NTNU studier for lærere

Videreutdanning for lærere, nettbasert

**Grunnleggende cyber- og informasjonssikkerhet for lærere i videregående opplæring**

Studiet inngår i et nasjonalt prosjekt for å styrke lærerens bevissthet og kompetanse om cyber- og informasjonssikkerhet i skolen, kalt CyberSMART**.**

CyberSmart er et nettstudium som først tar for seg de grunnleggende ferdigheter i cyber- og informasjonssikkerhet, med vekt på hvordan digital kompetanse kan formidles og anvendes for elever i videregående opplæring. Studiet tar utgangspunkt i nye læreplaner der bruken av digitale verktøy er en grunnleggende ferdighet. Derfor kobles relevant teori med praktiske øvelser og tar i bruk digitale verktøy i undervisningen som fremmer digital dømmekraft, problemløsning og gode digitale medborgere. Digitale ferdigheter er en viktig forutsetning for videre læring og for aktiv deltakelse i et arbeidsliv og i et samfunn i stadig endring. Studiet er inspirert av det amerikanske GenCyber programmet som har vist seg å engasjere og inspirere ungdom.

**Kurs som inngår i CyberSmart**

Emnekode

IK6520 Grunnleggende cyber- og informasjonssikkerhet for lærere

IK6521 Anvendt cyber- og informasjonssikkerhet for lærere

Kurset CyberSmart, består av to kurs som hver gir 7,5 studiepoeng, totalt 15 studiepoeng.

**Målgruppe**

Lærere som har behov for kompetanse i digitale ferdigheter og innsikt i cyber- og informasjonssikkerhet for videregående opplæring i tråd med nye læreplaner. Studiet gir innsikt i grunnleggende begreper som digital sårbarhet og personvern, trusler og risiko og gir innsikt i aktuelle problemstillinger knyttet til internett og sosiale medier. Etisk hacking og passordbeskyttelse og innsikt i ulike krypteringsteknikker, samt programmering er noen av emnene i dette kurset.

**Undervisningsform**

Undervisningen er nettbasert, og det legges vekt på oppgaveløsning både individuelt og i grupper. Obligatoriske innleveringer av arbeidskrav underveis. Studiet er inndelt i 5 digitale moduler som baserer seg på pensum bestående av lærebok og nettbaserte ressurser.

I undervisningen vil vi bruke ulike digitale verktøy som Sphero, droner, samt ulike krypteringsteknikker. Prinsippet er fra enkel tegningsprogrammering til mer blokkbaserte programmeringsverktøy der innsikt i Python brukes som et programmeringsspråk. I høst-semesteret vil fokuset være at du selv lærer deg cyber- og informasjonssikkerhet og kunne ta i bruk ulike digitale verktøy, mens i vårsemesteret er fokuset å lære bort og lage leksjonsplaner med praktiske øvelser til elevene.

Hvordan søke opptak?

Du søker via Utdanningsdirektoratet (udir.no). Søknadsperioden er fra 1. februar til 1 mars.

Opptakskrav

Godkjent lærerutdanning og tilsetting i skolen i studieperioden.

Anbefalte forkunnskaper

I undervisningen forutsettes det grunnleggende ferdighet i bruk av datamaskin, men det forutsettes ingen forkunnskaper i cyber- og informasjonssikkerhet eller programmering. Deltakeren må selv disponere egen datamaskin.

**Studiets innhold**

Kurset CyberSmart, består av to kurs som hver gir 7,5 studiepoeng, totalt 15 studiepoeng.

Det første kurset, *IK6520 i Grunnleggende cyber- og informasjonssikkerhet for lærere*, består av 5 moduler, hhv på høst og vårsemesteret.

Emnene er inndelt i følgende moduler:

Modul 1: Personvern

Modul 2: Cybersikkerhet

Modul 3: Sosiale medier og internetthygiene

Modul 4: Digital sårbarhet

Modul 5: Hacking metoder og passord sikkerhet

Hver enhet består av forelesning, gruppeoppgaver, øvelser og erfaringsutveksling. Hele kurset tar 10 uker fra start til innlevering.

