

CyberSmart

.....

– et pilotprosjekt for opplæring av ungdom i cybersikkerhet
Janne Hagen og Bodil Grødem (Godalen videregående skole)



Rapport, bokmål nr 35-2019

CyberSmart

Utgitt av: Norges vassdrags- og energidirektorat
Redaktør: Janne Hagen
Forfatter: Janne Hagen og Bodil Grødem (Godalen videregående skole)

Trykk: NVEs hustrykkeri
Forsidefoto: Bodil Ellen Grødem, Godalen videregående skole
ISBN: 978-82-410-1922-7
ISSN: 1501-2832

Sammendrag: Rapporten oppsummerer erfaringene fra det norske CyberSmart-prosjektet, som har pågått i perioden november 2017 til august 2019. Flere aktører har gått sammen om å utvikle og teste et opplæringsopplegg for lærere og elever i den norske ungdomsskolen og videregående skole. CyberSmart bygger på kunnskap fra det amerikanske opplæringsprogrammet i cybersikkerhet, «GenCyber».

Emneord: Cybersikkerhet

Norges vassdrags- og energidirektorat
Middelthunsgate 29
Postboks 5091 Majorstua
0301 OSLO

Telefon: 22 95 95 95
Epost: nve@nve.no
Internett: www.nve.no

August, 2019

Innhold

Forord	4
Sammendrag	5
1 Innledning	6
1.1 Bakgrunn	6
1.2 Formål	6
2 Prosjektorganisasjon	7
3 Forankring og utvikling av lærerkurs og elevseminar	7
3.1 Forankring og finansiering.....	7
3.2 Faglig utvikling av lærerkurs og elevseminar.....	9
4 Lærerkurs i cybersikkerhet.....	10
4.1 Ukeskurs for lærere	10
4.2 Firedagers kurs for lærere med undervisning fra USA	10
5 Elevseminar og sommerskole	11
5.1 Ukeskurs for ungdomsskolen 10. klasse	11
5.2 Ukeskurs på yrkesfag VG1	11
5.3 Ukeskurs på yrkesfag VG2	12
5.4 Sommerskole for ungdomstrinnet	13
6 Evaluering	14
6.1 Forankring og finansiering.....	14
6.2 Gjennomføring av lærerkurs	14
6.3 Gjennomføring av elevseminar og sommerskole	16
7 Fra pilot til nasjonalt tilbud.....	19
7.1 Behov for å lære ungdom om cybersikkerhet.....	19
7.2 Etablering av nasjonalt tilbud	20
7.3 Fagplan i cybersikkerhet.....	22
8 Konklusjon	23
Vedlegg A – Eksempel timeplaner.....	24
Vedlegg B – Deltakere	30
Referanser	31

Forord

Norsk senter for informasjonssikring (Norsis) har konkludert med at store grupper i samfunnet mangler kompetanse og forståelse for IKT-sikkerhet. Det er i hovedsak ansatte i bedrifter og virksomheter som får opplæring; De yngre, de eldre og de uten arbeid stiller svakere i et digitalt samfunn (Norsis, 2017). Norsis råder utdanningsmyndighetene til å ta et større ansvar for at norske ungdommer blir trygge digitale innbyggere, og sørge for å utvikle mer kunnskap om ungdom og digital sikkerhetskultur (Malmedal & Røislien, 2017).

Det gjøres tiltak nasjonalt for å heve kompetansen: Kunnskapsdepartementets strategi «Framtid, fornyelse og digitalisering» omtaler informasjonssikkerhet og personvern i flere runder. Rapporten framhever *at elevene skal tilegne seg gode digitale ferdigheter og dømmekraft og lære å utnytte digitale læremidler kreativt og skapende* (Kunnskapsdepartementet, 2017). Utdanningsdirektoratets rammeverk for grunnleggende digitale ferdigheter (Utdanningsdirektoratet, 2017) omtaler også informasjons- og datasikkerhet som ett ferdighetsområde.

Å utdanne ungdom i cybersikkerhet er viktig. De er framtidens arbeidskraft og vil bekle viktige stillinger i kritisk infrastruktur, i privat sektor og i forvaltningen. Med økt digitalisering av samfunnet blir kompetanse og ferdigheter innen cybersikkerhet enda viktigere.

Cybersmart er et initiativ fra NVE og NTNU som har vokst og inkludert flere aktører. I CyberSmart-prosjektet, som har pågått i perioden november 2017 til august 2019, har flere aktører gått sammen om å utvikle og teste et opplæringsopplegg for lærere og elever i den norske ungdomsskolen og videregående skole. CyberSmart bygger på kunnskap fra det amerikanske opplæringsprogrammet i cybersikkerhet, «GenCyber». Mange har bidratt fra myndigheter, akademia, privat sektor og Forsvaret. CyberSmart har også fått finansiell støtte fra flere norske samarbeidspartnere, samt fra Oslo Grant ved den amerikanske ambassaden i Oslo. I løpet av prosjektperioden ble prosjektet også inkludert i nasjonal strategi for digital sikkerhetskompetanse.

Denne rapporten avslutter pilotprosjektet. Erfaringene fra prosjektet viser at temaet og opplegget er interessant og engasjerer. Totalt har ca. 300 elever i Akershus og Rogaland vært på kurs og over 80 lærere har fått et innblikk i temaet, av disse har 14 deltatt på ukeskurs i regi av prosjektet. I rapporten evaluerer vi prosjektet og oppsummerer læring og råd for en eventuell nasjonal etablering.

Oslo, 25. august 2019



Ingunn Asgard Bendiksen

Direktør

Sammendrag

I CyberSmart har lærere og elever ved ungdomsskolen og videregående skole fått trening og opplæring i cybersikkerhet. Prosjektet har hentet inspirasjon fra GenCyber-opplæringsprogrammet i USA som National Science Foundation (NSF) og National Security Agency (NSA) finansierer. Fagplanen har dekket digital sårbarhet, både personlig og for samfunnet, passord, kryptering, programmering, nettvett og deling av informasjon og sikkerhet i sosiale medier. Prosjektet har blitt godt mottatt av både elever og lærere. Totalt har ca. 300 elever gjennomgått opplæring i cybersikkerhet. 14 lærere har deltatt på kurs med varighet inntil to uker og 70 lærere i Ski fikk gjennom egenutviklet intensivkurs i 2018 på 1,5 time høre og lære om cybersikkerhet. Kurset ble gitt av en av lærerne som deltok på lærerkurset samme år.

Prosjektet har gjennomført to lærerkurs, del 1 i 2018, og del 2 i 2019. I del 1 underviste Nasjonal sikkerhetsmyndighet (NSM), Norges vassdrags- og energidirektorat (NVE), Norsk senter for informasjonssikkerhet (Norsis), Norges teknisk naturvitenskaplige universitet (NTNU)/Cyberingeniørskolen (CIS) og Universitetet i Oslo (UiO). I kursets del 2 underviste inviterte eksperter fra Universitetet i Tulsa, USA.

Faglig sett leverer prosjektet godt og bidrar til å heve kompetanse og forståelse om cybersikkerhet. Modellen med å undervise lærere først, slik at de kan undervise elevene, er god. Erfaringene fra lærerkursets del 2 med eksperter fra Universitetet i Tulsa, viser at lærerne som deltok evner å lære kryptering, programmering og cybersikkerhet. Lærerne hadde ulike fagbakgrunn i samfunnsfag, salg, service, sikkerhet, IKT og engelsk.

Prosjektet har kjørt seminar med en ukes varighet for elever i skoletiden ved Ski Ungdomsskole, Godalen videregående skole og Haugaland videregående skole. I tillegg kjørte Ski og Flåtestad ungdomsskole et sommerkurs for elever i den nye Nordre Follo kommune, sommeren 2019.

Erfaringene viser at cybersikkerhet er tverrfaglig og kan inkluderes inn i mange skolefag, inklusive yrkesfag. Prosjektet har vist seg å være egnet til å kjøre på den enkelte skole. Forankring og støtte fra skoleledelsen er viktig. Videre er det gode erfaringer med å bruke lokale eksterne forelesere fra for eksempel myndigheter og privat næringsliv. Det skaper engasjement. Erfaringene fra sommerskolen viser at det er vanskelig å rekruttere jentene og at det trengs ekstra innsats her.

Rapporten skisserer til slutt ulike modeller for å videreføre cybersikkerhetsopplæring av ungdom, avhengig av finansiering. Det anbefales at NTNU/Realfagsenteret i Trondheim gis støtte til å videreutvikle prosjektet til et nasjonalt prosjekt.

