LINKS

Co-funded by the European Union

Rammen for Digital suveræ nitets-kompetencer

Co-funded by
the European Union

Dette projekt har støtte fra EU-Kommissionen gennem Erasmus+ programmet. Denne publikation afspejler kun forfatterens synspunkter, og Kommissionen kan ikke holdes ansvarlig for enhver brug, der måtte blive gjort af oplysningerne deri.

Læs mere om

LINKS

Introduktion

Introduktion

LINKS-projektet har til formål at støtte europæiske ungdomsarbejdere i at opnå deres datasuverænitet og forbedre deres digitale sikkerhedsfærdigheder gennem en ny, innovativ form for træningsindhold, der understøtter digital kompetenceopbygning.
Under de indledende planlægningsfaser af dette projekt og ansøgning understøttede behovsanalysen ideen om, at der i øjeblikket ikke findes en enkelt digital suverænitets- og sikkerhedskompetenceramme for Europa.

DigComp (Digital Competence Framework) refererer til mange af de overordnede og generelle kernefærdigheder og kompetencer relateret til digital sikkerhed som helhed, og dette output vil referere til denne eksisterende kompetenceramme, men er specifikt målrettet mod proaktiv bevidsthed hos ungdomsarbejdere i hele Europa om den digitale sikkerhedstrusler, der i øjeblikket eksisterer.

Rammen for digitale suverænitetskompetencer definerer nøglekomponenterne i de kompetencer, som ungdomsarbejdere har brug for for effektivt at integrere digitale suverænitets- og sikkerhedsprotokoller i deres lokaliserede kontekster og tilvejebringe og validere en EU-referenceramme til udvikling og evaluering af digitale sikkerhedskompetencer. Digitale sikkerhedskompetencer er stærkt knyttet til generiske digitale kompetencer og betragtes ikke som kompetencer i sig selv.

Rammen er rettet mod ungdomsarbejdere, men er også relevant og af interesse for IKT-lærere, undervisere, undervisere og politikere inden for uddannelse og livslang læring i forbindelse med teknologisk opkvalificering og kapacitetsopbygning af enkeltpersoner.

Vi forventer, at digitale uddannelses-NGO'er og uddannelsesorganisationer i hele Europa vil anvende denne ramme som en del af deres uddannelsesmæssige vurderings- og undervisningsaktiviteter, hvilket på lang sigt vil øge bevidstheden og tilskynde til integrationen af rammerne i lokale, regionale og nationale digitale uddannelser organer i europæiske lande.

Resultater af projektundersøgelsen og fokusgrupper

Den digitale suverænitetskompetenceramme er baseret på metodologien, resultaterne af projektundersøgelsen og fokusgruppernes resultater. Det ser også ud til at tilpasse sig DigComp Framework, som understøtter langsigtet udnyttelse og bæredygtighed som en yderligere, målgruppespecifik kompetenceramme.

Projektundersøgelsen hjalp med at lære om brugen af teknologi og databeskyttelse i ungdomsarbejderes digitale arbejdspraksis. Ungdomsarbejdere har brug for større bevidsthed kombineret med god styring af digitale identiteter; det kan hjælpe med at begrænse hændelser forårsaget af brugerens eller organisationens "uopmærksomhed". De skrev om behovet for at opsætte og kommunikere sikkerhedspolitikker for fjernarbejde, regulere brugen af personlig enhed, sikre kommunikations- og samarbejdskanaler og give årvågen it-support. De anbefalede at gøre kurser tilgængelige for flere medarbejdere og unge, ved at bruge relevante eksempler på specifikke opgaver, forbedre netværk og dele gode og dårlige erfaringer online. Det er vigtigt at blive ved med at opdatere, især med nye EU-dokumenter.

De fleste ungdomsarbejdere har ikke modtaget målrettet uddannelse, de træffer valg om online sikkerhed baseret på egen viden. De skrev, at det er nødvendigt at uddybe disse aspekter af hensyn til organisationernes og private brugeres sikkerhed og at organisere særlig uddannelse for databeskyttelsesansvarlige.