Emne ansvarlig /koordinator:

Nils Kalstad

Ansvarlig enhet

Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Det andre kurset, IK6521 *Anvendt cyber- og informasjonssikkerhet for lærere*, forutsetter at deltakerne allerede har noe grunnleggende kunnskap og ferdigheter i cybersikkerhet og programmering. Den fremtidige arbeidsstyrken trenger å vite hvordan de skal beskytte seg selv og sin organisasjon. CyberSmart bruker ulike teknikker for å hjelpe elevene til å bli mer bevisste, mer kreative, og problemløsere for å beskytte seg mot ulike cybertrusler de står overfor i en stadig mer teknologidrevet verden. CyberSmart bruker ulike krypterings- og dekrypteringsteknikker og etisk hacking for å engasjere og inspirere ungdom til å sikre seg i dag, og bidra til mer robusthet mot cyberkriminalitet i samfunnet for fremtiden.

I kurset IKS6521 *Anvendt cyber- og informasjonssikkerhet for lærere*, får deltakerne lære er rekke ulike krypterings og dekrypterings-teknikk, fra Cæsar til RSA ved å bruke Rasberry PII og får innsikt i programmeringsspråket Phyton. Dette studiet går mer i dybden innen styring av roboter, bruk av Raspberry PII, Micro:bit, Lego Mindstorm, krypering og kryperingsanalyse, og forklarer ulike hackingsmetoder for å fremme digital dømmekraft. Studiet skal demonstrere med praktiske eksempler evnen til refleksjon og vurdering av egen rolle for å unngå uønskede hendelser på nett og i sosiale medier.

**IKS6520 høst 2021**

Studiet er nettbasert og har ingen fysiske samlinger

Eksamen

Innlevering av obligatoriske arbeidskrav, vurderes til bestått/ikke bestått. Individuelle øvelser som alle må være godkjente, samt refleksjonsnotat om undervisningsmetode og egen læring i CyberSmart må være innlevert.

IK6521 vår 2022

Studiet er nettbasert og har ingen fysiske samlinger

Eksamen

Innlevering av prosjekt, vurderes til bestått/ikke bestått. Obligatoriske arbeidskrav og individuelle øvelser som alle må være godkjente.

**Hva lærer du?**

**Læringsutbytte i CyberSmart**

Modul 1: PERSONVERN

*I denne modulen, vil kursdeltakeren lære om personvern på nettet og hvordan de kan bruke en rekke sikkerhetsinitiativer når det gjelder beskyttelse og sikkerhet av persondata i klasserommet*.

*-på slutten av modulen vil elevene være i stand til å*

*Kunnskap*

* forklare de grunnleggende reglene og prinsippene for å beskytte personvern og personopplysninger
* forklare virkningen på personvernet i globale, lokale og trådløse nettverk
* forklare de underliggende teorier som er relevante for datanettverk og personvernadministrasjon
* forklare de grunnleggende juridiske personvernkonsepter og personvernforskrifter og personvernkonsekvens-utredning som er relevant for elever
* oppgi skolens- og læreansvaret når de samler inn og behandler personopplysninger
* forklare lærerens rolle med å beskytte elevdata
* kan identifisere de viktigste områdene som vil bidra til å veilede om digital personvernbevissthet
* definere begrepet "personvern", og relatere det til begrepet "digitalt fotavtrykk.
* beskrive nødvendigheten av en tverrfaglig tilnærming til cybersikkerhet og personvern i skolen
* diskutere EUs GDPR (General Data Protection Regulation) og hvordan det påvirker lærerens håndtering av elevdata

*Ferdigheter*

* lage leksjonsplaner for videregående opplæring i personvern
* gjøre rede for en rekke sikkerhetsinitiativer, for eksempel bevisstgjøring, strategier og regler som regulerer internett tilganger og bruk.
* gjøre rede for prinsippene for etisk tenkning omkring problemer knyttet til personvern, datamaskiner og digitale teknologier.
* lære elevene hvordan de kan identifisere personopplysninger og hvordan de kan sikre disse, samt rettighetene enkeltpersoner har angående sine personopplysninger.
* lære elevene hvorfor alt og alle som kobler seg til skolenettverket må overholde personvern og sikkerhetskrav
* kunne skille og lære forskjellen mellom personvern og datasikkerhet.