1 Innledning

1.1 Bakgrunn

Norge digitaliseres. Samfunnet blir mer avhengig av at de digitale systemene fungerer. Samtidig opplever vi at datatyveri, etterretning og alvorlig cyberangrep får betydelige konsekvenser for både privatpersoner og virksomheter. Slike angrep treffer også kritisk infrastruktur i samfunnet, slik som energisektoren. Cyberangrepet mot Ukraina i 2015 og senere krypteringsskadevaren som rammet Hydro i 2019, er eksempler på det. Alle samfunnssektorer henter arbeidskraft fra den samme befolkningen. Det også er en viss mobilitet i arbeidsstyrken mellom ulike sektorer. I et digitalisert samfunn bør derfor alle ha en viss grunnkompetanse i IKT-sikkerhet og ha god digital dømmekraft. Dette temaet har også opptatt Norsis som har studert og dokumentert norsk sikkerhetskultur (Norsis, 2017).

I 2017 pågikk det en offentlig debatt om mangelen på kvalifiserte sikkerhetsekspert. I energisektoren dreide mye av diskusjonen seg om digitalisering og effektivisering. Samme år utga NVE en rapport om informasjonssikkerhetstilstanden i energiforsyningen. Rapporten viste at 1 av 2 virksomheter hadde blitt utsatt for internettbedrageri, og 40% hadde erfart datavirus i sine IT-systemer (NVE og NSM, 2017). Rapporten viste at bransjen trengte et kompetanseløft.

Senhøsten 2017 tok derfor NVE sammen med NTNU CCIS initiativ til å sette i gang et opplæringsprosjekt innen cybersikkerhet – senere gitt navnet CyberSmart. Prosjektet var rettet mot opplæring i cybersikkerhet for framtidens arbeidskraft, ungdommen. Prosjektet skulle være en pilot for å teste ut et opplæringsprogram for lærere og elever på ungdomstrinnet og i videregående skole. Inspirasjonen kom på et arbeidsseminar hos NVE høsten 2017 der temaet var blant annet det amerikanske opplæringsprogrammet for barn og ungdom i cybersikkerhet – GenCyber. Bak GenCyber står National Science Foundation (NSF) og National Security Agency (NSA) i USA. Programmet tilbyr opplæring av lærere i cybersikkerhet og sommerskoler for barn og ungdom. I USA har dette programmet blitt en stor suksess som dekker flere stater. Det har i tillegg klart å mobilisere jentene, noe som generelt har vært en utfordring innen informatikkfaget.

CyberSmart fikk raskt drahjelp på en telefonkonferanse november 2017 der amerikanske professorer og eksperter på GenCyber og initiativtakerne hos NVE og NTNU deltok. NVE og NTNU samarbeidet etterpå om å skissere innhold i et pilotprosjekt, identifisere mulige samarbeidspartnere og lage et opplegg for finansiering.

1.2 Formål

Formålet med prosjektet var å utvikle en pilot for å teste et opplæringskonsept i cybersikkerhet for lærere og elever etter modell av amerikanske GenCyber. Ettersom piloten ble gjennomført samtidig som det ble foretatt en revisjon av læreplaner i skolen, ble det også et delmål i prosjektet å gi innspill til læreplaner i skolen på digital sikkerhet.

2 Prosjektorganisasjon

Kort tid etter at NVE og NTNU bestemte at det skulle lages en pilot, og det ble klart at NVE ville bidra med finansiering, ble det rekruttert en prosjektleder.

Styringsgruppen ble etablert i april 2018. Nasjonal sikkerhetsmyndighet (NSM) påtok seg styreledervervet. Styringsgruppens øvrige deltakere var NVE, NTNU, CIS, UiO, Norsis og Abelia. Styringsgruppen holdt totalt 6 møter.¹ NVE tok sekretærrollen og bidro med rapportskriving underveis.

Flere fagressurser ble også med på frivillig basis. Alle samarbeidspartnerne stilte med menneskelige ressurser og fagkompetanse. NVE, NSM og Rogaland fylkeskommune, Justis- og beredskapsdepartementet og Oslo Grant ved den amerikanske ambassaden bidro med finansiering (Hagen, 2019).

Denne rapporten avslutter pilotprosjektet.

3 Forankring og utvikling av lærerkurs og elevseminar

3.1 Forankring og finansiering

Prosjektleder og prosjektets samarbeidspartnere har jobbet aktivt med å forankre prosjektet. Figur 3.1 viser en forenklet skisse av forankringsarbeidet som er gjennomført.



Figur 3.1 Forankring og finansiering.

¹ 9. april, 2. mai, 29. august og 17. oktober 2018. I 2019 ble det holdt styringsgruppemøter 4. april og 7. juni.

Prosjektlederen har hatt kontakt med rektorer for å sikre forankring mot skolens ledelse, noe som er viktig for å lykkes med den praktiske gjennomføringen av elevkursene.

Prosjektlederen har også hatt møter med Stavanger kommune og Rogaland fylkeskommune, både med skoleadministrativt personell og politikere. Ordførerne i Ski og Oppegård besøkte sommerskolen i Ski 2019.

Prosjektet har hatt kontakt med Utdanningsdepartementet, Utdanningsdirektoratet, Olje- og energidepartementet og Justisdepartementet, Datatilsynet, private teknologiselskaper, IKT-Norge, Tekna, samt den amerikanske ambassaden for å informere og for å skaffe samarbeidspartnere og finansiering. RealFagssenteret ved NTNU og UiOs Center for Computing in Science Education ble også kontaktet, og viste positiv interesse for prosjektet.

Informasjon om Cybersmart er også formidlet på ulike mediekkanaler: NVEs (NVE, 2018), NSMs (Thon, 2018) (NSM, 2019) og Godalens nettsider (Godalen videregående skole, 2019). Prosjektet er presentert i et innlegg i Stavanger Aftenblad (Stavanger Aftenblad), Computerworld og på digi.no (Hagen & Grødem, 2019). Elevkurset i Stavanger ble presentert på TV Vest (TV-Vest, 2018). I tillegg har NTNU blitt vertskap for CyberSmart sin nettside (NTNU, 2018). Prosjektet ble også presentert på Rogalandskonferansen (Grødem & Dale, 2019) og i debatt på Sikkerhetsfestivalen på Gjøvik 2019 (Sikkerhetsfestivalen, 2019).

Forankringsarbeidet og prosjektresultatene har ført til at prosjektet CyberSmart ble en del av nasjonal strategi for digital sikkerhetskompetanse (Justis- og beredskapsdepartementet og Kunnskapsdepartementet, 2019).

RealFagssenteret ved NTNU er positive til å overta prosjektet, og UiOs Center for Computing in Science Education sammen med UiO /Ifis forskningsgruppe på cybersikkerhet ser også muligheter for å tilby lærerkurs i cybersikkerhet som en del av lærernes etterutdanning i koding.

Prosjektet er finansiert av NVE, NSM, Justis- og beredskapsdepartementet, Rogaland fylkeskommune og Oslo Grant. Finansiell støtte er vist i Tabell 3.1. I tillegg til dette er det lagt ned et betydelig arbeid i form av arbeidstimer fra samtlige partnere i prosjektet. Partnerne har bidratt med egeninnsats og utarbeidet undervisningsopplegg, samt stilt opp med fagressurser og undervisning. Denne innsatsen er ikke tallfestet.

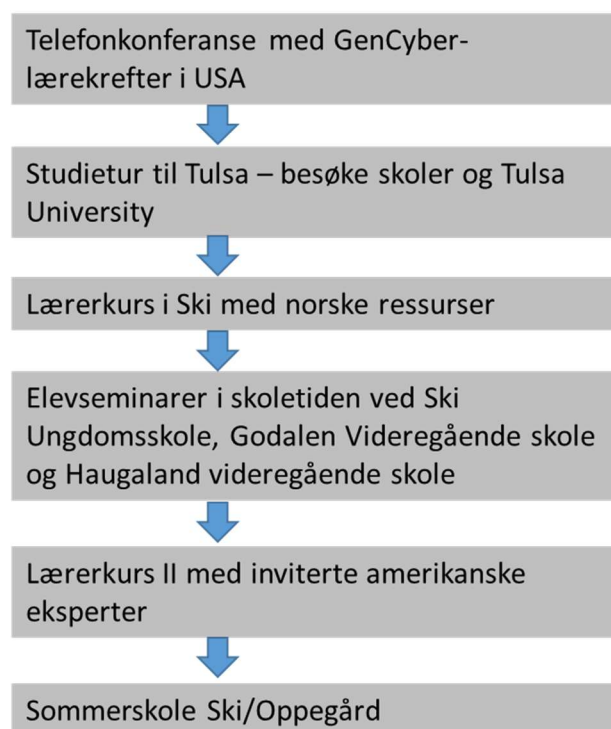
Tabell 3.1 Oversikt over økonomisk støtte

Aktør	Bevilgning i tusen kr
NSM 2018 og 2019	400
NVE 2018 og 2019	300
Justis- og beredskapsdepartementet 2018	400
Rogaland fylkeskommune 2018	250
OsloGrant	70
Sum	1420

De økonomiske midlene har vært brukt til å dekke frikjøp av prosjektleder og reiseutgifter samt lærerkurs og kompensasjon av vikarutgifter for lærere som deltar på kurs. Et mindre beløp har vært brukt til å kjøpe inn utstyr som Raspberry Pi² og droner (Sphero). Støtten fra Oslo Grant gikk til å dekke reise og opphold for amerikansk undervisningspersonell fra Universitetet i Tulsa, som ble invitert til Norge.

