups (volledig, incrementeel, differentieel) en beslissen welke het meest geschikt is voor specifieke situaties.
- Gebruik back-upservices en apparaten: Rust studenten uit met kennis over verschillende back-upservices en -apparaten, waaronder cloudgebaseerde en lokale back-upoplossingen, en hoe ze deze veilig kunnen implementeren.
- Beperk de risico's van gegevensverlies: Studenten zullen begrijpen hoe ze een strategie voor gegevensherstel moeten plannen en uitvoeren om downtime en gegevensverlies te minimaliseren in het geval van datalekken of rampen.

### *Aanbevolen literatuur*

- Preston, W., (2021), Modern Data Protection: Ensuring Recoverability of All Modern Workloads. This book is into modern data protection and how this is integrated into the overall hardware and software security.
- Data Backup And Recovery A Complete Guide - 2023 Edition
- Toigo, J. W. (2009). Disaster Recovery Planning: Preparing for the Unthinkable (3rd ed.). Prentice Hall.
    - Offers comprehensive insights into disaster recovery planning, including detailed discussions on backup strategies as a critical component of disaster recovery.
- Duffy, D. (2014). Cloud Computing: Strategies for Cloud Computing Adoption. Faithful Pen Publishing.
    - Discusses the adoption of cloud computing, focusing on cloud-based backup services and the security considerations associated with them.

Deze academische bronnen zullen het curriculum versterken door studenten zowel een fundamenteel begrip als praktische vaardigheden te bieden bij het beheren en implementeren van strategieën voor gegevensback-up en -herstel, essentieel voor het minimaliseren van potentieel gegevensverlies in moderne organisatorische omgevingen.

## Cryptografie, verificatie en wachtwoordbeheer

Gegevens en informatie zijn een van de meest cruciale activa van de organisatie geworden en zijn in veel gevallen de belangrijkste bepalende factor achter de waardering van bedrijven. De cruciale aard van dergelijke activa maakt het absoluut noodzakelijk dat ze met de grootste zorg worden behandeld. Een van de belangrijkste hulpmiddelen voor het beveiligen van gegevens en informatiemiddelen is cryptografie. Cryptografie is van cruciaal belang voor cyberbeveiliging, aangezien het essentieel is voor de bescherming van gevoelige gegevens en informatie en veilige communicatie. Het maakt robuuste authenticatieprotocollen en wachtwoordbeheer mogelijk. Cryptografie maakt een correcte implementatie van authenticatiesystemen mogelijk, die de vertrouwelijkheid, integriteit en beschikbaarheid van organisatorische gegevens en informatie voor het juiste personeelslid garanderen.

### *De belangrijkste onderwerpen die in dit onderwerp aan bod komen*

- Basisprincipes van cryptografie
- End-to-end versleuteling
- Encryptie standaarden
- Meervoudige verificatie
- Sleutelbeheer
- Het selecteren van de beste standaarden voor uw bedrijf
- Best practices bij het implementeren van versleutelingstechnologieën

### *Leerresultaten*

- Begrijp de basisprincipes van cryptografie: Studenten leren de fundamentele principes van cryptografie, inclusief de geschiedenis, het doel en de belangrijkste mechanismen.
- Implementeer end-to-end-codering: Leerlingen zullen vaardigheden opdoen in het opzetten en beheren van end-to-end-codering om communicatie te beveiligen.
- Versleutelingsstandaarden toepassen: Studenten zullen bekend zijn met verschillende versleutelingsstandaarden en leren hoe ze deze kunnen toepassen op basis van de behoeften van de organisatie.
- Gebruik multifactorauthenticatie: Geef studenten de mogelijkheid om multifactorauthenticatiesystemen te implementeren en te beheren om de beveiliging te verbeteren.
- Cryptografische sleutels beheren: Studenten begrijpen sleutelbeheerprocessen en best practices om de veiligheid en integriteit van cryptografische sleutels te waarborgen.
- Selecteer en implementeer versleutelingstechnologieën: Studenten leren hoe ze geschikte versleutelingstechnologieën voor hun bedrijf kunnen selecteren en best practices voor implementatie om gegevens effectief te beschermen.

### *Aanbevolen literatuur*

- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
    - This textbook provides a comprehensive introduction to the field of cryptography and network security, including detailed coverage of encryption technologies and authentication protocols.
- Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography (2nd ed.). CRC Press.
    - Offers an in-depth exploration of modern cryptographic techniques, focusing on rigorous security proofs and practical applications.
- Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley.
    - This book discusses the design and implementation of cryptographic systems, emphasizing the importance of proper implementation to prevent vulnerabilities.

Deze bronnen zijn geselecteerd om een theoretische achtergrond en praktische vaardigheden op het gebied van cryptografie, authenticatie en wachtwoordbeheer te bieden, ter ondersteuning van het doel van het curriculum om studenten uit te rusten met de nodige kennis om organisatiegegevens effectief te beveiligen.

## Beheer en beveiliging van mobiele apparaten

Organisaties zetten mobiele apparaten steeds vaker in als een belangrijk werkplatform en communicatiemiddel. Dit is vooral van toepassing op startups en KMO's waar wendbaar en te allen tijde

bereikbaar zijn een belangrijk criterium voor succes is geworden. Hoewel de mobiele technologie zo ver is gevorderd dat de meeste geavanceerde smartphones net zo krachtig en veelzijdig zijn als laptops en desktops, maakt het draadloze karakter van dergelijke apparaten ze vatbaar voor kwaadwillende actoren die ongeoorloofde toegang willen krijgen. Deze module is ontworpen om inzicht te geven in de kwetsbaarheden van deze apparaten en de bijbehorende platforms en hoe dergelijke risico's kunnen worden geminimaliseerd.

### *De belangrijkste onderwerpen die in dit onderwerp aan bod komen*

- Inzicht in de bedreigingen voor mobiele apparaten
- Beoordeling van de risico's voor mobiele applicaties
- Firewalls voor communicatie tussen processen
- Mobiele beveiligingstechnologieën
- Toegangscontroles voor mobiele gegevens en risicobeheer

### *Leerresultaten*

- Identificeer bedreigingen voor mobiele apparaten: Studenten leren verschillende bedreigingen te herkennen die gericht zijn op mobiele platforms en hun potentiële impact te begrijpen.
- Beoordeel risico's voor mobiele applicaties: Leerlingen zullen vaardigheden verwerven in het beoordelen van risico's in verband met mobiele applicaties, met de nadruk op beveiligingskwetsbaarheden.
- Implementeer mobiele beveiligingstechnologieën: Studenten kunnen beveiligingstechnologieën implementeren en beheren die speciaal zijn ontworpen voor mobiele apparaten.
- Firewalls voor communicatie tussen processen beheren: Rust studenten uit met de kennis om firewalls te configureren en te beheren die de communicatie tussen processen op mobiele apparaten regelen.
- Toegangscontroles voor mobiele gegevens toepassen: Studenten leren hoe ze gegevenstoegangscontroles kunnen instellen en afdwingen om gevoelige informatie op mobiele apparaten te beveiligen.

### *Aanbevolen literatuur*


- Doherty, J., (2021), Wireless and Mobile Device Security 2nd Edition. This book looks at the implications of the rapid integration of mobile devices into the organization's communication environment, the attendant security concerns, and how these can be mitigated.
- 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.
    - This book offers a deep dive into the security architecture of iOS, discussing common vulnerabilities and providing strategies to secure iOS applications.
- Fried, S. (2011). Mobile Device Security: A Comprehensive Guide to Securing Your Information in a Moving World. CyberAge Books.
    - This guide is essential for students and practitioners needing to understand the specific security challenges presented by mobile devices, which are increasingly used in both personal and professional contexts.

Deze bronnen zullen het curriculum ondersteunen door zowel basiskennis als specifieke vaardigheden te bieden die nodig zijn om mobiele apparaten effectief te beheren en te beveiligen, zodat studenten goed voorbereid zijn om mobiele beveiligingsuitdagingen in moderne organisatorische contexten aan te pakken.

# Unit 3 – Digitale hygiënebeoordeling en feedbackmechanismen voor beroepsonderwijs en -opleiding

## Introductie

Beoordeling en feedback zijn cruciale onderdelen van het onderwijsproces en bieden zowel docenten als studenten essentiële inzichten in de effectiviteit van lesgeven en leren. In de context van een curriculum voor digitale hygiëne zijn robuuste beoordelings- en feedbackmechanismen bijzonder cruciaal. Ze zorgen ervoor dat de aangeleerde kennis en vaardigheden niet alleen worden begrepen en onthouden, maar ook toepasbaar zijn in real-world scenario's waar digitale veiligheidsrisico's heersen.

Deze unit is ontworpen om de strategieën en methodologieën te schetsen voor het evalueren van de prestaties van studenten en het geven van constructieve feedback tijdens het programma voor digitale hygiëne. Dit omvat een combinatie van theoretische kennisbeoordelingen en praktische, hands-on evaluaties.

## Assessment Strategieën

### *Formatieve beoordelingen*

- **Quizzen en korte tests:** Tijdens elke module worden regelmatig quizzen en korte tests uitgevoerd om het begrip van de belangrijkste concepten te beoordelen en om onmiddellijke feedback te geven. Dit helpt bij het versterken van het leren en het identificeren van gebieden waar studenten mogelijk extra ondersteuning nodig hebben.
- **Praktische opdrachten:** Studenten krijgen opdrachten waarbij ze theoretische kennis moeten toepassen op praktische scenario's, zoals het configureren van een firewall, het ontwerpen van een gegevensherstelplan of het implementeren van coderingsprotocollen.
- **Peer Assessments:** Dit houdt in dat studenten elkaars opdrachten of projecten beoordelen. Peer assessments kunnen helpen bij het ontwikkelen van kritisch denken en analytische vaardigheden, aangezien studenten leren cyberbeveiligingsoplossingen te bekritiseren op basis van best practices.