Behovet for den digitale suverænitetskompetenceramme

Der er stigende bekymring for, at borgere, virksomheder og medlemslande i EU gradvist mister kontrollen over deres data, innovationskapacitet og evne til at forme og håndhæve lovgivning i det digitale miljø. På denne baggrund er støtten til en ny politisk tilgang designet til at styrke Europas strategiske autonomi på det digitale område vokset.

Teknologivirksomheder indsamler enorme mængder af personlige data, og bekymringen er vokset i EU for, hvordan europæiske borgere kan genvinde kontrollen over deres digitale data i et onlinemiljø, der primært er domineret af ikke-EU-teknologivirksomheder.

Efterhånden som ungdomsarbejdet i stigende grad tilpasser sig den digitale verden, ser vi ungdomsarbejdere tage nye tilgange til sig. Selvom det digitale er nyt og spændende og byder på utallige muligheder, kræver det ikke desto mindre en forbedret forståelse i forbindelse med ungdomsarbejde. Der er behov for flere tiltag for at kortlægge eksisterende digitale ungdomsarbejdspraksis, platforme, værktøjer og læringsrammer vedrørende digitale suverænitetskompetencer.

Digital suverænitet er et nyt koncept i den digitale æra, almindeligvis forstået som "enkeltpersoners evne til at eje deres private data og kontrollere deres brug".

COVID-19-pandemien har i høj grad påvirket de fleste menneskers dagligdag. Som reaktion herpå er teknologien blevet tilpasset for at forsøge at afbøde disse virkninger, ved at tilbyde enkeltpersoner digitale alternativer til mange daglige aktiviteter, som typisk ikke længere kan gennemføres. Virtuelt socialt samvær og onlinebegivenheder er blevet almindelige og har gået langt for at forhindre folk i at blive fuldstændig isoleret, mens de er i lockdown.

Online uddannelse er også blevet det nye normale mange steder, da skoler og universiteter henvender sig til online klasser for at holde elevernes uddannelse på sporet. Da enkeltpersoner har mere fleksible tidsplaner eller mere fritid under nedlukningen, har der været en betydelig stigning i mennesker, der bruger personlige lærings- og udviklingsværktøjer som sprogindlæringsapps. Sundhedsvæsenet har også vendt sig mod digitale løsninger, og det er blevet mere almindeligt at gøre psykisk og fysisk sundhedsvæsen tilgængeligt online. Det har haft relativt succes med at afbøde de negative virkninger af nedsat adgang til sundhedsydelser.

Existing relevant frameworks

Der er udviklet forskellige digitale pædagogiske kompetencerammer til at understøtte professionelle læreres effektive og meningsfulde kriteriebaserede faglige udvikling af digitale pædagogiske kompetencer.
Europæiske rammer, der er offentliggjort i de senere år, skitserer, hvordan en digitalt kompetent uddannelsesorganisation, DigCompOrg, og digitalt kompetent undervisningspersonale DigCompEdu skal se ud, og tilskynder organisationer til at sikre deres medarbejderes kompetencer og udvikle nationale løsninger til at sikre digital kompetence.

DigCompEdu er en digital kompetenceramme og har hovedsageligt en målgruppe af universitetsprofessorer og medarbejdere.
DigComp-rammen identificerer de kritiske komponenter i digital kompetence på fem områder:
1. Information og datafærdighed: At formulere informationsbehov, lokalisere og hente digitale data, information og indhold. At bedømme relevansen af kilden og dens indhold. Til at gemme, administrere og organisere digitale data, information og indhold.
2. Kommunikation og samarbejde: At interagere, kommunikere og samarbejde gennem digitale teknologier og samtidig være opmærksom på kulturel og generationsmæssig mangfoldighed. At deltage i samfundet gennem offentlige og private digitale tjenester og deltagende medborgerskab. At styre sin digitale tilstedeværelse, identitet og omdømme.
3. Oprettelse af digitalt indhold: At skabe og redigere digitalt indhold At forbedre og integrere information og indhold i en eksisterende viden og samtidig forstå, hvordan ophavsret og licenser skal anvendes. At vide, hvordan man giver forståelige instruktioner til et computersystem.
4. Sikkerhed: For at beskytte enheder, indhold, personlige data og privatliv i digitale miljøer. At beskytte fysisk og psykisk sundhed og være opmærksom på digitale teknologier til social velvære og inklusion. At være opmærksom på miljøpåvirkningen af digitale teknologier og deres brug.
5. Problemløsning: At identificere behov og problemer og løse konceptuelle problemer og bekymringer i digitale miljøer. At bruge digitale værktøjer til at innovere processer og produkter. At holde sig ajour med den digitale udvikling.