3.2 Faglig utvikling av lærerkurs og elevseminar

CyberSmart har gjennomført to lærerkurs og tre elevseminar samt sommerskole i cybersikkerhet. En forenklet skisse av prosessen er vist i Figur 3.2.



Figur 3.2 Kursutvikling for lærere og elever.

Prosessen var som følger:

Med utgangspunkt i dialogen med amerikanske eksperter på GenCyber ble det laget utkast til et norsk lærerkurs, med faglige bidrag fra ulike partnere som NSM, NVE, Norsis, CIS, NTNU og UiO.

CyberSmart-prosjektet ble invitert til Universitetet i Tulsa for å lære mer. En norsk delegasjon med fire lærere fra Godalen videregående skole, Ski ungdomsskole og NVE reiste til Tulsa i mars 2018. I Tulsa fikk den norske gruppen lære mer om GenCyber og diskutert et første utkast til plan for et norsk lærerkurs i Oslo. I tillegg fikk gruppen observert hvordan lærere i Owasso i Oklahoma underviste 6. klasse elever i cybersikkerhet.

² Datamaskin som er tilrettelagt for læring.

Deretter utarbeidet en arbeidsgruppe bestående av samarbeidspartnere og lærere et revidert opplegg for lærerkurs som ble kjørt i mai 2018 hos UiO.

Så fulgte tre elevseminarer, lærerkurs del II og til sist sommerskole i cybersikkerhet. Hvert seminar og kurs bygget videre på lærdom fra gjennomførte seminar og kurs.

4 Lærerkurs i cybersikkerhet

4.1 Ukeskurs for lærere

CyberSmart gjennomførte første lærerkurs i cybersikkerhet 28.5.2018 til 1.6 2018 med bidrag fra NVE, NSM, UIO, NTNU CCIS, Cyberingeniørskolen CIS og Norsis. På det første lærerkurset deltok totalt 12 lærere over fem dager, derav to lærere fra Ski ungdomsskole, en lærer fra Oppegård kommune, to lærere fra Haugaland videregående skole, og seks lærere fra Godalen videregående skole i Rogaland. Rektor fra Godalen videregående skole deltok en dag som observatør. Det var bestemt at piloten ikke skulle ha større omfang enn at prosjektgruppen klarte å håndtere den praktiske gjennomføringen på en god måte. Tilgang til klasserom og teknisk utstyr (lab) begrenset antall deltakere.

Kurset ble holdt på UiO. I løpet av de fem dagene kurset pågikk, fikk lærerne undervisning i cybersikkerhet. Deler av dagen ble brukt på å utvikle et eget undervisningsopplegg som i etterkant skulle gjennomføres og testes ut på egen skole.

I forkant av kurset fikk lærerne tilsendt motivasjonsbrev på epost med ulike oppgaver. Disse presenterte cybersikkerhet som fagtema og refererte til aktuelle nyhetsoppslag.

Målgruppen for kurset var ikke lærere med høy teknisk ekspertise, men lærere med annen fagbakgrunn, uten forkunnskaper om cybersikkerhet. Blant deltakerne var lærere som underviste i service, samferdsel og sikkerhet, i engelsk, samfunnsfag, programmering og i IKT-drift. De kom fra videregående skoler i Rogaland og ungdomsskoler i Akershus.

4.2 Firedagers kurs for lærere med undervisning fra USA

CyberSmart gjennomførte et nytt lærerkurs for 14 lærere 18.-21. februar 2019. Her deltok de samme lærerne som deltok på første kurset, men med utvidelse til Vågen videregående skole og Flåtestad ungdomsskole.

Med økonomisk støtte fra Oslo Grant ved den amerikanske ambassaden i Oslo, ble undervisningspersonell fra Universitet i Tulsa invitert til Norge for å undervise norske lærere. Det norske lærerkurset ble holdt ved Universitetet i Oslo (UiO). Instructor in mathematics Kimberly Adams og Visiting Associate Professor Donna Farrior fra University of Tulsa har undervist amerikanske lærere i cybersikkerhet etter den amerikanske modellen GenCyber i flere år. De underviste nå norske lærere. I løpet av disse fire dagene, lærte lærerne en rekke ulike krypterings- og kryptoanalyseteknikker fra

Caesar-siffer til RSA³ ved å bruke blant annet Raspberry Pi⁴ og programmeringsspråket Python⁵.

5 Elevseminar og sommerskole

5.1 Ukeskurs for ungdomsskolen 10. klasse

I juni 2018 ble det gjennomført en ukes kurs i Cybersikkerhet for 10. klasse elever ved Ski ungdomsskole. Lærere fra Ski ungdomsskole og fra Godalen videregående skole underviste og testet ut ulike temaer innen cybersikkerhet, som koding, kryptering, biometri og sikre passord. Klassen hadde undervisning en dag ved UiO. Der fikk de en gjennomgang av etisk hacking og fikk også testet ut hvordan de overvåker og endrer trafikk i nettleseren (tampertools). I tillegg fikk Ski ungdomsskole besøk en hel dag av professor Sujeet Shenoï fra University of Tulsa. Han underviste elevene i cybersikkerhet, og dekket blant annet Stuxnet, som er kjent som det første cyberfysiske våpenet. Stuxnet er dataviruset som ødela sentrifugene i atomanlegget i Natanz, Iran i 2010 (Kushner, 2013) .

5.2 Ukeskurs på yrkesfag VG1

Ved Godalen videregående skole var CyberSmart godt forankret i skolens ledelse med støtte underveis fra ledergruppen. I tillegg ble en egen arbeidsgruppe etablert ved skolen.

I september 2018 ble det gjennomført en ukes elevkurs i CyberSmart i Stavanger for 120 elever på yrkesfaglig studieretning. Lærerne ved Godalen videregående skole tok med seg erfaringene fra lærerkurset i mai og den praktiske gjennomføringen i Ski inn i egen undervisning.

Faginnholdet for elever på VG1, Service og samferdsel ved Godalen videregående skole ble utarbeidet på bakgrunn av kunnskapen og erfaringene fra lærerkurset ved UiO. Ved Godalen videregående skole ble det gjennomført et undervisningsopplegg der både NSM, NVE, Norsis, UiO og Politiet deltok med foredrag gjennom hele uke 37. I tillegg kjørte lærerne et praktisk undervisningsopplegg med droneprogrammering, kryptering og scenariotrening, inspirert av GenCyber og den amerikanske opplæringsmodellen. Skolens IT-gruppe ble engasjert. Arbeidsgruppen ved skolen bidro aktivt med både tekniske løsninger og hjelp under ulike aktiviteter hele cyberuken. Elevene fikk etter gjennomført kurs et sertifikat Figur 5.1

³ Krypteringsalgoritme utviklet av Ron Rivest, Adi Shamir og Leonard Adleman ved MIT, 1977.

⁴ Raspberry Pi er en meget rimelig datamaskin bygget på et enkelt kretskort på størrelse med et bankkort. Den er utviklet av det britiske selskapet Raspberry Pi Foundation med tanke på å oppmuntre til å lære grunnleggende databehandling i skolen. <https://www.raspberrypi.org/>

⁵ Python er et programmeringsspråk hvor det er mulig å raskt kunne skrive enkel kode uten tidligere erfaring med koding. <https://www.python.org/>



Emner:

- Cyberspace: menneskelig og teknologisk sårbarhet
Jørgen Dyrhaug, Nasjonal sikkerhetsmyndighet (NSM)
- Samfunnets og individets sårbarhet i det digitale samfunnet
Janne Hagen, Norges vassdrags- og energidirektorat (NVE)
- Nettrett og netthyggiene
Peggy Heie, Norsk senter for informasjonssikring (NorSIS)
- Datakriminalitet
Rune Gåre og Anita Søndresen, Atea
- Straffeloven og digitale spor
Politinspektør Knut Erik Rame, Digitalt politiarbeid
- Kryptering og hacking
Omid Mirmotahari, Universitetet i Oslo (UiO)
- Koding og programmering
Ulike – inkludert Vitensenteret Sandnes og Godalen vgs.
- I tillegg praktisk arbeid innen:
 - o Dilemmatrenning / rollespill knyttet til nettkrenkelsers og sosiale medier
 - o Styre drone, sphere o.l. gjennom programmering / koding

Figur 5.1 Sertifikat i cybersikkerhet til elever ved Godalen videregående skole.

Etter første dag i cyberuken ble det holdt et eget seminar på kveldstid der flere rektorer i Rogaland og representant fra Stavanger kommune og Rogaland fylke ble invitert av rektor ved skolen. Her ble prosjektet presentert, og en representant fra skolens ledergruppe organiserte en paneldebatt mellom deltakere og ressurspersoner om erfaringene så langt. Det var ca. 30 fremmøtte deltakerne både fra administrasjon, andre skoler og næringslivet.