### *Summatieve beoordelingen*

- **Eindexamens:** Uitgebreide examens aan het einde van elke module zullen studenten testen op een breder scala aan onderwerpen die tijdens de cursus worden behandeld. Deze examens bevatten zowel meerkeuzevragen als essayvragen om het theoretische en praktische begrip van studenten te beoordelen.
- **Sluitstukprojecten:** Aan het einde van het programma zullen studenten een sluitstukproject uitvoeren waarbij uitgebreide digitale hygiënestrategieën voor hypothetische organisaties worden

gecreëerd of beheerd. Dit project zal worden beoordeeld op verschillende criteria, waaronder innovatie, toepasbaarheid en naleving van cyberbeveiligingsprincipes.

### *Permanente evaluatie*

- **Portfoliobeoordelingen:** Studenten houden gedurende het hele programma een portfolio bij van hun werk en prestaties. Deze portfolio's worden periodiek beoordeeld door instructeurs om de voortgang te beoordelen en gepersonaliseerde feedback te geven.
- **Zelfbeoordelingen:** Door studenten aan te moedigen om aan zelfbeoordeling te doen, kan een grotere verantwoordelijkheid voor hun leerproces worden bevorderd. Er zullen zelfbeoordelingsinstrumenten en checklists worden verstrekt om studenten te helpen hun begrip en vaardigheden te evalueren.

## Feedback Mechanismen

- **Feedback van de docent** : Feedback wordt systematisch gegeven voor alle beoordelingen, waarbij de nadruk ligt op de sterke en zwakke punten van het werk van studenten. Deze feedback zal tijdig, specifiek en constructief zijn, gericht op het aanmoedigen van studenten om na te denken over hun leerproces en verbeterpunten te identificeren.
- **Peer Feedback:** In groepsprojecten en peer assessments worden studenten aangemoedigd om elkaar feedback te geven. Dit zal worden gestructureerd om ervoor te zorgen dat het constructief is en gericht op specifieke criteria.
- **Geautomatiseerde feedback:** Voor bepaalde soorten beoordelingen, met name quizzen en bepaalde praktische oefeningen, zullen geautomatiseerde feedbacksystemen worden gebruikt. Deze systemen kunnen onmiddellijke resultaten en inzichten opleveren, waardoor snel herstel mogelijk is.
- **Feedbackloops:** Het creëren van feedbackloops binnen het curriculum waar studenten kunnen reflecteren op de feedback, hun werk kunnen herzien en opnieuw kunnen indienen voor verdere beoordeling, bevordert een groeimindset en continue verbetering.

## Feedback implementeren in curriculumontwikkeling

De feedback die deze verschillende mechanismen krijgen, is niet alleen in het voordeel van de studenten. Het speelt ook een cruciale rol bij de ontwikkeling van het curriculum:

- **Curriculumaanpassingen:** Regelmatige beoordelingen van prestatiegegevens en feedback van studenten zullen helpen bij het identificeren van gebieden van het curriculum die mogelijk moeten worden aangepast of verbeterd.

- **Ontwikkeling van instructeurs:** Feedback van studenten kan ook leiden tot de professionele ontwikkelingsbehoeften van instructeurs, waarbij wordt aangegeven op welke gebieden ze mogelijk meer ondersteuning of training nodig hebben.

## Conclusie

De beoordelings- en feedbackmechanismen die zijn ontworpen voor het curriculum voor digitale hygiëne in instellingen voor beroepsonderwijs en -opleiding zijn een integraal onderdeel om ervoor te zorgen dat de onderwijsdoelstellingen worden bereikt. Door gebruik te maken van een verscheidenheid aan beoordelingsstrategieën en feedbacksystemen via meerdere kanalen, evalueert het programma niet alleen het leren van studenten effectief, maar verbetert het ook voortdurend de onderwijsmethoden en het curriculumontwerp. Deze dynamische aanpak zorgt ervoor dat het curriculum relevant en effectief blijft om studenten voor te bereiden op het aanpakken van echte digitale hygiëne-uitdagingen.

# Deel 4 – Goede praktijken van beroepsonderwijs en -opleiding

## Introductie

In het dynamische veld van Digitale Hygiëne zorgt theoretische kennis in combinatie met praktische toepassingen voor de meest effectieve leeromgeving. Deze eenheid verdiept zich in goede praktijken die zijn toegepast door instellingen voor beroepsonderwijs en -opleiding (VET) die met succes digitale hygiëneprincipes in hun curricula hebben geïntegreerd. Deze casestudy's dienen als benchmarks voor het ontwikkelen en verfijnen van digitale hygiëneprogramma's en bieden inzicht in succesvolle strategieën en methodologieën die kunnen worden gerepliceerd of aangepast door andere instellingen.

## Casestudy 1: CyberVET Academie

**Overzicht:**

CyberVET Academy staat bekend om zijn robuuste curriculum voor digitale hygiëne dat rigoureuze academici combineert met real-world toepassing. Deze instelling is een model geworden voor de naadloze integratie van opkomende technologieën en best practices op het gebied van cyberbeveiliging in beroepsopleidingen.

**Belangrijkste strategieën:**

- Partnerschappen met de industrie: CyberVET heeft partnerschappen gevormd met toonaangevende technologiebedrijven om ervoor te zorgen dat hun curriculum is afgestemd op de huidige industrienormen en -praktijken. Deze partnerschappen vergemakkelijken ook gastcolleges, stages en toegang tot geavanceerde technologie.
- Gesimuleerde leeromgevingen: De academie heeft geïnvesteerd in het creëren van state-of-the-art gesimuleerde cyberbeveiligingslabs waar studenten veilig realtime cyberdreigingen kunnen verkennen en beperken. Deze hands-on ervaring is van onschatbare waarde.

**Resultaten:**

- Een duidelijke toename van de inzetbaarheid van studenten, waarbij 90% van de afgestudeerden binnen zes maanden na afstuderen een baan in cyberbeveiliging krijgt.
- Verbeterde betrokkenheid en tevredenheid van studenten, toegeschreven aan de hands-on leeraanpak en directe betrokkenheid van de industrie.

## Casestudy 2: TechBridge VET

**Overzicht:**

TechBridge VET onderscheidt zich door zijn focus op het beheer en de beveiliging van mobiele apparaten, gebieden die steeds meer zorgen baren op het gebied van digitale hygiëne.

**Belangrijkste strategieën:**

- Modulair curriculumontwerp: Het curriculum bij TechBridge is zeer modulair, waardoor studenten hun leertrajecten kunnen afstemmen op hun carrièredoelen en technologische vooruitgang.
- Gemeenschapsprojecten: Studenten nemen deel aan gemeenschapsprogramma's waar ze hun kennis toepassen om lokale kleine bedrijven te helpen hun digitale beveiligingsmaatregelen te verbeteren.

**Resultaten:**

- Gemeenschapsprojecten hebben niet alleen de praktische vaardigheden van de studenten vergroot, maar hebben ook het bewustzijn van cyberbeveiliging bij lokale eigenaren van kleine bedrijven vergroot.
- De modulaire aanpak heeft geleid tot een hoge flexibiliteit in het onderwijs, waardoor snelle veranderingen in technologie en de behoeften van studenten kunnen worden opgevangen.

## Casestudy 3: SecurePath Institute

**Overzicht:**

SecurePath Institute heeft digitale hygiëne geïntegreerd in zijn beroepsopleidingen en laat zien hoe cyberbeveiliging van fundamenteel belang is voor verschillende technische disciplines.

**Belangrijkste strategieën:**

- Interdisciplinaire aanpak: Door lessen in digitale hygiëne te integreren in programma's zoals gezondheidszorg, autotechnologie en bedrijfsbeheer, zorgt SecurePath ervoor dat alle studenten het belang van cyberbeveiliging in hun respectievelijke vakgebieden erkennen.
- Continue evaluatie van het curriculum: Het instituut gebruikt een AI-gestuurd analysesysteem om zijn curriculum continu te beoordelen en bij te werken op basis van de nieuwste informatie over cyberdreigingen en trends in de sector.

**Resultaten:**

- Studenten van niet-technische programma's studeren af met een sterk begrip van digitale hygiëne, waardoor ze veelzijdiger en aantrekkelijker zijn voor werkgevers.
- Door de voortdurende evaluatie van het curriculum blijft SecurePath voorop lopen op het gebied van onderwijs in digitale hygiëne en past het zich snel aan opkomende bedreigingen aan.

## Implicaties voor best practices

De successen van deze instellingen illustreren verschillende beste praktijken die door andere aanbieders van beroepsonderwijs en -opleiding kunnen worden overgenomen of aangepast:

- Samenwerking met de industrie: Sterke banden met de industrie houden niet alleen het curriculum relevant, maar verbeteren ook de kansen op een baan voor studenten na hun afstuderen.
- Praktische toepassing: Hands-on leren door middel van labs, simulaties of gemeenschapsprojecten is cruciaal voor het begrijpen en effectief toepassen van digitale hygiëneprincipes.
- Flexibiliteit en interdisciplinariteit: Een flexibele en interdisciplinaire aanpak zorgt ervoor dat digitale hygiëne-educatie zich snel kan aanpassen aan veranderingen en kan inspelen op een breed scala aan beroepsgebieden.
- Feedback en continue verbetering: Voortdurende beoordeling en herziening van het curriculum op basis van feedback van verschillende belanghebbenden, waaronder studenten, docenten en industriële partners, zorgen voor de effectiviteit en relevantie van het programma.