Der er en DigComp Conceptual referencemodel, hvor 21 kompetencer er relevante for disse områder. Yderligere dimensioner ou

Den Digitale suverænitetskompetenceramme for ungdomsarbejdere

Baseret på en undersøgelse og analyse af eksisterende rammer besluttede partnerne i dette projekt at fokusere på fire sikkerhedsemner i DigiComp og tilføje de nødvendige kompetencer til ungdomsarbejdere. Her er kompetencerne i DigiComp-rammen:

4.1 Beskyttelse af enheder

Beskyt enheder og digitalt indhold og forstå risici og trusler i digitale miljøer. At kende til sikkerheds- og sikkerhedsforanstaltninger og tage behørigt hensyn til pålidelighed og privatliv.

4.2 Beskyttelse af personlige data og privatliv

For at beskytte personlige data og privatliv i digitale miljøer. At forstå, hvordan man bruger og deler personligt identificerbare oplysninger, mens man beskytter sig selv og andre mod skader. For at forstå, at digitale tjenester bruger en "privatlivspolitik" til at informere om, hvordan personlige data bruges.

4.3 Beskyttelse af sundhed og velvære

For at undgå sundhedsrisici og trusler mod fysisk og psykisk velvære ved brug af digitale teknologier. Beskyt sig selv og andre mod mulige farer i digitale miljøer (f.eks. cybermobning). At være opmærksom på digitale teknologier til social trivsel og social inklusion.

4.4 Beskyttelse af miljøet

At være opmærksom på miljøpåvirkningen af digitale teknologier og deres anvendelse.

https://joint-research-centre.ec.europa.eu/digcomp/digital-competence-framework_en#ref-4-safety

Når man definerer væsentlige digitale kompetencer for ungdomsarbejdere, er det nyttigt at overveje de universelle (DigComp-kompetencer for borgere) og specifikke (daglige aktiviteter i ungdomsarbejdet) træk ved den resulterende praktiske læring.

Kompetencer til at beskytte persondata og privatliv

* tekniske digitale teknologiske færdigheder,
* evnen til at bruge digitale teknologier på en meningsfuld måde til arbejde, studier og andre daglige aktiviteter;
* Evnen til kritisk at vurdere digitale teknologier;
* at kende de grundlæggende regler vedrørende online sikkerhed;
* at forstå, hvordan online fungerer;
* at forstå, hvad e-marketing er, og hvordan det fungerer;
* at forstå privatlivets fred og være opmærksom på intellektuelle ejendomsrettigheder;
* at vide, hvordan man implementerer sikkerhedsforanstaltninger;
* at udvikle selveffektivitet ved hjælp af digitale teknologier.

Kompetencer til at beskytte enheder

Beskyttelse af computeren og smartphonen med robust og opdateret sikkerhedssoftware. Hvis computeren eller telefonen er inficeret med ondsindet software, er andre sikkerhedsforanstaltninger til ringe hjælp, fordi kriminelle måske allerede har nøglen til alle onlinehandlinger. Det er også vigtigt at være sikker på, at alle operativsystemopdateringer er installeret. Ungdomsarbejdere bør tage sig af alle deres egne enheder. De skal være opdateret med effektiv antivirussoftware. Forskellige producenter udgiver opdateringer, der forbedrer funktionerne og retter eventuelle sikkerhedsfejl, der kan sætte enheder på.
I fare. Som en generel sikkerhedsregel er det tilrådeligt ikke at bruge nogen anden computer eller enhed til aktiviteter, der kræver, at du 'logger ind' på nogen af de tjenester, du bruger.