*Generell kompetanse*

* demonstrere kritisk tenkning om styrker og svakhetene ved personvernparadigmer som er relevante for lærere og elever.
* vurdere og reflektere med kolleger om hvordan GDPR, som er utformet for å sikre at integriteten til personopplysninger som samles inn, administreres, lagres eller behandles, er fullt beskyttet.
* engasjere seg i kritisk selvrefleksjon over relevante etiske og faglige personvernspørsmål, som en del av den livslange læringsstrategien som kreves av en cybersikkerhets-profesjonell i skolen.
* diskutere kritisk og evaluere nåværende prosesser og forstyrrende teknologier innen cybersikkerhet og personvern med elever og kolleger.
* reflektere med kolleger om ansvarsoppgavene skolene har når de deler data internt, eksternt og på tvers av landegrenser
* reflektere med kolleger om viktigheten av å undervise alle elever og ansatte om personvern og sikkerhet, eksternt og over lande-grensene.
* gjøre rede for de viktigste komponentene som kreves for å etablere et trygt og sunt digitalt miljø i klasserommet.

MODUL 2: CYBERSIKKERHET

*I denne modulen, vil kursdeltakeren lære om de grunnleggende prinsippene for cyber- og informasjonssikkerhet og hvordan de skal reagere på digitale trusler og lære elevene å bli cybersmarte*

*-på slutten av modulen vil elevene være i stand til å*

*Kunnskap*

* forklare de grunnleggende prinsippene og beste fremgangsmåtene for å svare på cybersikkerhetshendelser.
* forklare enkel angrepsmetodikk og mistenkelige forsøk på tilkobling for å få uautorisert tilgang til en datamaskin og dets ressurser.
* beskrive cyberforsvar og angrepsteknikker, teknologier og verktøy for å forklare passende løsninger for å forberede seg på, forsvare seg mot cyber inntrenging.
* kan analysere et problem, identifisere og definere sikkerhetsrisikoer og krav som passer til løsningen.
* diskutere den menneskelige rollen i sikkerhetssystemer med vekt på etikk, sårbarheter med sosial manipulering og trening.
* forklare prinsippene rundt web-sikkerhet.
* forklare cybersikkerhets-teknikker for å beskytte datamaskinen når du bruker Internett-søk, e-post og sosiale nettverksnettsteder.
* forklare betydningen av informasjons- og kommunikasjons-teknologier og hvordan de endrer det moderne samfunn.