## Casestudy 4: DigitalDefenders College

**Overzicht:**

DigitalDefenders College staat bekend om zijn gespecialiseerde benadering van het onderwijzen van cyberbeveiliging, met name de nadruk op ethisch hacken en digitale forensische technieken. Deze instelling voor beroepsonderwijs en -opleiding zet zich in om bekwame professionals af te leveren die klaar staan om de complexiteit van cyberdreigingen in het moderne digitale landschap aan te pakken.

**Belangrijkste strategieën:**

- Modules voor ethisch hacken: Door uitgebreide modules over ethisch hacken op te nemen, biedt het college studenten de vaardigheden om kwetsbaarheden in het systeem te identificeren en te exploiteren, allemaal in een gecontroleerd, ethisch en juridisch kader.

- Real-World Cyber Forensics: Studenten nemen deel aan praktische cyberforensische oefeningen die real-world scenario's voor datalekken nabootsen, waardoor ze begrijpen hoe ze inbreuken effectief kunnen opsporen, analyseren en beperken.

**Resultaten:**

- Afgestudeerden staan bekend om hun proactieve benadering van cyberbeveiliging, met veel veilige posities in sectoren met een hoge inzet, zoals financiën en overheid.
- De praktische ervaring in ethisch hacken en cyberforensisch onderzoek heeft geleid tot een hoge betrokkenheid onder studenten, waardoor een diepgaand begrip van de praktische implicaties van cyberdreigingen is bevorderd.

## Casestudy 5: InnovateTech Institute

**Overzicht:**

InnovateTech Institute onderscheidt zich door geavanceerde technologische trends, zoals kunstmatige intelligentie (AI) en machine learning (ML), te integreren in het curriculum voor digitale hygiëne. Deze aanpak bereidt studenten voor op het steeds meer AI-gestuurde landschap van cyberbeveiliging.

**Belangrijkste strategieën:**

- AI-gestuurde beveiligingsoplossingen: Studenten leren AI en ML te gebruiken bij het ontwikkelen van geavanceerde cyberbeveiligingsmaatregelen, waardoor ze cybercriminelen voor blijven die ook geavanceerde technologieën gebruiken.
- Samenwerkingsprojecten met technologiebedrijven: Studenten werken aan projecten in samenwerking met technologiebedrijven en creëren op AI gebaseerde beveiligingsoplossingen, die hen realtime inzicht geven in de uitdagingen en eisen van de industrie.

**Resultaten:**

- Studenten hebben verschillende op AI gebaseerde beveiligingstools ontwikkeld die zijn overgenomen door partnerbedrijven en die hun directe impact op de huidige cyberbeveiligingsoplossingen laten zien.
- De integratie van AI en ML in het onderwijs in digitale hygiëne heeft niet alleen het curriculum robuuster gemaakt, maar heeft ook de inzetbaarheid van studenten in door technologie gedreven industrieën aanzienlijk vergroot.

## Samenvatting van goede praktijken

Deze aanvullende casestudy's van DigitalDefenders College en InnovateTech Institute versterken de kritieke aspecten van een succesvol curriculum voor digitale hygiëne in instellingen voor beroepsonderwijs en -opleiding:

- Specialisatie en geavanceerde training: Programma's die gespecialiseerde training bieden op veelgevraagde gebieden van cyberbeveiliging, zoals ethisch hacken en AI, kunnen de relevantie en aantrekkelijkheid van het curriculum aanzienlijk vergroten.
- Toepassing in de echte wereld: Praktische, real-world toepassing van geleerde vaardigheden, hetzij door middel van cyberforensisch onderzoek of samenwerkingsprojecten in de industrie, zorgt ervoor dat studenten niet alleen bekend zijn met theoretische concepten, maar ook bekwaam zijn in het toepassen ervan in echte situaties.
- Innovatief en toekomstbestendig curriculum: Door het curriculum af te stemmen op de nieuwste technologische ontwikkelingen, worden studenten voorbereid op nieuwe bedreigingen en kansen, waardoor ze waardevolle activa zijn in elke cyberbeveiligingsrol die ze na hun afstuderen op zich nemen.
- Deze voorbeelden laten de diverse strategieën zien die kunnen worden geïmplementeerd om de voorlichting over digitale hygiëne effectief te verbeteren, en die elk op unieke wijze bijdragen aan het overkoepelende doel om bekwame professionals te bevorderen die zijn uitgerust om digitale activa te beschermen in een steeds complexere cyberomgeving.

# Conclusie

De vijf casestudy's die zijn onderzocht door CyberVET Academy, TechBridge VET, SecurePath Institute, DigitalDefenders College en InnovateTech Institute bieden een rijk scala aan succesvolle strategieën en benaderingen voor het integreren van digitale hygiëne in de curricula van beroepsonderwijs en -opleiding. Elke instelling, met zijn unieke focus en methodologie, onderstreept de cruciale rol van praktisch, op de industrie afgestemd en innovatief onderwijs bij het voorbereiden van studenten op de complexiteit van cyberbeveiliging in de moderne digitale wereld.

## Belangrijkste punten en best practices

- Samenwerking en afstemming van de sector: Een gemeenschappelijk thema in alle casestudy's is het belang van het onderhouden van sterke banden met marktleiders en bedrijven. Deze partnerschappen houden niet alleen het curriculum up-to-date met de nieuwste technologieën en

praktijken, maar verbeteren ook de inzetbaarheid van studenten door middel van stages, real-world projecten en blootstelling aan industriestandaarden.

- Hands-on en praktische ervaring: Elke instelling benadrukt de noodzaak van praktische toepassing van geleerde concepten. Of het nu gaat om cyberlabs, gesimuleerde omgevingen of forensisch onderzoek in de echte wereld, praktijkervaring is cruciaal. Het versterkt niet alleen de theoretische kennis, maar bereidt studenten ook voor op echte uitdagingen waarmee ze in hun carrière te maken zullen krijgen.
- Gespecialiseerde modules en geavanceerde training: Instellingen zoals DigitalDefenders College benadrukken de voordelen van het aanbieden van gespecialiseerde training op gebieden als ethisch hacken en cyberforensisch onderzoek. Evenzo illustreert de focus van het InnovateTech Institute op AI-gestuurde beveiligingsoplossingen het voordeel van het integreren van geavanceerde technologieën in het curriculum, waardoor studenten worden voorbereid op toekomstige trends en innovaties op het gebied van cyberbeveiliging.
- Interdisciplinaire en flexibele leerbenaderingen: De integratie van digitale hygiëne door het SecurePath Institute in verschillende beroepsopleidingen illustreert de waarde van een interdisciplinaire aanpak, die de toepasbaarheid en relevantie van cyberbeveiligingsonderwijs verbreedt. Bovendien zorgt het modulaire curriculumontwerp van TechBridge VET voor meer flexibiliteit, waardoor snelle technologische veranderingen en uiteenlopende interesses van studenten kunnen worden opgevangen.
- Continue verbetering en aanpassing: Het gebruik van AI-gestuurde analyses door het SecurePath Institute voor continue curriculumevaluatie en de dynamische updateprotocollen van het InnovateTech Institute onderstrepen het belang van voortdurende beoordeling en aanpassing. Door het curriculum responsief te houden op het evoluerende cyberdreigingslandschap, zorgt u ervoor dat educatieve programma's relevant en effectief blijven.

Uit de synthese van inzichten van deze diverse instellingen voor beroepsonderwijs en -opleiding blijkt dat de effectiviteit van een digitaal hygiënecurriculum afhangt van het vermogen om theoretische kennis te combineren met praktische vaardigheden, zich aan te passen aan technologische vooruitgang en sterke connecties met de industrie te bevorderen. Deze elementen zijn cruciaal om studenten niet alleen voor te bereiden om te voldoen aan de huidige eisen van het cyberbeveiligingsveld, maar ook om te innoveren en het voortouw te nemen in het licht van toekomstige uitdagingen. Deze holistische benadering verbetert niet alleen de leerervaring, maar verhoogt ook aanzienlijk de inzetbaarheid en bereidheid van afgestudeerden om digitale activa te beschermen in een wereldwijd verbonden wereld. Terwijl instellingen voor beroepsonderwijs en -opleiding hun programma's blijven ontwikkelen en verfijnen, bieden de lessen uit deze casestudy's waardevolle blauwdrukken voor het ontwikkelen van robuuste, uitgebreide digitale

hygiënecurricula die zijn toegerust om de uitdagingen van het cyberbeveiligingslandschap van morgen aan te gaan.

# Bronnen:


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.