5.3 Ukeskurs på yrkesfag VG2

I februar 2019 ble det gjennomført en ukes elevkurs i CyberSmart i Haugesund for 105 elever på yrkesfaglig studieretning og IKT servicefag. Lærerne ved Haugaland videregående skole tok med seg erfaringene fra lærerkurset og den praktiske gjennomføringen i Stavanger og Ski. Undervisningsopplegget ble gjennomført over fire dager i uke 6 med bidrag fra NSM, NVE, Norsis, Atea og det lokale politiet. I tillegg kjørte lærerne ved Haugaland, med hjelp fra lærere ved Godalen videregående skole, et praktisk undervisningsopplegg med droneprogrammering og kryptering.

Et par elever fra Godalen videregående skole ble invitert for å snakke om sine erfaringer fra cyberuka i Stavanger. De snakket for elever på dagtid og for inviterte gjester på seminaret som ble holdt på kveldstid første dagen. Det ble godt mottatt av både elever og lærere. På kveldsseminaret var rektorer og representanter fra næringslivet invitert av avdelingslederen på Service og Samferdsel ved Haugaland videregående skole. Prosjektet ble presentert av Godalen videregående skole, NSM og NVE. Hatteland AS holdt et foredrag, som understreket behovet for cybersikkerhet i næringslivet og et bedre

samarbeid mellom skole og næringsliv. Til slutt var det en debatt mellom innleiderne og de ca. 12 frammøtte fra skole og næringsliv.

5.4 Sommerskole for ungdomstrinnet

Fire lærere i Ski kommune og Oppgård kommune utarbeidet i felleskap et undervisningsopplegg for en ukes sommerskole med tema cybersikkerhet for ungdomsskoleelever i Ski og Oppgård. Forarbeidet innebar å lage oppgaver, sette i stand Raspberry Pi'ene, lage «break-up boks», lage programmer og løyper, og handle premier og kodelåser. Elevene skulle senere knekke kodene ved hjelp av dekrypteringsteknikker. Inne i den låste boksen ventet godteri som belønning når alle kodene var knekket.

Sommerskolen ble holdt på Ski ungdomsskole. Elevene ble invitert via kommunens skoleportal til å delta på kurset. Kurset var gratis for elevene og de fikk kursbevis.



Figur 5.2 Kursbevis ved sommerskolen i Ski.

Sommerskolen ble fulltegnet med 29 elever. 26 elever stilte 1. dag – 19 stykker var igjen siste dag. Av de påmeldte var det 3 jenter.

Lærerne fra Ski og Oppgård hadde utformet opplegget og lagt vekt på at uken måtte bli så aktiv for elevene som mulig. Målet var å unngå «kjedelige» stillesittende foredrag, da dette var vurdert å være demotiverende for ungdom som gjør dette frivillig i sommerferien sin. Lærerne engasjerte en informatikkstudent som de møtte på UiOs CyberSmart-seminar i vinterferien samme år. Han stilte villig og helt gratis, og ordnet tilgang til relevante digitale nettsider – slik at elevene kunne lære om etisk hacking.

6 Evaluering

6.1 Forankring og finansiering

Prosjektet har gjennomgående blitt møtt med velvilje og stor interesse både fra private bedrifter og offentlige aktører. Det at cybersikkerhet i utgangspunktet er et dagsaktuelt tema har nok bidratt til å gjøre forankringsarbeidet lettere.

I tillegg til partnerne i prosjektet, bidro Politiets avdeling for digitalt politiarbeid (avdeling Rogaland) med undervisning på skolene i Rogaland.

Også private virksomheter viste interesse for prosjektet, eksempler er CISCO, Apple, IBM, Microsoft, og Atea. Atea bidro med undervisning på elevseminar i Rogaland. Tidsrammen og ressurssituasjonen i prosjektet tillot ikke prosjektet å teste ut andre næringslivsbidrag.

Prosjektet har gjort følgende erfaringer:

- Forankring hos skoleledelsen er en viktig suksessfaktor. Godalen videregående skole ble en pådriver for videreutvikling og tilpasning av undervisningen på videregående skoler i Rogaland. Det skal legges til at prosjektlederen var ansatt ved Godalen videregående skole, og dette var nok også en fordel. I Ski var rektor tilstede på flere av øktene i pilot-uka.
- Tid og ressurser til lærere som vil ha faglig oppdatering og delta på kurs er svært begrenset. Å løfte kompetansen i skolen krever derfor midler som ikke er der i dag. Et praktisk-teoretisk fag som cybersikkerhet krever at lærere får frigjort arbeidstid til å utdanne seg. Kunnskap om cybersikkerhet er ferskvare, og slik kunnskap må oppdateres.
- Seminar og debatt på kveldstid for rektorer og ansatte i kommunen og fylkeskommunen mv. kan bidra til å spre forståelse for CyberSmart prosjektet hos skoleeiere og opplæringskontoret i fylket. Seminar bidrar også til å rekruttere deltakere til neste lærerkurs.
- Det er viktig å sette av nok tid til å forankre prosjektet i de administrative og politiske organene på fylkesnivå og nasjonalt.

6.2 Gjennomføring av lærerkurs

Prosjektet erfarte at det var svært nyttig å besøke Universitetet i Tulsa i forkant av gjennomføringen av lærerkurset del I. Prosjektet hadde allerede utarbeidet et utkast til norsk undervisningsopplegg for lærere, og dette ble oversatt til engelsk og revidert etter besøket i Tulsa, der den norske delegasjonen fikk observere deler av et GenCyber opplegg i praksis. Den norske delegasjonen fikk se sjette klasse elever dekryptere koder og samarbeide om å løse problemer i «break-up boks» trening.

Deltakere på lærerkurset i mai 2018 med norsk undervisningspersonell og i februar 2019 med amerikansk undervisningspersonell fra Universitet i Tulsa ga gode tilbakemeldinger på at de hadde fått ny og nyttig kunnskap og at det var et spennende og et interessant

kurs. Det ble gitt tilbakemelding på at nettvett som tema er svært viktig og nyttig i undervisningssammenheng, og lærerne erfarte at de fikk større innsikt i egen sårbarhet på nett. Kursinnholdet ble gjenbrukt i senere elevseminarer og tilpasset elevgruppen og skolene. Anslagsvis 70% av det som ble undervist på lærerkurset i februar ble for eksempel gjenbrukt i sommerskolen i Ski/Oppegård. De vanskeligste oppgavene var det ikke tid til å gjøre ved sommerskolen.

Et sitat fra en lærer illustrerer nytteverdien og også utfordringene: *«Jeg kan bruke mye av kurset i min undervisning. Noe deler mer enn andre. Andre tema føler jeg at jeg trenger mer opplæring i for å kunne formidle videre selv. Verktøyene i hacking var for avanserte slik at her kan jeg ikke ta i bruk så mye. Deler av krypteringsverktøyene var ok. Mens opplegget som ble presentert av «NORSIS-slett meg» var helt topp! Mange av verktøyene er relevante, noe må nok forenkles til våre elever.»*

Tilbakemeldingen fra visiting associate professor Donna Farrior og lecturer in mathematics Kimberly Adams fra Universitetet i Tulsa til de norske lærerne som deltok på kursets del 2, var oppløftende. De norske lærerne ble oppfattet som aktive, løsningsorienterte og flinke til å samarbeide.

En sideeffekt av lærerkursets del 1 var at det ble arrangert kurs i cybersikkerhet for lærere som en del av planleggingsdagene i august 2018. På planleggingsdagene i august 2018 holdt en av kursdeltakerne fra Ski ungdomsskole et internt kurs for lærere i cybersikkerhet. Hun underviste 35 lærere i to puljer med varighet 1,5 time i cybersikkerhet, totalt 70 lærere. Det ble også holdt kurs for lærerne på en av planleggingsdagene ved Godalen videregående skole i august 2019. Dette framstår som en bærekraftig modell for å spre interesse og oppmerksomhet om tematikken til flere skoler i kommunen.