*Ferdigheter*

* demonstrere evnen til å løse enkle problemer innen cyber- og informasjonssikkerhet ved å foreslå løsninger.
* demonstrere evne til å uttrykke kritiske holdninger til begrensninger av manglende kunnskap innen cyber- og informasjonssikkerhet
* definere og bruke førstelinje cyber forsvar - og lære elevene hvordan de skal reagere på trusler som oppstår over Internett
* analysere gjeldende prosedyrer og standarder for håndtering av cyberrisikoer og trusler, foretar penetrasjonstesting og sikrer nettverkssikkerhet med elever.
* lære ulike typer av cyberangrep, og hvordan disse kan beskyttes mot eller reduseres.
* lære elever om ulike typer skadelig programvare som en angrepsvektor som i de fleste tilfeller avhenger av sårbarheter, av brukeren og hvordan de fungerer.
* lære om forskjellene mellom virus og skadelig programvare, og diskutere deres innvirkning på personvern og datadrift .
* kan lære om både positive og negative konsekvenser av digitalisering av samfunnet.
* planlegge og gjennomføre en cybersikkerhetsuke i grunnleggende cybersikkerhet i samarbeid med elever og kolleger.
* beskrive typiske trusler mot moderne digitale systemer, og skissere teknikker for motstand mot dem
* kan demonstrere evne til å arbeide effektivt i team, samarbeide med andre innen cyber- og informasjonssikkerhet og ta initiativ til å løse enkle cybersikkerhetsproblemer.
* utvide sitt kunnskapsfelt innenfor cybersikkerhet som er relevant i skolen.
* forklare og diskutere betydningen av begreper som beskriver vanlige cyberangrep, for eksempel phishing, pharming, skuldersurfing og blagging.
* beskrive cyber sikkerhetsteknikker med elever for å beskytte personlig informasjon når de bruker Internett-søk, e-post, chatterom, og sosiale nettverk nettsteder.
* utføre en antivirusskanning på et datasystem for å se etter virus og skadelig programvare.
* reflektere med kolleger om cybertrusler som er relevante i skolen.

*Generell kompetanse*

* planlegge og gjennomføre en cybersikkerhetsuke i grunnleggende cybersikkerhet i samarbeid med elever og kolleger.
* beskrive typiske trusler mot moderne digitale systemer, og skissere teknikker for motstand mot dem.
* kan demonstrere evne til å arbeide effektivt i team, samarbeide med andre innen cyber- og informasjonssikkerhet og ta initiativ til å løse enkle cybersikkerhetsproblemer.
* utvide sitt kunnskapsfelt innenfor cybersikkerhet som er relevant i skolen.
* forklare og diskutere betydningen av begreper som beskriver vanlige cyberangrep, for eksempel phishing, pharming, skuldersurfing og blagging.
* beskrive cyber- og informasjonssikkerhetsteknikker med elever for å beskytte personlig informasjon når de bruker Internett-søk, e-post, chatterom, sosiale nettverk og nettsteder.
* utføre en antivirusskanning på et datasystem for å se etter virus og skadelig programvare.
* reflektere med kolleger om cybertrusler som er relevante i skolen.

*MODUL 3: SOSIALE MEDIER OG INTERNETTHYGIENE*

*I denne modulen, vil kursdeltakeren lære om faglige, etiske, juridiske, sikkerhetsmessige spørsmål og ansvar knyttet til sosiale medier og nettmobbing.*

*-på slutten av modulen vil elevene være i stand til å*

Kunnskap

diskutere virkningen av digitalisering på individ – organisasjon og samfunn.

diskutere de juridiske og etiske problemstillinger og ansvar knyttet til sosiale medier og innvirkningen på elever

oppsummere og bevisstgjøring om ledelse, økonomiske, juridiske, sosiale, profesjonelle og etiske spørsmål knyttet til bruk av sosiale medier.

forklare hvordan du administrerer og sikrer personlige digitale fotavtrykk

gjenkjenne hvordan du kan hjelpe elever med å håndtere sikkerhetsrisikoer på sosiale medier

diskutere relevant lovgivning og etisk retningslinjer for elever i sikkerhetshåndtering.

gjenkjenne hvordan ulike sosiale medieplattformer målrettet kan brukes av organisasjoner mot ulikt publikum.

forutsi risiko forbundet med nettspill, og identifisere måter å redusere disse risikoene på.