Online bronnen en websites:

- Cybersecurity & Infrastructure Security Agency (CISA)
    - Website: https://www.cisa.gov/
    - CISA provides a wealth of resources on cybersecurity best practices and threats, offering guidelines, tools, and alerts that are crucial for cybersecurity education and awareness.
- National Institute of Standards and Technology (NIST) Cybersecurity Framework
    - Website: https://www.nist.gov/cyberframework
    - NIST's framework is a widely used standard for managing cybersecurity risks, and it provides structured guidance that can be integrated into educational curriculums.
- Open Web Application Security Project (OWASP)
    - Website: https://owasp.org/
    - OWASP is an online community delivering free and open resources on web application security, including tools, standards, and best practices.
- SANS Institute
    - Website: https://www.sans.org/
    - A recognized leader in cybersecurity training, the SANS Institute offers a variety of research papers, training materials, and security guidelines.
- Krebs on Security
    - Website: https://krebsonsecurity.com/
    - Run by journalist Brian Krebs, this blog offers in-depth security news and investigation, focusing on the latest threats and breaches.
- Infosec Institute
    - Website: https://resources.infosecinstitute.com/

- Infosec Institute provides resources and training focused on information security, including insightful articles and industry updates.

- The Hacker News
  - Website: https://thehackernews.com/
  - An online cybersecurity news magazine, The Hacker News offers up-to-date information on current cybersecurity threats and innovations.

- Bruce Schneier's Blog
  - Website: https://www.schneier.com/
  - Bruce Schneier is a renowned security technologist whose blog provides insights into security and privacy issues in the digital world.

# Module 3: Implementeren en in stand houden

## Unit 1 - Bouwen aan een digitale hygiënecultuur in startups en instellingen voor beroepsonderwijs en -opleiding

### Wat is een digitale hygiënecultuur?

Zoals we in de vorige modules hebben ontdekt, is digitale hygiëne een term die voor het eerst ontstond in de vroege jaren om de principes uit te leggen voor veilige, georganiseerde en ethische digitale praktijken, die tot doel hebben de gegevens, privacy en integriteit van een systeem effectief te beschermen [1]. In deze module onderzoeken we de systemische toepassing van deze principes op grotere schaal, op maat gemaakt voor aanbieders van beroepsonderwijs en -opleiding in heel Europa, en doen we suggesties voor het opbouwen van een betere digitale hygiënecultuur die innovatie en enthousiasme in organisaties zal inspireren.

Dus, wat is digitale hygiënecultuur precies? Net als veel andere netwerkculturen die streven naar een succesvolle organisatie, of het nu gaat om structuur of verkenning [2], draait de digitale hygiënecultuur om een gedeelde mentaliteit. In deze mindset gelooft elk lid in de missie van de organisatie en formuleert strategieën die gebaseerd zijn op collectieve verantwoordelijkheid en het integreren van veilige digitale praktijken.

Laten we eens kijken hoe de digitale hygiënecultuur kan worden uitgebreid van het leiderschapsniveau naar werkgroepen, en naar elk individu.

### Ontwikkeling van een digitale hygiënecultuur op leiderschapsniveau

In een post-Covid-tijdperk waarin werken op afstand het nieuwe normaal is en de kwetsbaarheden in de digitale wereld zowel emotioneel als technisch kunnen zijn [3] (bijv. social engineering-aanvallen die de vorm kunnen aannemen van een emotioneel verhaal dat een phishing-poging is), vraagt de situatie niet alleen om een manager, maar ook om een leider die door de complexiteit van de digitale wereld op een efficiënte manier, terwijl digitale hygiënepraktijken worden gedemonstreerd als een integraal onderdeel van de waarden van de organisatie. Hieronder staan enkele van de belangrijke punten waarop een leider een veilige en ondersteunende digitale hygiënecultuur kan bevorderen:

- **Stimuleer organisatorische flexibiliteit** [4]:

Leiders moeten ervoor zorgen dat hun organisaties zich kunnen aanpassen aan digitale vooruitgang en uitdagingen die zich kunnen voordoen als gevolg van digitale praktijken. Om hun team door deze veranderingen te loodsen, moeten alle leiders eerst hun positie, beslissingen en emoties begrijpen [5] in verschillende omstandigheden voordat ze anderen motiveren door middel van een gemeenschappelijk doel.

- **Managementuitdagingen aanpakken [5]:**

Leiders in elke organisatie moeten potentiële managementuitdagingen erkennen die kunnen voortvloeien uit digitalisering, zoals cyberbeveiligingsbedreigingen, privacyproblemen, lacunes in vaardigheden of problemen die worden veroorzaakt door werken op afstand. Ze moeten klaar zijn om de vaardigheden van hun teams bij het handhaven van digitale hygiëne te beoordelen. Dit vereist een bepaald niveau van technische expertise; Daarom wordt geadviseerd dat de leiders technische problemen effectief kunnen begrijpen en verwoorden met hun teams.

- **Relaties en samenwerkingsprocessen creëren 6:**

Leiders in elke organisatie moeten relaties aangaan met een breed scala aan belanghebbenden op zowel intern als extern niveau. Dit vereist dat ze in hoge mate gecoördineerd en verantwoordelijk zijn, en ook de leiding nemen om een sterk gevoel van samenwerking tussen werknemers en andere belanghebbenden aan te moedigen.

- **Investeren in onderwijs en opleiding [5]:**

Leiders in elke organisatie moeten investeren in voortdurende opleiding en training van zichzelf en hun werknemers om op de hoogte te blijven van de nieuwste digitale hygiënepraktijken en -technologieën. Sommige cyberbeveiligingsbedrijven [7] en sommige overheidsinstanties in Europa, zoals het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), bieden een verscheidenheid aan online en persoonlijke cursussen aan over de thema's cyberbeveiligingsbewustzijn en crisisbeheer [8].

## Ontwikkeling van een digitale hygiënecultuur op groepsniveau

Nadat er een routekaart is opgesteld voor een digitale hygiënestrategie, moeten de cyberbeveiligingsproblemen van elke organisatie ook op groepsniveau worden besproken. Werkgroepen, waaronder afdelingen, programma's, studenten of projectmanagers, kunnen een aanzienlijke bijdrage leveren aan het bevorderen van een digitale hygiënecultuur binnen hun instellingen, met de steun en samenwerking van relevante Computer Emergency Response Teams (CERT's) [Voeg deze term toe aan de woordenlijst].

Hieronder staan enkele belangrijke punten waar elke werkgroep gebruik van kan maken om een digitale hygiënecultuur te creëren:

- **Effectieve communicatie in groepen tot stand brengen:**

Een effectieve communicatiemethode voor groepen is om vergaderingen of cursussen op gang te brengen met discussies over cyberbeveiliging. Elke groep kan in het begin vijf minuten vrijmaken voor vragen van de leden. Tijdens deze bijeenkomsten kunnen regels en richtlijnen over hoe apparaten binnen de afdelingen of klaslokalen moeten worden gebruikt, verder worden vastgesteld om de digitale hygiënecultuur te versterken [9].

Een andere handige methode voor groepen kan zijn om elektronische handtekeningen of QR-codes te vereisen voor gedeelde documenten die kunnen bepalen of een e-mail of een digitale transactie wordt gedaan door een lid van groep [10]. Een andere factor die aandacht vereist, is het kiezen van veiligere opslagopties zoals de cloud, in plaats van USB-flashdrives [10].

- **Het vaststellen van effectieve documentatiemethoden voor digitale aanvallen:**

Het documenteren van digitale aanvallen is een cruciaal aspect van het handhaven van cyberbeveiliging. Alle organisaties moeten de richtlijnen voor documentatie duidelijk uitleggen. Enkele van de procedures voor het ontwikkelen van documentatie voor digitale aanvallen kunnen als volgt zijn [11]:

**STAP 1:** Houd een georganiseerd logboek bij: Moedig in het geval van een incident elk lid van uw team aan om gegevenspunten op te nemen , zoals datum, tijd, e-mailadres, relevante links, accountnamen en metadata.

**STAP 2:** Implementeer gestructureerde sjablonen: Gebruik kant-en-klare sjablonen om de incidenten met datalekken te documenteren. U kunt bijvoorbeeld het incidentlogboeksjabloon gebruiken van Access Now, een internationale ngo die tot doel heeft de digitale burgerrechten van mensen over de hele wereld te beschermen.

**STAP 3:** Gebruik diverse documentatieformaten: Moedig uw teamleden aan om een breed scala aan formaten te gebruiken voor het documenteren van hun problemen. Ze kunnen de Wayback Machine van Internet Archive gebruiken om een webpagina op te slaan of video-opnametools gebruiken om video op te nemen als bewijs van hun problemen.

**STAP 4:** Veilig informatie opslaan: Maak back-ups op uw eigen apparaten, in vertrouwde opslagopties, en bescherm uw bestanden indien mogelijk met versleuteling.

- **Opzetten van regelmatige digitale hygiënebeoordelingen:**

Het uitvoeren van regelmatige audits en risicobeoordelingen kan helpen kwetsbaarheden te identificeren en ervoor te zorgen dat digitale hygiënepraktijken worden gevolgd [11]. Enkele van de manieren om regelmatige digitale hygiënebeoordelingen op te zetten, zijn de volgende:

- Het ontwikkelen van een routine van gewoonten op het gebied van cyberhygiëne, zoals het scannen op virussen, het wijzigen van wachtwoorden, het bijwerken van software en het opschonen van harde schijven [12].
- De juiste tools gebruiken, zoals een netwerkfirewall, antivirussoftware, versleuteling of back-upoplossingen [13].
- Zoek hulp bij betrouwbare diensten, die kwetsbaarheidsscans, webapplicatiescans en phishing-beoordelingen bieden [14].

## Ontwikkeling van een digitale hygiënecultuur op individueel niveau

Menselijke factoren zijn een van de zwakste componenten van cyberbeveiliging. Enkele voorbeelden van menselijke fouten op het gebied van digitale praktijken kunnen zijn: Slecht wachtwoordbeheer, onbedoelde verwijdering van gegevens of het slachtoffer worden van phishing of andere social engineering-zwendel. Het is echter altijd mogelijk om de risico's te verkleinen door op te letten en digitale hygiënepraktijken te volgen.