Prosjektet har gjort følgende erfaringer:

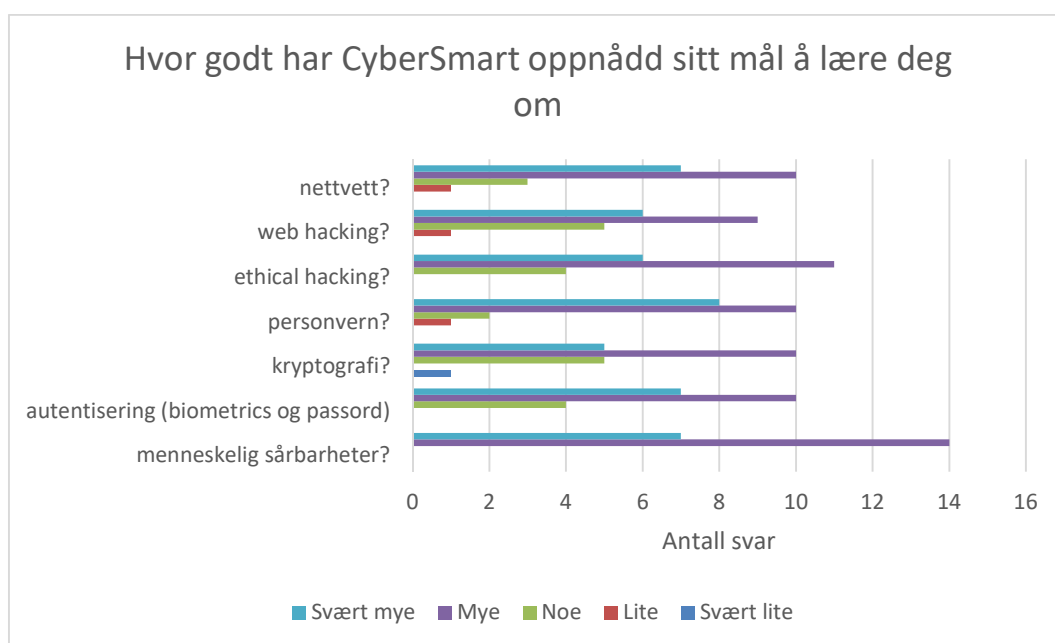
- Opplegget viser at alle kan lære. Det er ikke noe krav at lærere kan koding på forhånd, og det er heller ikke slik at lærere må ha god teknisk IT-kompetanse for å kunne undervise i cybersikkerhet.
- Tverrfaglig bakgrunn og samarbeid i lærergruppen på kurset bidrar til god problemløsning og forståelse.
- Å delta på to kurs gir bedre utbytte enn å delta på kun det ene. De lærerne som deltok på begge kursene hadde bedre totalforståelse enn de som bare deltok på kurs nr. 2. Også i USA hadde de tilsvarende erfaringer – det ga best effekt å delta to ganger. Dette handler om modning og å sette prosjektet inn i en teoretisk ramme før en går videre på de praktiske oppgavene som kryptering.
- Motivasjonsbrevne i forkant av det første lærerkurset gir best effekt om de blir lest på forhånd før kurset starter.
- Fagressurser er viktig for engasjementet. Fagressurser fra myndigheter og universiteter bidro med undervisning og til å skape stort engasjement. Det var en ubetinget stor suksess å bli undervist av undervisningspersonell fra Universitetet i Tulsa på lærerkursets del 2.

- De to lærerkursene har demonstrert at denne type kurs er god modell for undervisning i cybersikkerhet og for å teste ut ulike verktøy innen cybersikkerhetsundervisning.

6.3 Gjennomføring av elevseminar og sommerskole

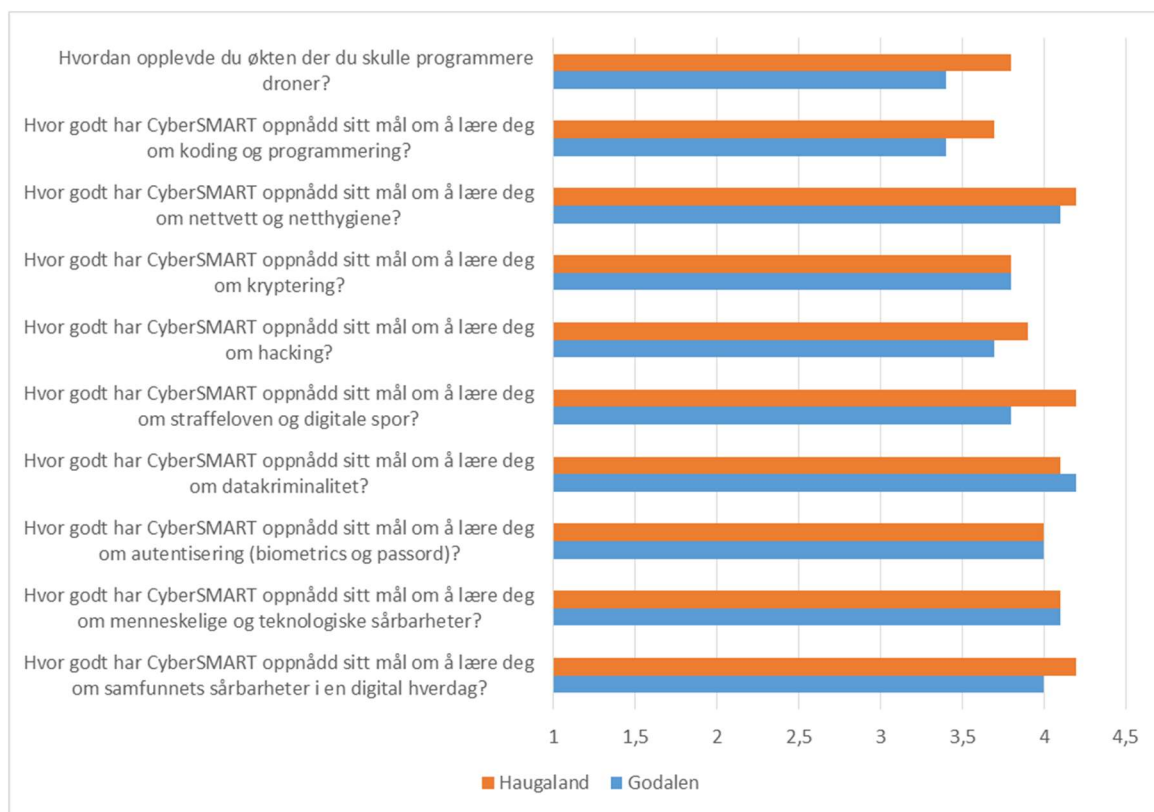
Prosjektet gjennomførte en elev-evaluering ved hjelp av spørreskjemaer. Alle tilbakemeldinger viser høy score fra elevene, både på temaet og de praktiske aktivitetene.

Elev-evalueringen fra Ski ungdomsskole i juni 2018 (Akershus fylke) viste at elevene var interessert i tematikken og at mange syntes dette var spennende. Det var generelt meget gode tilbakemeldinger og få som uttrykte misnøye, se Figur 6.1. Gitt at dette var slutten på 10-årig utdanning og varme sommerdager, er dette en tilbakemelding som viser at opplegget faglig fungerte veldig bra. Et suksesskriterium var nok at læreren her kjente elevene godt og deres faglige nivå, og undervisningen som ble gitt holdt god kvalitet. Både Godalen videregående skole og Ski ungdomsskole deltok med undervisning. I tillegg gjestet professor Sujeet Shenoï, fra universitetet i Tulsa elevseminaret.



Figur 6.1 Elevenes evaluering av elevkurset i Ski 2018, N= 21, karakter 1-5, der 5 er best.

Også ved Godalen og Haugaland videregående skoler i Rogaland fylke ble det gjennomført evaluering av elevkurset og alle kursmodulene. På en skala fra 1-5, der 5 er best, ble modulene gitt ca. 4 i snitt, se Figur 6.2, som gir en bedre oversikt over fordelingen.



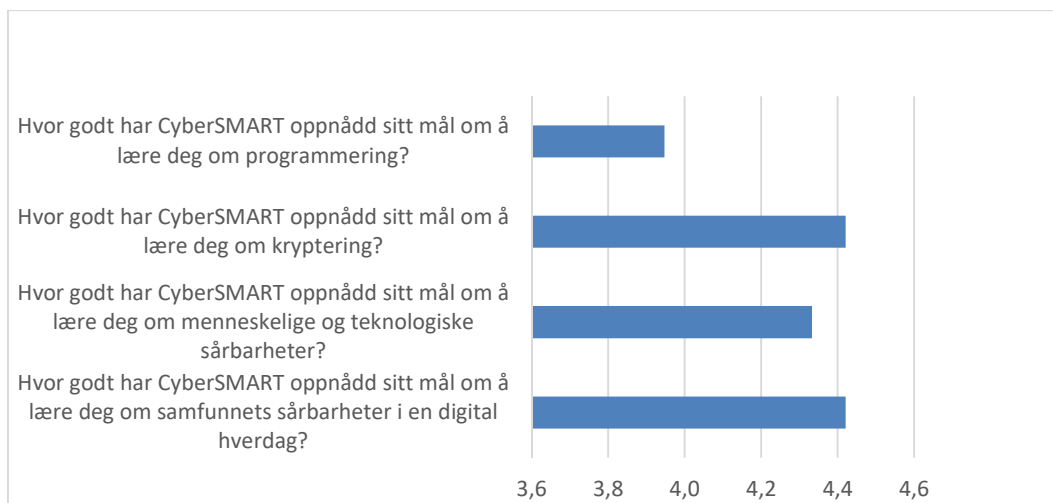
Figur 6.2 Evaluering av elevkurs ved Godalen (N=41) og Haugaland (N=42), karakter 1-5, der 5 er best.

Enkelte elever ved Godalen og Haugaland videregående skoler var svært engasjerte og interessert i tematikken. Mange oppga at de fikk ny kunnskap om deres egen digitale sårbarhet. Elevene opplevde dette som nyttig.