At lære at spotte spam og svindel

Selvom nogle er nemme at identificere, kan andre phishing-forsøg i e-mails, sociale netværkssider eller websteder se legitime ud. Den eneste måde at aldrig falde for phishing-svindel er ved aldrig at klikke på et link, der er blevet sendt. Hvis e-mailen siger, at det er fra en bank med alle de korrekte logoer og kender navnet, kan det være fra den faktiske bank eller ej. I stedet for at bruge det angivne link, kan det at finde webstedet og bruge en søgemaskine hjælpe med at forhindre fidusen. På denne måde vil brugeren vide, om han er landet på et legitimt websted og ikke et falskt websted.

Brug af anerkendte websteder, når du foretager køb

Hvis en bruger ikke kender omdømmet til en virksomhed, han ønsker at købe fra, er det vigtigt at studere webstedet, før du gør det. Spørg: "Hvordan anmelder andre brugere dem?". Bruger de en sikker, krypteret forbindelse til personlige og økonomiske oplysninger?"

Forbliver opmærksom

De er på vagt over for offentlig WiFi og tænker sig om to gange, før de tilslutter sig et usikkert netværk. Nogle værktøjer kan hjælpe brugere med at få mere privatliv og beskytte sig mod andre brugere og websteder på offentlige WiFi-netværk under browsingaktivitet.

Hold dig sikker online

Onlineverdenen er blevet så hurtigt i forandring, at dagens tips måske er forældede i morgen. Ungdomsarbejdere skal være opmærksomme på, at det indhold, de forbruger (som nogle gange kan være meget af det) skal filtreres. Det er vigtigt at være lidt mistænksom. Det er relativt nemt at forfalske ting på internettet. Det er nemt at placere noget på internettet, som ikke er helt sandt eller løgn. Vi skal passe på ikke at tro på alt, hvad vi ser og læser online. Som et godt råd bør vi grave dybere for at skelne, hvad der er sandt, og hvad der ikke er, hvis vi er i tvivl om noget. Prøv at være kritisk omkring ting online og minimer dermed risikoen forbundet med onlineaktiviteter.

Deling af oplysninger på sociale netværk

"Informationsdeling beskriver dataudvekslingen mellem forskellige organisationer, mennesker og teknologier" (Techopedia). Der er flere typer informationsdeling: Oplysninger delt af enkeltpersoner (såsom en video delt på Facebook eller YouTube);

- Information, der deles af organisationer (såsom RSS-feedet for en online vejrrapport);
- Oplysninger, der deles mellem firmware/software (såsom IP-adresserne på tilgængelige netværksknuder eller tilgængeligheden af diskplads)

Alle sociale netværk (eller de fleste af dem) lader brugere oprette profiler så detaljerede som de ønsker. I nogle tilfælde hjælper denne procedure brugerne med at finde andre brugere med fælles interesser. På sociale medier som Facebook er det muligt at ændre privatlivsindstillingerne for at kontrollere, hvilke oplysninger der er offentlige, og hvilke oplysninger der kun opbevares for "venner". Det er dog vigtigt at vide, at sociale netværk har disse oplysninger uanset privatlivsindstillinger.

Normalt deler folk alder, køn, familie, andre interesser, uddannelsesbaggrund og detaljer relateret til deres beskæftigelse. At poste billeder eller "status" er en hurtig måde at vise følelser og situationer og dele information. De fleste sociale netværk er designet til at opnå det på den hurtigst mulige måde. Det er vigtigt at være opmærksom på de ting, en bruger deler. Deling afslører de oplysninger, der gør det muligt for annoncører at spore potentielle forbrugeres præferencer og smag.

GDPR

GDPR blev anvendt på alle medlemmer af EU og EØS fra og med den 25. maj 2018. Den har erstattet nutidens lovgivning vedrørende privatlivets fred i medlemslande, der i øjeblikket er underlagt EU-direktivet 95/46. GDPR er mere detaljeret og præcist på visse områder og tager højde for udfordringerne i den hastigt udviklende digitale verden, hvilket giver anledning til privatlivsrisici for registrerede.

Referencer

Data protection and online privacy

https://europa.eu/youreurope/citizens/consumers/internet-telecoms/dataprotection-online-privacy/i ndex_en.htm

Techopedia

https://www.techopedia.com/definition/24839/information-sharing

Step-by-step guidelines on setting up your computer and creating a user

https://www.wikihow.com/Use-a-Computer

Privacy Rights

https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and -social