Hier zijn enkele belangrijke punten waar elk individu kan bijdragen aan het creëren van een hygiënecultuur binnen een organisatie:

- **Wees bewust van uw digitale voetafdruk [15]:**

Navigeren door online ruimtes kan complex zijn en mensen moeten waakzaam zijn over hun digitale voetafdruk. Volgmechanismen van webbrowsers, e-mailproviders, mobiele apps, zoekmachines en sociale-mediaplatforms kunnen de persoonlijke privacy in gevaar brengen. Om de beveiliging van dagelijkse surfactiviteiten op het web te verbeteren, voert u de volgende stappen uit:

**STAP 1:** Houd rekening met informatie die op sociale platforms wordt gedeeld en log uit bij uw sociale media-accounts, aangezien sociale-mediasites analyses op uw accounts kunnen uitvoeren, zelfs als u ze niet gebruikt [16].

**STAP 2:** Gebruik privacybewuste browsers zoals duckduckgo.com en startpage.com die privacy voorop stellen en gebruikers zoekresultaten bieden zonder gepersonaliseerde tracking.

**STAP 3:** Wees je bewust van de online activiteiten van je sociale kringen[16]: Erken dat de online aanwezigheid van vrienden en familie van invloed kan zijn op je digitale veiligheid. Adviseer hen over veilige online praktijken.

**STAP 4:** Wees je bewust van de instellingen van je smartphone: Net als je laptops zijn ook je smartphones een cruciaal onderdeel van je online activiteiten. Geef prioriteit aan beveiliging door consequent uit te loggen bij apps die gevoelige informatie bevatten. Uitloggen is ook gunstig voor uw werkproductiviteit. Uit een

onderzoek naar het monitoren van smartphonegebruik bleek dat de deelnemers minder tijd doorbrachten in elke sessie door uit te loggen en zich af te melden voor trackingcookies [17].

- **Let op software-updates:**

Regelmatige software-updates zijn essentieel voor een goede digitale hygiëne, aangezien het niet bijwerken van uw software of uw webbrowsers kan leiden tot ernstige kwetsbaarheden.

Een recent voorbeeld dat het belang van software-updates aantoont, deed zich voor in 2021, toen Adobe onthulde dat het stopt met Flash, waarbij beveiligingsproblemen een grote rol speelden in hun beslissing [18]. De beveiligingsproblemen in kwestie omvatten de mogelijkheid om de beveiligingsmaatregelen van webbrowsers effectief te omzeilen. De Computer Emergency Response Teams (CERT's) moesten de problemen aanpakken. Zoals dit voorbeeld laat zien, is aandacht besteden aan updates een belangrijk onderdeel van het beschermen van uw software en applicaties tegen kwetsbaarheden.

- **Gebruik sterke wachtwoorden[19]:**

Zwakke wachtwoorden die gemakkelijk te raden zijn, kunnen individuen en organisaties blootstellen aan het risico van datalekken. Gebruik dus niet je naam of geboortedatum als wachtwoord. De sterkste wachtwoorden zijn de wachtwoorden die gemakkelijk te onthouden zijn, maar moeilijk te kraken. Hier zijn enkele tips voor het maken van sterke wachtwoorden en hoe u ze kunt onthouden[19]:

STAP 1: Construeer een zin met verschillende symbolen, waaronder hoofdletters en kleine letters. Een zin als 'Ik hou van appels, maar ik haat sinaasappels' kan bijvoorbeeld worden omgezet in 'IL@bIH0'

STAP 2: Gebruik tweefactorauthenticatie: Naast het maken van robuuste wachtwoorden, verbeter je je beveiliging met tweefactorauthenticatie (2FA). De authenticatie voegt een extra beveiligingslaag toe door een tweede verificatiestap te vereisen, zoals een code die naar uw mobiele apparaat wordt verzonden, waardoor het risico op geautoriseerde toegang wordt verkleind.

STAP 3: Houd uw wachtwoorden vertrouwelijk en bewaar ze indien nodig veilig met een wachtwoordmanager of authenticator-app zoals Dashlane of 1Password. (Houd er echter rekening mee dat de beveiliging van deze managers slechts zo sterk is als hun zwakste schakel!)

STAP 4: Zorg voor de veiligheid van uw wachtwoorden door ze regelmatig bij te werken.

- **Voorzichtige klikken: pas op voor phishing[14]:**

Phishing is bedoeld om mensen te misleiden om hun gevoelige informatie te geven door zich voor te doen als een betrouwbare bron. Phishing is een ernstig misdrijf. Als oplichters mensen misleiden om persoonlijke informatie te geven, kunnen ze toegang krijgen tot hun e-mail-, bank- of sociale media-accounts. Daarom, als iets er een beetje ongewoon uitziet, of misschien wordt u in een e-mail gevraagd om persoonlijke

informatie te verifiëren, vooral met een bijlage of een link die ze u aanraden om te klikken, vertrouw dan eerst op uw instinct en denk na voordat u klikt.

# Unit 2 - Monitoring, evaluatie en continue verbetering van digitale hygiënepraktijken

Beschouw uw digitale aanwezigheid als een waardevol bezit, zoals uw huis of uw auto. Zoals u regelmatig onderhoudssessies moet hebben om uw auto of huis veilig en functioneel te houden, is het op dezelfde manier belangrijk om uw digitale hygiënepraktijken te controleren om uw systemen continu veilig en functioneel te houden. In deze unit zullen we kijken naar de praktijken die u op institutioneel en individueel niveau kunt realiseren om uw competenties up-to-date te houden naarmate de technologie uitblinkt.

## Praktijken op institutioneel niveau

Hier zijn enkele van de tools en methoden die nuttig kunnen zijn om uw digitale hygiëne op instellingsniveau te monitoren, te beoordelen en te verbeteren.

- **Vind de meest recente EU-regelgeving:**

Het begrijpen en implementeren van de nieuwste regelgeving helpt instituten om de meest urgente problemen te identificeren en dienovereenkomstig te handelen om bedreigingen te beperken en voordelen te benutten.

Een van de ernstigste uitdagingen waar beleidsmakers zich zorgen over maakten, is AI. Op 9 december 2023 heeft de Europese Unie een nieuwe wet ingevoerd, de "AI Act", die tot doel heeft "de potentiële voordelen van de technologie te benutten en tegelijkertijd te beschermen tegen de mogelijke risico's ervan, zoals het automatiseren van banen[20]." Op de hoogte blijven van de nieuwste regelgeving van de Europese Unie inzake AI is cruciaal voor verantwoorde en geautoriseerde digitale praktijken. U kunt bijgewerkte regelgeving, zoals de AI Act, online bekijken op de wetgevingspagina van de Europese Unie, om ervoor te zorgen dat de richtlijnen worden nageleefd en mogelijke juridische implicaties te voorkomen.

- **Veiligheidscontroles:**

Het uitvoeren van een uitgebreide beoordeling van uw beveiligingsinstellingen is cruciaal voor het bewaken van de efficiëntie van uw digitale hygiënerichtlijnen. U kunt gebruik maken van de routinematige beveiligingscontroles van Google en Facebook die u door privacymaatregelen, toestemmingen en controle over uw laatste activiteiten leiden. U kunt ook online bronnen gebruiken waarmee u kunt zoeken naar meerdere datalekken, zoals haveibeenpwnd.com om op de hoogte te zijn van de risico's en de frequentie van datalekken.

- **SWOT-analyse:**

SWOT is een acroniem voor Strengths, Weaknesses, Opportunities en Threats, en het is een strategische analysemethode die een routekaart zal creëren voor het definiëren van de positie van elke organisatie en strategieën voor toekomstige ontwikkeling.

Hier zijn enkele tips om in gedachten te houden bij het uitvoeren van een SWOT-analyse voor uw organisatie volgens een onderzoek naar de e-gereedheid van bedrijven[21]:

1. **Voorbereiding op SWOT-analyse:**
    a. BEGIN MET EEN DOEL: Overweeg het doel en de langetermijneffecten van het toepassen van een SWOT-analyse.
    b. DEFINIEER GEBIEDEN die moeten WORDEN GEANALYSEERD: Identificeer specifieke gebieden die verband houden met de digitale hygiënecultuur, bijv. bewustzijn van werknemers, het volgen van beveiligingsprotocollen, infrastructuur, enz.
    c. WIJS TEAMS toe aan de GEDEFINIEERDE GEBIEDEN: Vorm teams die experts zijn op de gebieden die u wilt analyseren en zorg ervoor dat alle verschillende teams op één lijn zitten over de methodologie voor het uitvoeren van de analyse
2. **Analyse van sterke en zwakke punten:**
    a. IDENTIFICEER UW STERKE EN ZWAKKE PUNTEN: De sterke en zwakke punten van een organisatie zijn tekenen van de interne factoren die de effectiviteit en ineffectiviteit van die organisatie aantonen. Het is belangrijk om rechtvaardigingen op te nemen om de beslissingen over een bepaalde factor als een zwakte te beschouwen. (Verouderde applicaties kunnen bijvoorbeeld als een zwakte worden beschouwd vanwege de vatbaarheid voor aanvallen op de systemen).
    b. BEPAAL DE RELEVANTIE VAN GEÏDENTIFICEERDE PROBLEMEN: Bepalen wat een zwakte is en wat een sterk punt is, kan verwarrend zijn. Onderzoekers stellen [21 voor] met behulp van de '100-puntenmethode' om ze te evalueren en te prioriteren. Aan elk teamlid kunnen 100 punten worden toegewezen aan een sterke of zwakke punten, en hoe meer punten worden toegekend, hoe belangrijker het wordt gevonden. Nadat iedereen zijn punten heeft toegekend, neemt het team het gemiddelde om hun algehele belang te bepalen.
3. **Analyse van kansen en bedreigingen:**
    a. Evalueer de relevantie en waarschijnlijkheid van bedreigingen door te proberen ze in deze categorieën te ordenen: economisch, sociaal, politiek, technologisch en ecologisch.
    b. Bereken de kansen die bij elke ontwikkeling horen. Dit kunnen financiële middelen zijn, een toename van het publieke belang of internationale kansen.
4. **Ontwikkeling van een SWOT-matrix:** Selecteer de sterke en zwakke punten, kansen en bedreigingen en groepeer ze op basis van de hoogste betekenis voor de digitale hygiënecultuur van uw organisatie.