Prosjektet har gjort følgende erfaringer i forbindelse med elevseminar på videregående skole i skoletiden:

- Undervisningsopplegget i skoletiden fungerte godt faglig sett. Her trengte man ikke bli kjent aktiviteter. Elevene var engasjerte og ga gode tilbakemeldinger på innholdet i kurset.
- Læringsmålene er relevante men temaet er stort, og det viste seg å være krevende å klare å sette av nok tid til praktiske elevoppgaver.
- Elever fra Godalen videregående skole var innledere på elevkurset på Haugaland Videregående skole. De informerte om sine erfaringer fra cyberuken i Stavanger.

Sommerskolen (Ski og Oppegård) fikk også god tilbakemelding (karakter ca. 4 fra de 19 elevene som fullførte kurset), se Figur 6.3.



Figur 6.3 Elevenes evaluering av sommerskolen i Ski 2019 (N=19), karakter 1-5 der 5 er best.

Dette var en aktivitet utenom skoletid. Frafallet var imidlertid stort – av 29 påmeldte fullførte 19. Kjønnsfordelingen var skjev – 3 jenter og 26 gutter var påmeldt.

Mulige forklaringer på frafallet er at kurset ikke helt svarte til forventningene til alle elevene. Evalueringen viste at mange forventet å lære koding og hacking. Programmering og «break-up boks» leken fikk god tilbakemelding. Dessuten var elevmassen spredt i alder og programmeringsferdigheter. Noen hadde mye programmeringsbakgrunn og andre ikke noe. Aldersmessig dekket gruppen 4 års-trinn.

Prosjektet har gjort følgende erfaringer i forbindelse med sommerskolen:

- Høstferien og vinterferien kan være bedre tidspunkt for denne type elevkurs. Sommerskolen i Ski/Oppegård kom på tampen av skoleåret, og siste dag forlot alle skolens ansatte arbeidsplassen.
- Diversitet i elevgruppen var en utfordring med tanke på å tilby et tilpasset opplegg som engasjerte alle.
- Det er viktig å motivere elevene til å delta i bli-kjent aktiviteter. Å bli kjent er ett av områdene som de amerikanske erfaringene har erfart er viktige. Lærerne kjørte bli-kjent aktiviteter etter lunsj første dag.
- I forbindelse med sommerskolen krevde forberedelsene mer tid enn forventet. Forberedelsene inkluderte planlegging av faglig opplegg, innkjøp og klargjøring av Raspberry Pi og «break-up box» med premier.
- Det er viktig at markedsføringen er tydelig i sitt budskap om kursinnhold, slik at elevenes forventning kan innfris i størst mulig grad. Youtube video kunne kanskje vært et aktuelt medium å bruke for å nå ut med budskapet. Invitasjonen gikk bredt ut uten at elevene måtte søke om plass og begrunne egen motivasjon.
- Det er viktig at bestillingene til eksterne foredragsholdere er tydelige slik at overlappende foredrag unngås.

7 Fra pilot til nasjonalt tilbud

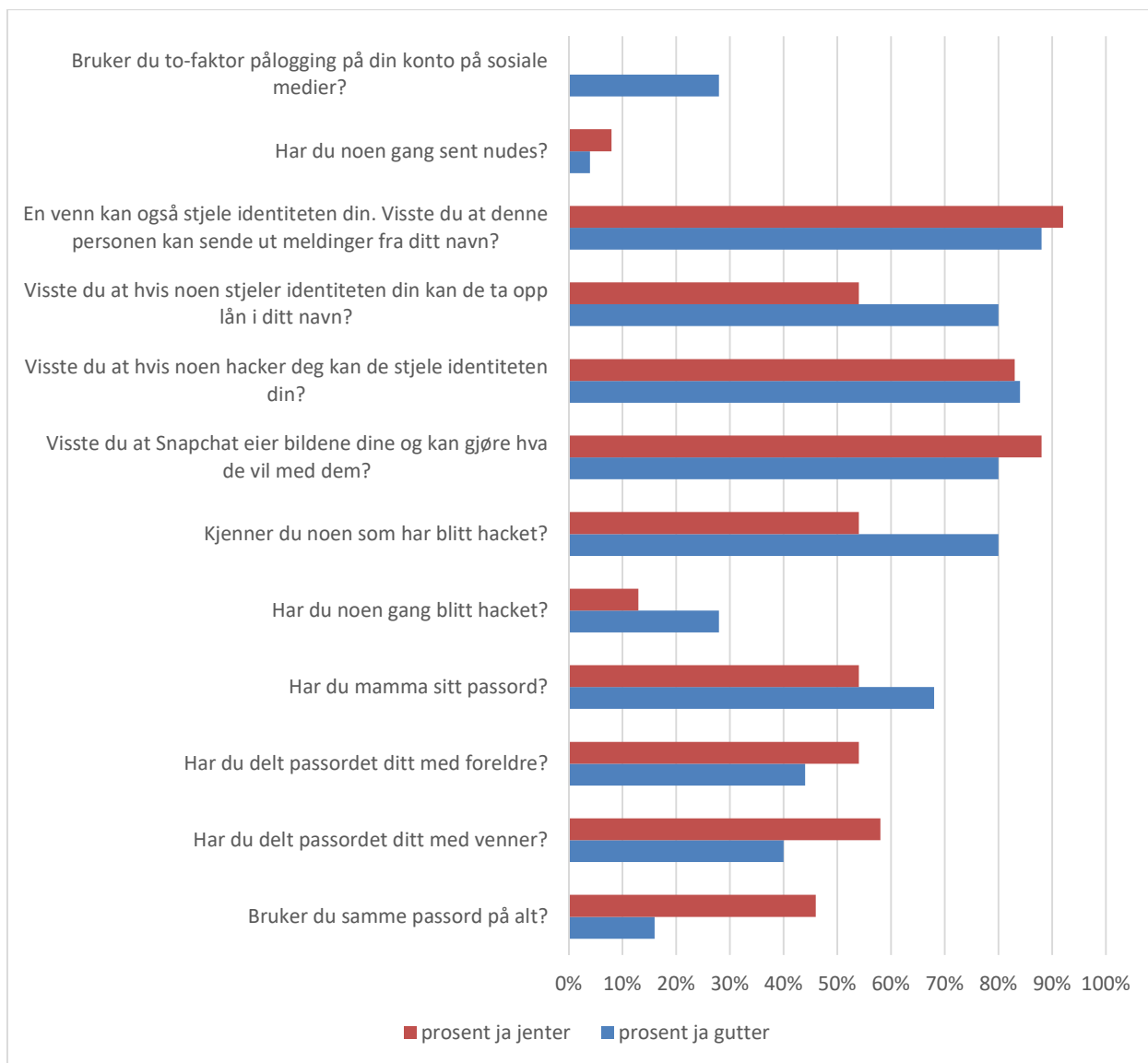
7.1 Behov for å lære ungdom om cybersikkerhet

I følge Norsis får ungdom lite opplæring i informasjonssikkerhet, sammenlignet med befolkningen for øvrig. Læringsmetodene er også annerledes for ungdommene, enn det de er for resten av befolkningen. Der 27% av befolkningen oppgir at de lærer av eksperter, oppgir kun 7% av ungdommene det samme. Dette gir grunn til bekymring fordi mye av praksisen omkring informasjonssikkerhet både kunnskapsbasert og ”ferskvare”.

Trusselbildet endrer seg over tid, og det samme gjør beskyttelsestiltakene. Dette krever at den enkelte får jevnlig påfyll av kunnskap om hvordan en skal sørge for at de er trygge på nett. Kun 6 av 10 ungdommer sier at de vet hva informasjonssikkerhet er. Norsis har også avdekket signifikante forskjeller mellom kjønnene. Gutter er mer interessert i teknologi og IT enn jenter. Jenter lærer primært av sine venner, mens gutter lærer primært av seg selv. Gutter har større tro på egne ferdigheter enn det jenter har, men har samtidig større tro på at de selv kan gjøre noe feil. Jenter oppfatter ulike aktiviteter på nett som mer risikofylte enn det gutter gjør (Malmedal & Røislien, 2017).

NVE hadde i april 2019 en ungdomsskoleelev utplassert i skolens arbeidsuke som en del av CyberSmart-prosjektet. Han gjennomførte en kartlegging av to ungdomsskoleklasser (46 elever) i 9 trinn på skolen sin i Moss. Svarene på undersøkelsen er vist i Figur 7.1. Resultatet viser at det er være et behov for opplæring i grunnleggende IKT-sikkerhet. Resultatet viser videre at det er kjønnsforskjeller. Ingen av jenter i undersøkelsen oppgir å bruke to-faktor-pålogging på tjenester. Flere av jentene delte passord med venner, men det kom også fram at foreldre har delt passordet med sine barn, og omvendt. Resultatet av kartleggingen er vist i Figur 7.1.

Resultatene samsvarer med Norsis sine funn, og underbygger behovet for opplæring av ungdom i cybersikkerhet.