*Ferdigheter*

* undervise elever om faglige, etiske, juridiske, sikkerhetsmessige og sosiale spørsmål og ansvar knyttet til sosiale medier.
* dele beste praksis i bruk av sosiale medier og formidle videre til sine elever.
* organisere og lage undervisnings opplegg for internetthygiene og bruk av sosiale medier.
* lære elevene hvordan de skal fremme et positivt "digitalt selvbilde", inkludert å snakke med elevene om nettinnhold og aktiviteter.
* forklare de ulike typer nettbasert risiko og tegn på nettmobbing, for å forebygge og gi et passende tilsvar på slike hendelser.
* hjelpe elevene med å forebygge uønsket hendelse på sosiale medier og lære dem hvordan de skal reagere på slike hendelser.
* undervise elevene om risiko forbundet med sexting (inkludert juridiske spørsmål og sosiale konsekvenser), og diskutere metoder for respons, rapportering og forebygging.

*Grunnleggende kompetanse*

* analysere og diskutere juridiske og etiske aspekter ved bruk av sosiale medier med kolleger.
* gi et kritisk og reflektert syn på cybersikkerhet i forskjellige læreplaner
* utveksle meninger, erfaringer og ideer med kolleger om sosiale medier og risiko.
* diskutere eksempler på nettmobbing for å hjelpe elever til å forstå viktigheten av å håndtere denne og grensen for det som kan aksepteres.
* diskutere med kolleger om risiko på nettet, som nettmobbing, upassende meldinger, seksuell trakassering, upassende nettsteder og radikalisering på nettet, deling (strømming) på nettet og upassende bruk av sosiale nettverk.
* reflektere med kolleger om det grunnleggende med tilstedeværelse på sosiale medier for personlige formål og foreslå måter å redusere disse risikoene.
* vurdere nettmobbing, dens innvirkning på gjerningsmenn og ofre, og foreslå måter å svare dette på.

*MODUL 4: DIGITAL SÅRBARHET*

*I denne modulen, vil kursdeltakeren lære om de vanligste digitale sikkerhetsutfordringene og sårbarhetene i IKT-systemer, samt metoder for å lindre disse problemene.*

*-på slutten av modulen vil elevene være i stand til å*

Kunnskap

* diskutere hva digital sårbarhet er og hvordan de kan hjelpe elevene til å bli mer robuste mot angrep.
* vise en praktisk forståelse av de vanligste sikkerhetsutfordringene og sårbarhetene i IKT-systemer, samt metoder for å lindre disse problemene.
* diskutere cyberkriminalitet og trusler, sårbarheter og forsvarsmetoder og verktøy.
* oppsummere ulike digitale verktøy, teknikker og praksiser som understøtter sikker IKT-bruk.
* forklare det teoretiske grunnlaget for sikkerhetstesting og sårbarhetsvurdering.
* beskrive sårbarhet til ulike angrep på elevene sine enheter og hvordan de kan forhindres.
* beskrive ulike verktøyene som beskytter data og nettsteder. Disse inkluderer sterke passord, biometri, tofaktorautentisering og brannmurer.
* diskutere de mulige sikkerhetsrisikoene og ulempene for elever som deltar i ulike online aktiviteter.

*Ferdigheter*

* skissere trusler og bestemme risiko, og komme med anbefalinger til elevene.
* reflektere over sin egen akademiske praksis og utvikling som sikkerhetsprofesjonell, og identifisere områder i læreplanen der temaet passer inn, og kan tilpasse undervisningen til fremtidige cybersikkerhetsverktøy, teknikker, teknologi og trusler.
* finne, tilpasse, bruke og evaluere relevante akademiske cyber sikkerhetsleksjonsplaner og spill som finnes gjennom nettbasert søk og inkorporer disse i undervisningen.
* utføre sårbarhetsvurdering med elever og kolleger.
* forklare hvordan "anti-virus" programvare fungerer og hjelpe elevene med å installere disse på datamaskinen.
* forklare betydningen av begreper som beskriver vanlige cyberangrep, for eksempel phishing, pharming, skuldersurfing og blagging
* forklare elevene hvordan databehandlingsressurser kan misbrukes på grunn av deres ulike nettaktiviteter og hvordan de kan minimere risikoen.