Ontwikkel actieplannen op basis van geïdentificeerde strategieën die: (1) zich richten op het corrigeren van de zwakke punten door gebruik te maken van uw kansen, (2) zich richten op het benutten van een kracht om te profiteren van een kans, (3) zich richten op het minimaliseren van een zwakte om een bedreiging te voorkomen, of (4) zich richten op het benutten van een kracht om een bedreiging te voorkomen.

5. **Bekijk uw resultaten**: Evalueer regelmatig de voortgang van geïmplementeerde strategieën en herhaal de SWOT-analyse regelmatig om u aan te passen aan nieuwe ontwikkelingen in het digitale landschap.

- **Regelmatige back-ups:**

  Back-ups zijn essentieel wanneer het nodig is om gevoelige informatie te herstellen, in het geval van wachtwoordverlies, technische incidenten, enz. Soms is het monitoren van de oorzaken van een systeemcrash ook mogelijk door de beveiligingslekken of fouten in het systeem te bekijken. Het gebruik van een open-source back-upsysteem, zoals UrBackUp, waarmee u een kopie van uw documenten kunt bewaren, kan een waardevol hulpmiddel zijn om uw digitale hygiënepraktijken te controleren en te herzien in geval van nood.

## Oefeningen op individueel niveau

Elk individu speelt een belangrijke rol bij het ontwikkelen van een digitale hygiënepraktijk en er kunnen tal van stappen worden genomen om uw bestaande praktijken te herzien, te controleren en te ontwikkelen. Hier zijn enkele manieren om uw digitale hygiëne op individueel niveau te verbeteren.

- **Bewustwording en educatie:**

Het omarmen van digitale geletterdheid gaat niet alleen over het kennen van tools en methoden, maar ook over het begrijpen van het steeds evoluerende technologische landschap. Onszelf informeren over online bedreigingen en up-to-date blijven kan worden bereikt door deel te nemen aan continue leermogelijkheden zoals Microsoft Digital Literacy Courses, waarin deelnemers kunnen leren over de basisprincipes van digitale geletterdheid, zoals het werken met een computer. evenals geavanceerde competenties zoals het creëren van online inhoud. Evenzo wijzen onderzoekers[22] op het belang van onderwijs over mediageletterdheid en veilig en verantwoord internetgebruik, dat de ervaringen uit het echte leven en de interesses van de individuen moet weerspiegelen.

- **Verantwoordelijk online gedrag:**

Ons online gedrag heeft gevolgen in de echte wereld. Zoals benadrukt in academische studies[23], is het van cruciaal belang om ethisch online te zijn en digitaal geletterd te zijn. Verantwoordelijk online gedrag houdt in dat je met respect en gevoeligheid online discussies aangaat. Bovendien draagt het bewust zijn van digitaal beleid bij aan een veiligere en respectvollere online gemeenschap. Als u niet zeker weet of uw

digitale acties goede praktijken met zich meebrengen. U kunt de Good Digital Citizen-gids van de Universiteit van Michigan gebruiken.

- **Herziening en aanpassing:**

Net als elk aspect van de digitale wereld is het technologische landschap dynamisch en vereist het dat we onze praktijken voortdurend aanpassen. Daarom zijn het beoordelen van onze digitale acties, het aanpassen aan oplichting, het herkennen van phishing-pogingen en het voorzichtig zijn met wat u downloadt, essentiële aspecten van het handhaven van online veiligheid.

Een tool die u kan helpen bij het herzien van praktijken en die regelmatig wordt bijgewerkt, is The Digital Competence Framework of DigComp. Het is een naslagwerk voor instellingen, individuen en opvoeders dat is ontwikkeld door de EU en voortdurend wordt bijgewerkt met de laatste versie 2.2 vanaf de publicatiedatum van dit handboek. DigComp is beschikbaar op de website van EU Publications.

Regelmatige updates van DigComp zorgen ervoor dat het framework relevant blijft en een afspiegeling blijft van de huidige digitale omgeving. Net als DigComp kunt u ook uw digitale hygiënepraktijken herzien en bijwerken om ervoor te zorgen dat ze aansluiten bij de huidige behoeften van uw organisatie, en overwegen om vaardigheden op te nemen die verband houden met opkomende technologieën.

# Unit 3 - De toekomst van digitale hygiëne: uitdagingen en kansen

Naarmate we de toekomst ingaan, zullen we naar verwachting nieuwe uitdagingen en kansen zien in technologische ontwikkelingen. Het evoluerende landschap van digitale technologieën, met name kunstmatige intelligentie (AI), creëert nieuwe complexiteiten, omdat het meer vaardigheden en vaardigheden krijgt. Het begrijpen van deze complexiteiten en kansen is essentieel om een veilige, beveiligde en innovatieve ervaring voor iedereen te garanderen. In deze unit zullen we kijken naar enkele van de meest urgente kwesties voor de toekomst van digitale hygiëne, met een specifieke focus op opkomende technologieën, en wat deze kunnen betekenen voor innovatie.

## A-Opkomende technologieën

Van verschillende opkomende technologieën zoals Blockchain, Robotica, Internet of Things (IoT), Augmented Reality (AR) en Virtual Reality (VR) wordt verwacht dat ze de toekomst vormgeven. Hiervan hebben generatieve AI-chatbots zoals ChatGPT de meeste krantenkoppen gehaald, sinds de oprichting in 2022.

De opkomst van AI brengt nieuwe dimensies met zich mee op het gebied van digitale hygiëne en cybersecurity. AI-technologieën kunnen "al vragen beantwoorden, poëzie schrijven, computercode genereren en gesprekken voeren".[24] Sommige deskundigen zijn van mening dat AI veel werknemers in gevaar zal brengen, aangezien de banen zullen worden geautomatiseerd[25], terwijl veel bedrijven al generatieve AI gebruiken voor hun praktijken[26]. Hoe kan een onderwijsinstelling zoals mbo-instellingen profiteren van de mogelijkheden van AI?

- **Verbetering van de leerervaring:**

Op het gebied van beroepsonderwijs en -opleiding kan generatieve AI een groot potentieel hebben om een revolutie teweeg te brengen in de leerervaring. Onderzoekers suggereren dat AI realistische scenario's, simulaties of beoordelingen kan maken die aansluiten bij de behoeften, interesses en capaciteiten van de student[27]. Realistische scenario's kunnen praktische, meeslepende ervaringen bieden die cruciale ervaringen kunnen creëren voor gebieden zoals de gezondheidszorg. Daarnaast kan het onderwijs in de gezondheidszorg enorm profiteren van het optimaliseren van routinetaken, het stellen van diagnoses of het aanbieden van gepersonaliseerde geneeskunde, wat discussies vereist over het voeren van gesprekken over privacy en robuust bestuur [28].

- **Verbeteren van onderwijs en toetsing:**

Door zich aan te passen aan trends in de branche en AI te integreren in het onderwijs en de beoordeling van beroepsonderwijs en -opleiding in beroepsonderwijs en -opleiding kunnen instructeurs hun workflow

optimaliseren. NGO's en internationale organisaties onderzoeken al de mogelijkheden om de nauwkeurigheid, volledigheid en algehele kwaliteit van het werk van de student te verbeteren, wat ook onmiddellijke feedback kan opleveren[29]. Net als in het onderwijs in de gezondheidszorg zal het geven van AI de mogelijkheid om het werk van leerlingen te beoordelen ongetwijfeld vragen oproepen over de ethiek van AI, een belangrijk discussiepunt dat leraren en ouders in gedachten moeten houden.

- **Adaptieve leerlingbeheersystemen:**

Learning Management Systems (LMS) hebben de horizon van leerkrachten in beroepsonderwijs en -opleiding al verbreed, omdat ze les- en leermateriaal op één locatie aanbieden en de voortgang en prestaties van leerlingen volgen[30]. Met AI heeft LMS de mogelijkheid vergroot om een revolutie teweeg te brengen in LMS [31]. AI-aangedreven LMS kan geavanceerde taken uitvoeren die verder gaan dan automatisering, waaronder het voorspellen van de prestaties van studenten, waardoor docenten strategieën kunnen ontwikkelen voor het verbeteren van de prestaties van studenten [32]

## B-Uitdagingen op het gebied van regelgeving

In de bovenstaande eenheden hebben we al onderzocht hoe nieuwe technologische ontwikkelingen meer baanbrekend worden in verschillende industrieën en onderwijssystemen. Deze vooruitgang vereist dat alle belanghebbenden verantwoordelijk en aangemoedigd zijn voor een veiliger gebruik van opkomende technologieën. Kwesties als gegevensprivacy, algoritmische vooringenomenheid, ethisch gebruik en verantwoordingsplicht vereisen uitgebreide regelgevingskaders.