Figur 7.1 Resultater av en spørreundersøkelse på en ungdomsskole – sikkerhetskultur (N= 46)

7.2 Etablering av nasjonalt tilbud

CyberSmart-modellen for etterutdanning av lærere er faglig god, men ressurskrevende i sin nåværende organisatoriske form. Lønnskostnader for undervisningspersonale og lærere som deltar på kurs blir høye. Lærerne mangler dessuten ledig tid for å drive med denne type faglig utvikling. I tillegg foretrekker lærerne kurs som gir studiepoeng. Basert på erfaringene i CyberSmart-prosjektet gir vi følgende anbefaling for etablering av et nasjonalt tilbud.

En opplæringsaktør bør få ansvaret for koordinering nasjonalt:

- NTNU/Realfagsenteret i Trondheim har vist interesse for CyberSmart-prosjektet og for å koordinere og utvikle et nasjonalt prosjekt. Vi anbefaler at

Realfagssenteret får en tilleggsbevilgning for å kunne gjøre denne oppgaven, som et minimum finansiering av en prosjektstilling.

Vi anbefaler følgende minimumsløsning dersom det ikke er mulig å frigjøre offentlige midler:

Initiativet drives videre av private på kommersiell basis eventuelt i regi av ideelle organisasjoner.

- Sommerskoler med vekt på å lære ungdom cybersikkerhet blir et tilbud som når de ungdommene som er mest interessert i koding og IT.
- Tilbud kan spesialsys til ulike målgrupper alt etter alder og kompetanse.
- På yrkesfag vektlegges et godt samarbeid med næringslivet, men dette kan utnyttes i sterkere grad. Det er et ubenyttet potensiale i å samarbeide med næringslivet. Så langt har Atea vært med i Rogaland. Prosjektet har vært i dialog med andre private selskap som har vist interesse for å bidra med teknologi eller undervisning i prosjektet, herunder Microsoft, CISCO, IBM og Apple.

Dersom det er mulig å frigjøre noe offentlig støtte anbefaler vi nettkurs i cybersikkerhet for lærere. Etterutdanningskurs som tilbys av universiteter for lærere og gir studiepoeng, er noe som lærerne har gitt tilbakemelding på er foretrukket framfor ikke poenggivende kurs.

- Bruk av digital teknologi og tilgang til virtuell lab vil gjøre det mulig å undervise bredden av lærere eller enkelte målgrupper av lærere, for eksempel lærere i IKT og koding. Et nettbasert kurs kan kombineres med samlingsbasert undervisning. Et eksempel på denne type kurs er etterutdanning i koding for lærere. Det er UiOs Center for Computing in Science Education som allerede tilbyr dette kodekurset, og de har opplyst at de kan inkludere noen cybersikkerhetstema i eksisterende opplegg.
- Lærere som deltar på cybersikkerhetskurs og som underviser elever kan kjøre korte kurs for lærere i kommunen. En modell her er Ski Ungdomsskole der en lærer underviste 35 lærere på to kurs, hvert av varighet på 1,5 time. Dette skjedde i Ski og ved Godalen videregående skole i forbindelse med skolens planleggingsdager.
- Opplæring av 10.klasse elever i cybersikkerhet kan gjennomføres av lærere som har deltatt på lærerkurs og inkluderes i eksisterende undervisning i andre fag, eksempelvis samfunnsfag, engelsk, sikkerhet, IKT-drift mm.
- Opplæring av 10. klasse elever i cybersikkerhet kan gjennomføres siste ukene av 10-årig grunnskole. Modellen ved Ski Ungdomsskole med undervisning på slutten av skoleåret – 10. klasse fungerte bra. Denne perioden, der noen elever har eksamen og andre ikke, kan utnyttes og gjøres mer interessant med et faglig godt undervisningsopplegg i cybersikkerhet.
- Ukeskurs i cybersikkerhet kan arrangeres ved videregående skoler av lærere som har deltatt på lærerkurs eller har på annet vis skaffet seg nødvendig kompetanse.

Undervisningen kan tilbys i flere av yrkesfagene. Cybersikkerhet hører naturlig med i linjevalg som fokuserer på sikkerhet og IKT-drift.

- Samarbeid med lokalt næringsliv, vitensentre mm. kan bidra til å gjøre undervisningen enda mer yrkesrettet og relevant for elevene.

Dersom det i større grad bevilges økonomisk støtte til prosjektet, nasjonalt eller regionalt, anbefaler vi at modellen i CyberSmart rulles ut over tid. CyberSmart bygger først tilbud lokalt og sprer så opplegget videre regionalt:

- En kurs- eller utdanningsleverandør kan utvikle del I lærerkurs basert på CyberSmart-erfaringene for hele nasjonen. Lærerkurs del I gir et bredere bilde av cybersikkerhetskontekst og nettvett, og del 2 rettes mot praktiske øvinger og problemløsning.
- Samarbeidet med USA videreføres inntil Norge har et godt nok og bærekraftig undervisningsmiljø selv, med opplæringsverktøy fra GenCyber og invitert undervisningspersonell med kompetanse på GenCyber. CyberSmart har kjørt rene samlingsbaserte kurs for lærere.
- I en videreføring anbefaler vi at universitetene i Norge lærer fra GenCyber og CyberSmart slik at de kan ta over opplæringen av lærerne og videreutvikle tilbudet. UiO og NTNU har allerede vært partnere i prosjektet, men det er flere fagmiljøer som kan være aktuelle.
- De ulike fylkeskommunene kan etablere et fylkesvis CyberSmart-prosjekt der en starter med opplæring av et lærerteam på videregående skole, som deretter videreutvikler elevkurs ved egen skole. Senere kan dette lærerteamet gjennom samarbeid bidra til å spre elevkurs og kompetanse til andre skoler i fylket. Rogaland fylkeskommune og Godalen videregående skole framstår som modell her.

7.3 Fagplan i cybersikkerhet

Læringsmålene for alle elevseminarene har vært å lære elever om nettvett, om egne sårbarheter når elevene er på sosiale medier og internett, lære generell IT-sikkerhet som passord, programvareoppdatering, koding og kryptering og forstå risiko for personvern ved publisering og deling av informasjon på nett. Læringsmålene opplevdes som hensiktsmessige og relevante av lærerne.

På yrkesfag inngår IKT sikkerhet i læreplanen i Service og Samferdsel. De nye læreplanene legger vekt på dybdelæring og tverrfaglighet. Derfor vil deler av cybersikkerheten passe inn i andre fag som lærerne underviser i. Lærerne erfarte på lærerkursets del I og del 2 at temaet cybersikkerhet er relevant også innen andre fagfelt, eksempelvis samfunnsfag, engelsk, matematikk og andre yrkesfaglige studieprogramfag. I samfunnsfag kan for eksempel trusselforståelse, egen sårbarhet og samfunnets sårbarhet inngå. Kryptering kan inngå i koding og matematikk.

Det ble lagt vekt på praktiske øvinger i CyberSmart. Cybersikkerhet som fag bør ha stort innslag av praktiske øvinger.

Temaet cybersikkerhet er omfattende. Elevseminarene viste at eldre elever på videregående skole hadde bedre forutsetninger for å forstå cybersikkerhet sammenlignet med elever på ungdomskolen, videre at elever på IKT-drift hadde bedre forståelse enn elever fra service og samferdsel. Dette taler for at det er fornuftig å tenke en nivådeling etter alder og kompetanse.

8 Konklusjon

Formålet med prosjektet var å utvikle en pilot for å teste et opplæringskonsept i cybersikkerhet for lærere og elever etter modell av amerikanske GenCyber. Et annet delmål i prosjektet var å gi innspill til læreplaner i skolen på digital sikkerhet.

Denne rapporten oppsummerer prosjektets erfaringer. Prosjektet har høstet gode erfaringer og fått tilbakemelding på at det faglige opplegget er interessant, lærerikt og givende. Økonomi og ressursbruk hos eksperter i piloten er ikke egnet for videreføring nasjonalt uten at modellen forenkles og noen tar et samlet ansvar.

Prosjektet anbefaler at det arbeides videre med å lære opp ungdom i cybersikkerhet i Norge. Rapporten skisserer noen mulige veier framover basert på ulike økonomiske ambisjonsnivåer. Uavhengig av de økonomiske begrensningene anbefaler rapporten at:

En opplæringsaktør får ansvaret for koordinering nasjonalt, og at som et minimum bør det bevilges midler til en prosjektstilling.

Avhengig av økonomisk ramme anbefales følgende:

1. Initiativet drives videre av private på kommersiell basis eller av ideelle organisasjoner (Ingen til lite offentlig økonomisk tilskudd)
2. Nettkurs i cybersikkerhet for lærere, eventuelt med noen samlinger (En viss økonomisk ramme – medium satsing).
3. CyberSmart bygger først tilbud lokalt og sprer så opplegget videre regionalt (Stor økonomisk ramme).

Prosjektet har ikke hatt anledning til å utrede de økonomiske rammene, og det anbefales derfor at en egen utredning er på dette.