*Grunnleggende kompetanse*

* å identifisere og diskutere med elever og kolleger ulike tilnærminger til sikkerhetssikring for bruk i undervisning.
* anerkjenne behovet for- og en evne til å engasjere seg i kontinuerlig faglig utvikling i undervisnings-praksis innen cybersikkerhet.
* identifisere og hensiktsmessig handle på komplekse etiske og sosiale spørsmål som oppstår innen akademisk og profesjonell praksis som en cyber sikkerhetsprofesjonell, samtidig som de er klar over de større implikasjonene av sine handlinger og beslutninger.
* utforske, undervise og diskutere/reflektere over sårbarheter i informasjonssikkerhet, som refererer til en feil i et system som kan være åpent for angrep.
* utvide og bygge egen kunnskap om de ulike verktøyene som beskytter data og nettsteder.
* anbefale og diskutere med kolleger hvordan personopplysninger kan være sårbare for angrep og hvordan å sikre dem.
* oppsummere hvordan databehandling og informasjonsressurser kan være sårbare for angrep og hvordan dette påvirker undervisningen av cybersikkerhet i skolen.

*MODUL 5: HACKING METODER OG PASSORDSIKKERHET*

*I denne modulen, vil kursdeltakeren lære om det grunnleggende i moderne kryptografi, etisk hacking og anvendt passordsikkerhet.*

*-på slutten av modulen vil elevene være i stand til å*

Kunnskap

* Forklare grunnlaget for moderne kryptografi.
* forklare datamaskinen, nettverksikkerhet, mekanismer og protokoller.
* diskutere vanskeligheter og sikkerhetsproblemer som elever og lærere står overfor på daglig basis.
* skissere de juridiske aspektene ved å utføre etisk hacking for å reflektere hva som er innenfor og utenfor tillatte aktiviteter.
* Beskrive noen teknikker for hemmelig skriving, spesielt kode og chiffersystemer, metoder samt prosedyrer, prosesser, metoder for å lage og bruke hemmelig skriving, som koder eller chiffer.
* diskutere viktige ting som elever og lærere kan gjøre for å sikre at datamaskinen er beskyttet mot virus og hackere og sørge for at de ikke blir utsatt for noen form for sikkerhetsrisiko.

*Ferdigheter*

* identifisere, beskrive og diskutere med elever fordelene og ulempene ved ulike krypteringsteknologier.
* illustrere sikkerhetsaspekter som er relevante for elever, og foreslå konkrete løsninger på spørsmål i klasserommet.
* identifisere sikkerhetsoppgaver som bør håndteres av eksperter og kan lære elevene om hvordan de skal lete etter dem og hvor de skal henvise problemene videre.
* utføre en analyse av cybersikkerhetsangrep, motivasjon for angrep og risiko. Er i stand til å lære elevene hvordan de kan beskytte seg selv mot angrep.
* lage leksjonsplaner og gjennomføre økter med enkle øvelser for elever innen hemmelig skriving, spesielt kode- og chiffersystemer.
* Beskrive og undervise elevene hva som definerer et sterkt passord og hjelpe elevene å velge sterke passord.

*Grunnleggende kompetanse*

* utveksle meninger med kolleger og delta i diskusjoner om utvikling av god praksis hvordan man velger og ivaretar passord.
* planlegge, utføre og administrere en rekke aktiviteter og cybersikkerhetsrelaterte prosjekter, alene eller som en del av et team, til et vellykket resultat og i samsvar med relevante juridiske og etiske krav og prinsipper.
* vise til og reflektere med kolleger om de faglige og etiske spørsmålene som er relevante for feltet cybersikkerhet og nettverk som er relevante for elevene.
* diskutere grunnlag for nettverks- og kommunikasjonssikkerhet som er relevant for elever og hvordan man beskytter seg mot angrep.
* bruke ulike verktøy og teknikker for å sikre og beskytte elevene med sine internetterfaringer.
* reflektere og undervise hvordan angripere får uautorisert tilgang til systemer og data.