- **Gegevensprivacy in het onderwijs**

In de context van het onderwijs, en met name het online onderwijs dat met grote hoeveelheden gegevens omgaat, zijn er zorgen over privacy en veiligheid [33]. Ongeoorloofde toegang tot een cloud of misbruik van gevoelige informatie vormt een aanzienlijk risico voor onderwijsinstellingen en sinds 2018 verplicht de Algemene Verordening Gegevensbescherming (AVG) van de EU alle instellingen binnen en buiten de EU om te voldoen aan haar bezwaren voor de bescherming en verplaatsing van persoonsgegevens [34]. Daarom wordt het voor elke instelling voor beroepsonderwijs en -opleiding aangemoedigd om toezicht te houden op de naleving van de AVG en de nodige maatregelen toe te passen naarmate deze zich ontwikkelt.

- **Algoritmische vooringenomenheid**

Een AI-aangedreven LMS kan vooroordelen erven van de gegevens die worden gebruikt om het te trainen. Op het gebied van werkgelegenheid kunnen AI-aangedreven arbeidsprocedures bijzonder schadelijk zijn voor sommige groepen, zoals ontdekt in het geval van een Amazon-wervingsproces waarbij het voorspellende systeem werd getraind met de cv's van een meerderheid van mannelijke kandidaten. Dit creëerde een vooroordeel waarbij de mannelijke kandidaten meer de voorkeur kregen boven vrouwelijke kandidaten [35].

Docenten moeten zich zelf bewust zijn van dit aspect van AI-aangedreven systemen en hun eigen vooroordelen over studenten controleren. Het wordt ook steeds belangrijker voor beleidsmakers om de ontwikkeling van controleerbare en transparante algoritmen aan te moedigen [36].

- **Ethiek van opkomende technologieën**

Net als de bezorgdheid over algoritmische vooringenomenheid, roept de integratie van opkomende technologieën zoals AI in het onderwijs aanzienlijke vragen op. Wat zou de rol moeten zijn van opkomende technologieën in het onderwijs in termen van besluitvorming? Zijn er significante verschillen tussen diverse studentengroepen over de invloed van opkomende technologieën op hun leerproces?

Op het gebied van AI beschouwen onderzoekers privacy, vooringenomenheid, toezicht en autonomie als belangrijke gebieden die wijzen op ethische uitdagingen voor het gebruik van deze systemen in het onderwijs [37]. Deze gebieden, evenals de bovenstaande voorbeeldvragen, vereisen meer professionele ontwikkelingsmogelijkheden voor leraren om toekomstige generaties voor te lichten over het ethische gebruik en de ethische ontwikkeling van AI. In dit verband kunnen initiatieven zoals het Digital Competence Framework (DigComp) van de EU als waardevolle leidraad dienen.

Uitvoerende actievoerders zoals de Europese Raad erkennen het belang van het bevorderen van ethisch gebruik van AI en zijn al bezig met het definiëren van ethische richtlijnen en het bevorderen van transparantie die de technologiebedrijven verantwoordelijk zal houden. Afgezien van de hierboven genoemde verordening inzake de AI-verordening ontwikkelt de Europese Unie ook beleid ter ondersteuning en bevordering van het gebruik van opkomende technologieën, zoals VR, robotica en biotechnologie, die naar verwachting grotere gevolgen zullen hebben voor het leven van de burgers [38].

## C-Kansen voor innovatie

Volgens een OESO-rapport uit 2021 zijn virtual reality, augmented reality, robotica en kunstmatige intelligentie steeds wijdverbreider geworden in beroepsonderwijs en -opleiding voor veel sectoren, zoals logistiek, landbouw, horeca, energie en informatietechnologie, en zal het de komende jaren nog vaker voorkomen [39]. In dit gedeelte zullen we bekijken hoe verschillende industrieën deze technologieën al gebruiken en welk potentieel in het verschiet ligt.

- **Informatietechnologie (IT)**

Opkomende technologieën zoals virtual reality-cloudlabs kunnen IT-studenten praktische ervaring bieden op verschillende gebieden, zoals netwerkconfiguratie of cyberbeveiliging [40]. Cybersecurity Labs [vul hier een woordenlijst in] simuleert cyberdreigingen en -aanvallen en biedt studenten in het beroepsonderwijs een praktische omgeving om de kwetsbaarheden in digitale systemen te begrijpen zonder echte risico's te lopen.

Systemen zoals High-Performance Computing [vul hier een woordenlijst in], evenals Blockchain [vul hier een woordenlijst in], bieden nieuwe manieren om cyberbeveiliging te trainen [41].

- **Logistiek en transport**

Commerciële producten zoals simulatiegames kunnen studenten helpen om echte uitdagingen aan te gaan, en in het geval van logistiek doet een commercieel beschikbaar spel genaamd Truck & Logistics Simulator precies dat, waarbij studenten logistieke taken van begin tot eind kunnen uitvoeren . Aangezien technologie een cruciale rol speelt bij de planning van complexe taken, moeten aanbieders van beroepsonderwijs en -opleidingen, docenten en studenten een goede digitale hygiëne toepassen en de integriteit van informatie in de logistieke netwerken waarborgen terwijl ze informatie delen met gecommercialiseerde producten.

- **Landbouw**

Van drones tot AI, opkomende technologieën hebben het potentieel om de productiviteit van landbouw en landbouwpraktijken te verhogen, de impact op het milieu te verminderen en hogere inkomens te garanderen. Drone-onderzoeksmodellen met een hogere resolutie kunnen resulteren in een efficiëntere irrigatieplanning en een nauwkeurigere monitoring van gewassen en vee [42]. Op dezelfde manier kan AR worden gebruikt om slimme landbouw te bevorderen [43,] die tot doel heeft risico's te minimaliseren, gewasopbrengsten te verhogen en stress in de agribusiness te verminderen [44]. De risico's die verbonden zijn aan het gebruik van sommige van deze technologieën mogen echter niet worden verwaarloosd [45]. Door een goede cyberhygiëne te handhaven en verantwoorde AI-praktijken toe te passen, kunnen de risico's van het gebruik van AI, AR en andere opkomende technologieën worden beperkt.

- **Gastvrijheid**

Horeca is een van de belangrijkste sectoren in veel landen in Europa, draagt bij aan de economie en zorgt voor miljoenen banen. Emerging Technologies kan meeslepende leerervaringen bieden voor studenten gastvrijheid en toerisme. Simulaties van hotelbeheer en klantenservicescenario's, mogelijk gemaakt door het Internet of Things [vul hier de definitie van de woordenlijst in] waarmee de kamertemperatuur, verlichting en andere functies kunnen worden geregeld, kunnen betere ervaringen voor gasten creëren[46]. VR-trainingsmodellen die ervaring hebben met het dragen van een headset zijn al gebruikt door prominente horecaleiders in de branche [47]. De gesimuleerde wereldervaring kan mensen helpen sneller te leren, kennis voor een langere tijd vast te houden en meer betrokken te zijn bij training [48]. Hoezeer deze ontwikkelingen de gebruikerservaring ook verbeteren, ze kunnen voor sommige gebruikers ook storend en desoriënterend zijn. Daarom is het belangrijk om bij het doorvoeren van veranderingen rekening te houden met de gebruikersinterface en gebruikerservaring [49].

- **Hernieuwbare energie**

Opkomende technologieën zoals AI-aangedreven voorspellende onderhoudssystemen, verbonden sensoren en augmented reality kunnen de acceptatie van hernieuwbare energiebronnen versnellen [50,] terwijl het simuleren van de werking en het onderhoud van zonnepanelen, windturbines of waterkrachtsystemen studenten in staat stelt praktische vaardigheden op te doen in een gecontroleerde omgeving [51]. Net als in de landbouwsector brengt het gebruik van opkomende technologieën aanzienlijke risico's met zich mee, waardoor digitale hygiënepraktijken een belangrijk middel zijn om de systemen te beschermen[52]

Het gebruik van innovatieve technologie zoals robots, virtual reality (VR), augmented reality (AR) en simulatoren stelt leraren in staat om de beroepsvaardigheden van studenten te ontwikkelen en tegelijkertijd hun digitale en zachte vaardigheden te bevorderen. Deze technologieën zullen de komende jaren waarschijnlijk gebruikelijker worden in beroepsonderwijs en -opleiding, omdat ze voordelen hebben op het gebied van flexibiliteit, kosten en veiligheid. [39] Het aanleren van goede digitale hygiëne is essentieel om digitale technologie op veilige, gezonde, verantwoorde en respectvolle manieren in ons leven te integreren [9]

# Unit 4 - Digitale hygiënecultuur Good Practice Use Case:

In de vorige units hebben we ons verdiept in de belangrijke aspecten van het cultiveren van een robuuste digitale hygiënecultuur in zowel start-ups als instellingen voor beroepsonderwijs en -opleiding. We onderzochten het belang van het monitoren, herzien en voortdurend verbeteren van digitale hygiënepraktijken om een veilige en efficiënte digitale omgeving te garanderen. Uit deze discussies kwam naar voren hoe belangrijk het is om een goede digitale hygiënecultuur te cultiveren.

Nu, terwijl we het laatste deel van module 3 binnenstappen, in Unit 4, staan we op het punt om in real-world toepassingen te duiken met voorbeelden die de praktische gebruiksscenario's van digitale hygiëneprincipes laten zien.

## Gebruiksscenario's voor digitale hygiëne over de hele wereld

- **Een gespecialiseerde toolkit om digitale hygiënepraktijken te promoten (Servië)**

Een opmerkelijk voorbeeld van de toepassing van goede digitale hygiënepraktijken is een gids die is opgesteld door Share Cert, een in Belgrado gevestigde stichting die de nadruk legt op strategische cyberbeveiligingsmaatregelen[53]. Door systematische categorisering van de meest voorkomende bedreigingen en beveiligingsmaatregelen wordt deze gids ondersteund door een open platform waar individuen en organisaties kunnen worden geïnformeerd over de meest urgente onderwerpen in de digitale omgeving en algemene tips kunnen krijgen over de digitale hygiënecultuur.

- **Bewustmakingscampagnes voor de bescherming van digitale rechten (Griekenland)**

Een ander belangrijk initiatief op het gebied van de bescherming van digitale rechten is gevestigd in Griekenland en heet Homo Digitalis, een niet-gouvernementele organisatie (NGO) die zich richt op het recht op privacy, de bescherming van persoonsgegevens, het verbod op discriminatie in digitale ruimtes en vrijheid van informatie. Met hun meer dan 100 leden nemen zij actief deel aan studies en voeren zij onderzoeken uit namens het algemeen belang, wat op zijn beurt wetgevers kan helpen de kwesties in verband met digitale rechten beter te begrijpen [54].

- **Een kit voor snelle respons voor een steeds digitalere burgermaatschappij (wereldwijd)**

De internationale netwerken van Computer Emergency Response Teams (CERT's) en Rapid Response Network (RaReNet) hebben samengewerkt om snelle hulpverleners, trainers op het gebied van digitale beveiliging en technisch onderlegde activisten te helpen zich beter te beschermen tegen de meest voorkomende soorten digitale noodsituaties met een zogenaamde digitale EHBO-doos, die een verscheidenheid aan problemen begeleidt [55]. De digitale EHBO-kit is beschikbaar in 13 talen en evolueert voortdurend met bijdragen van buitenaf,  en is een waardevolle bron voor het bevorderen van een verantwoord en veilig gebruik van internet.

- **Veerkrachtige tools ontwikkelen om digitale hygiënepraktijken voor het maatschappelijk middenveld bij te houden (wereldwijd)**

Het Center of Digital Resilience is een non-profitorganisatie die actief is in meer dan 20 landen met de bedoeling veerkrachtige digitale systemen op te zetten om de veiligheid van het maatschappelijk middenveld te waarborgen [56]. Hun projecten omvatten het aanbieden van diensten en instrumenten, zoals een crowdsourcingtool die is ontworpen voor het identificeren en rapporteren van valse informatie, een digitaal platform voor het melden van beveiligingsproblemen, een visualisatietool voor het monitoren van bedreigingen en aanvallen op de digitale systemen, en een community-tool die gericht is op het creëren van een sterk participatienetwerk binnen het CiviCERT.

- **Netwerken die de uitwisseling tussen responsteams wereldwijd vergemakkelijken inhoud om digitale hygiënepraktijken voor het maatschappelijk middenveld bij te houden (wereldwijd)**

CiviCERT is een netwerk dat CERT's, onafhankelijke internetinhouds- en serviceproviders, evenals ngo's en individuen 57 samenbrengt. De leden van het netwerk uitvoeren, coördineren en ondersteunen de reactie op digitale beveiligingsincidenten die aan hen worden gemeld in een samenwerkingsmechanisme waarbij het standpunt van andere partners nodig is. CiviCERT zelf houdt gelijke tred met goede digitale hygiënepraktijken, waarbij de leden communiceren via versleutelde platforms, zoals een versleutelde mailinglijst en een Malware Information Sharing Platform, om informatie te delen over opkomende bedreigingen voor het maatschappelijk middenveld, en sjablonen om betrouwbare en gestandaardiseerde procedures te garanderen om noodsituaties aan te pakken.

- **Bevordering van digitale mensenrechten in ontwikkelingslanden in (West-Azië en Noord-Afrika)**

SMEX is een ngo die opkomt voor mensenrechten in digitale omgevingen in West-Azië en Noord-Afrika [58]. Op het gebied van digitale hygiënepraktijken bieden ze ondersteuning aan internetgebruikers, activisten en mensenrechtenorganisaties voor hun cyberbeveiligingsproblemen, en creëren ze programma's om het grote publiek te informeren over de regelgeving en internetwetgeving. SMEX werkt ook actief samen met lokale en internationale partners om het bewustzijn en de implementatie van digitale hygiënepraktijken te bevorderen, waardoor een veiligere online omgeving wordt bevorderd voor individuen en organisaties die pleiten voor mensenrechten in de digitale ruimte in West-Azië en Noord-Afrika.

- **Een curriculum voor digitale vaardigheden voor K-12-studenten (Noord-Amerika)**

Het concept van digitale hygiëne wordt steeds belangrijker gevonden in de onderwijssystemen wereldwijd. Een van de organisaties die gespecialiseerd is in het voorbereiden van digitaal geletterdheidsmateriaal dat specifiek is voor K-12-studenten, is Common Sense Media, een onafhankelijke organisatie gevestigd in Noord-Amerika die tot doel heeft studenten, ouders en leraren te voorzien van datagestuurde inzichten over de impact van media en digitale omgevingen op de fysieke, emotionele, sociale en mentale behoeften van de kinderen [59]. Hun door onderzoek ondersteunde curriculum voor digitaal burgerschap behandelt belangrijke media- en technologiekwesties op scholen, zoals: Hoe pesten te beschermen? Hoe beschermen we onze privacy? en Hoe om te gaan met verkeerde informatie?

- **Educatief materiaal voor betere digitale geletterdheid (Noord-Amerika)**

Center of Digital Literacy is een Amerikaanse non-profitorganisatie die tot doel heeft het onderzoek naar en de creatie van open-sourcemateriaal [60 te bevorderen] , evenals tools, lessen, activiteiten en beoordelingen voor het ontwerpen van leerplannen die kunnen worden gebruikt en aangepast aan verschillende onderwijscontexten [61]. Mediageletterdheid is een belangrijk onderdeel van digitale hygiënepraktijken en de nadruk op mediageletterdheid verbetert niet alleen de digitale hygiëne, maar cultiveert ook een beter geïnformeerde en kritische samenleving, die beter voorbereid is om deel te nemen aan de complexiteit van de digitale wereld.

- **Europese Maand van de Cyberbeveiliging (Europa)**

Elk jaar wordt oktober gevierd als de Europese Maand van de Cyberbeveiliging (ECSM), een belangrijk jaarlijks evenement dat wordt georganiseerd door het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) en de Europese Commissie [62]. ECSM is gericht op het versterken van het cyberbeveiligingsbewustzijn onder EU-burgers en -organisaties en is een van de vele multidimensionale benaderingen van de EU voor het bevorderen van goede digitale hygiënepraktijken. In oktober creëren conferenties, workshops en webinars een uitgebreide campagne die niet alleen het bewustzijn over cyberbeveiliging vergroot, maar ook actief bijgewerkte informatie en deskundig advies deelt. Met het oog op het bevorderen van een veiliger gebruik

van internet, biedt ECSM tips voor digitale hygiëne en komt het naar voren als een alomvattende en gezamenlijke inspanning, verwant aan wereldwijde netwerken zoals CiviCERT en regionale NGO's zoals SMEX, die een cruciale rol spelen bij het bevorderen en ondersteunen van goede digitale hygiënepraktijken in de hele Europese Unie.

- **Cybersecurity-game voor kleuters (wereldwijd)**

Interland [63] is een interactief spel van Google dat deel uitmaakt van 'Be Internet Awesome' [64], een geïntegreerd programma voor het promoten van digitale hygiënepraktijken onder jonge leerlingen. Als een dynamisch en interactief spel betrekt Interland studenten door middel van zijn gameplay en biedt het een praktische benadering voor het onderwijzen van enkele van de kernaspecten van goede digitale hygiënepraktijken door middel van gamification [65] BRON. Complexe kwesties zoals privacy, phishing, hacken en cyberpesten worden vertaald naar jongere studenten in kleurrijke animaties die geschikt zijn voor hun competentieniveau [66] Over het algemeen is Interland een opmerkelijk voorbeeld van het bijbrengen van goede digitale hygiënepraktijken vanaf jonge leeftijd door het gebruik van technologie.

In deze module hebben we de implementatie van en het belang van goede digitale hygiënepraktijken besproken. We hebben gekeken naar onderwerpen als het ontwikkelen van een digitale hygiënecultuur in uw organisatie op verschillende managementniveaus, het verkennen van methoden voor continue verbetering van deze praktijken, het informeren over toekomstige oogstmogelijkheden en uitdagingen die moeten worden overwonnen, en vervolgens het verkennen van casestudy's van over de hele wereld.

Bekijk de andere modules van deze gids voor meer advies en strategieën over goede digitale hygiënepraktijken, en bezoek de website van Good Digital Hygiene for Startups.

# Bronnen

**Unit 1 - Building a Digital Hygiene Culture in Startups and VET Institutions**


[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]

## Unit 2 - Monitoring, Review, and Continuous Improvement of Digital Hygiene Practices

[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.

**Unit 3 - The Future of Digital Hygiene: Challenges and Opportunities**

[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]

**UNIT 4 - Digital Hygiene Culture Good Practice Use Case:**

[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]