Vedlegg A – Eksempel timeplaner

Lærerkurs ved UiO (28/5-1/6-2018)					
Time	Mandag NSM	Tirsdag NTNU/FIH	Onsdag NVE	Torsdag UIO	Fredag NORSIS
09.30 – 10.15	Cybersikkerhet Hva er det? Innledende teori	Oppsummering/ refleksjon Omid	Oppsummering/ refleksjon Omid	Oppsummering/ refleksjon Omid	Oppsummering/ refleksjon Omid
10.15 – 12.00	Menneskelige sårbarheter Sikkerhetskultur * Manglende forståelse for trusler og risiko * Vår egen verdi og betydning i et større perspektiv * Forholdet vårt til sikkerhetsregler * Passord * Sårbarhetsutnyttelse * E- post * Kompetanse	Autentisering Passord med en praktisk oppgave Biometri med en praktisk oppgave	Karrieremuligheter Eksempler fra virkeligheten Konsekvenser av dårlig sikkerhet Hvordan bidrar myndigheter og næringsliv til bedre sikkerhet Dilemmaer Personvern, sikkerhet og innovasjon	Etisk hacking Informasjons - innsamlingsteknikker: verktøy og metoder for å samle informasjon fra målet Oppgaver: samle inn spesifikk informasjon ved hjelp av google hacking	Nettvett Grunnleggende ferdigheter med praktiske oppgaver (på PC)
12:00 – 13:00	<i>Lunsj</i>	<i>Lunsj</i>	<i>Lunsj</i>	<i>Lunsj</i>	<i>Lunsj</i>
13.00 – 16.00	Oppsummering og diskusjon Hvordan kan vi forklare dette for elevene? Hva slags metoder vil fungere best? Teknologiske sårbarheter *Epost *Vannhull *innloggings - informasjon	Krypto Klassisk krypto med hånd – papir oppgaver Moderne krypto On-line verktøy med oppgaver	Prosjektoppgaver Teste ut prosjektoppgaver som kan brukes i andre fag og få ideer til å lage egne oppgaver	Web-hacking Hovedtyper av web-sårbarheter og hvordan disse kan utnyttes Oppgaver: tilgang til skjult innhold på nettsider, enkel sql injeksjon utnyttelse Programvare - sårbarheter: Kort oversikt over programvare bugs Oppgaver: Krasje en binær	Slett meg Utfordringer knyttet til bruk av internett og sosiale medier. Dilemmatrenning knyttet til utfordringene med nettkrenkels er

Elevseminar ved Ski ungdomsskole (11/6-15/6-2018)					
Time	Mandag NSM/Bodil/Omid?/ Kristin	Tirsdag UIO	Onsdag Sujeet	Torsdag Tone/Anne	Fredag Egil
8.15 – 10.00	Gym	Avreise fra Ski med tog 8.57	9.00: Kristin Intro av Sujeet	Kryptering	Slett - meg
10.00	Cybersikkerhet Hva er det? Innledende teori/intro	UIO Med Omid Hacking	Sujeet Varierte eksempler	Hva er kryptering?	Slett meg
10.30 - 11.30	Menneskelige sårbarheter Sikkerhetskultur Sårbarhet Hva deler du i dag Øvelse : - hva deler du	Informasjons - innsamlingsteknikker: verktøy og metoder for å samle informasjon fra målet	OBS: foto og filmforbud	Eksempler på dagligdags koding SMS Caesar chiffer Hva er det?	Utfordringer knyttet til bruk av internett og sosiale medier. Dilemmatrening knyttet til utfordringene med nettkrenkelser
11:30 - 12:15	<i>Lunsj</i>	<i>Lunsj</i>	<i>Lunsj</i>	<i>Lunsj</i>	<i>Lunsj</i>
12.15 – 14.00	film om passord – Personlig informasjon - hvem deler du med - __hvorfor Inngangsvinkel: Deling av bilder - bilder – apper – rettigheter Snapchat – tillatelser *Oppgave: google	Hacking Div oppgaver med Omid Web-hacking Hovedtyper av web-sårbarheter og hvordan disse kan utnyttes	Sujeet Varierte eksempler OBS: foto og filmforbud Holder på så lenge han føler at publikum er med kanskje helt til klokken 15.00	Hva er biometri? Biometriske kjennetegn Filmsnutter fra Youtube	rebus/kodeknekkingsoppgave

Elevseminar ved Godalen VGS. (10/09-14/09-2018)					
Time	Mandag NVE/NSM	Tirsdag UIO/Norsis	Onsdag UIO/Politiet/Atea	Torsdag UIO/vitensenteret	Fredag NSM
08.30 – 09.00	Oppstart mandag 10.9 Kl. 09.30 Rektor ønsker velkommen Intro ved Trond Øvstedal Kommunikasjonssjef hos NSM	Kl. 8.30 Oppsummering/ refleksjon Omid	Kl. 8.30 Oppsummering/ refleksjon Omid	Kl. 8.30 Oppsummering/ refleksjon Omid	Kl. 9:00
09.00 – 11.30	Det digitale samfunnet- din sårbarhet og samfunnets sårbarhet Hvorfor bry seg - karrieremuligheter ved Janne Hagen NVE	Nettvett Gruppeinndeling: Gruppe 1: Aud Gruppe 2: SS Grunnleggende ferdigheter med praktiske oppgaver (på PC) Slett meg Utfordringer knyttet til bruk av internett og sosiale medier. Peggy Heie hos Norsis	Datakriminalitet Hvordan operer de kriminelle? Eksempler på ulike angrep v/Rune Gåre og Anita Sondresen hos Atea Gruppeinndeling – oppstart 10.15 Gruppe 1: stasjoner Gruppe 2: Aud Straffeloven og digitale spor Politiinspektør Knut Erik Rame Leder for digitalt politiarbeid	Kryptering/hacking Hovedtyper av web-sårbarheter og hvordan disse kan utnyttes Omid Mirmotahari UIO Div. oppgaver relatert til hacking	Menneskelige sårbarheter Cyberspace og teknologiske sårbarheter v/ Jørgen Dyrhaug NSM (Nasjonal sikkerhetsmyndig- het)
11.30	<i>Lunsj</i>	<i>Lunsj</i>	<i>Lunsj</i>	<i>Lunsj</i>	<i>Lunsj</i>
12.15 – 14.00	Cyberspace og menneskelige sårbarheter Jørgen Dyrhaug i NSM Nasjonal sikkerhetsmyndig- het	Gruppeinndeling: Gruppe 1: SS Gruppe 2: Aud Dilemmatrening i klasserommet knyttet til utfordringene med nettkrenkelser	Gruppeinndeling: Gruppe 1: Aud Gruppe 2: stasjoner Fire stasjoner: - Droner - Sphere - Kodeleker -Google home	Vitensenteret: Buss fra skolen kl. 12 Gruppeinndeling: 1. Programmering - microbit 2. Utstilling 3D- print 3. Film	Avslutning med diplom for Vg1 elever Evalueringsav- kurset

		Diskusjon i grupper i forhold til nettvett/sosiale medier Film: Catfish	Ansvarlig for stasjonene: Jarle Børge Solveig Anne Tone		
--	--	--	--	--	--

Eleve seminar ved Haugaland VGS uke 6 2019				
Time	Mandag NVE/NSM	Tirsdag Norsis/NSM	Onsdag	Torsdag
08.30 – 09.00	08:30 Test - forkunnskaper (klasserom)	Oppsummering/ refleksjon person (klasserom)	Oppsummering/ refleksjon (klasserom) <i>Film frem til kl 10.00</i>	Oppsummering/ refleksjon (klasserom)
09.00 – 11.30	Tim ønsker velkommen Presentasjon av Cyber uken (Ari og Malin kommer og deler noe av deres erfaring fra Godalen) Det digitale samfunnet- din sårbarhet og samfunnets sårbarhet Hvorfor bry seg- Karrieremuligheter Janne Hagen NVE (Aud 1)	Menneskelige sårbarheter Jørgen Dyrhaug NSM Sikkerhetskultur * Manglende forståelse for trusler og risiko * Vår egen verdi og betydning i et større perspektiv (Aud 1)	Data kriminalitet 10.00 – 11.30 Politiet v/ Knut Gjerde Hvordan operer de kriminelle? Eksempler på ulike angrep Politiet – Straffeloven (Aud 1)	09.00 - 13.00 <i>Vi møtes først i aud 1 for å deles i tre grupper., så går elevene til sin første stasjon.</i> <i>Vi begynner på ny stasjon kl 10 og 11</i> Stasjon 1: - Droner og Sphere (Jarle og Børge) Rom 1401 og 2401 Stasjon 2: - Kodeøvelser (Mona/Bodil/ Monica) Cafe C Stasjon 3

11.30 – 12.00	<i>Lunsj</i>	<i>Lunsj</i>	<i>Lunsj</i>	- IKT servicefag (<i>Arne og Rune</i>) IKT klasserommet
12.00 – 15.00	12.00 – 14.30 Passord Biometri <i>Jørgen Dyrhaug NSM</i> (Aud 1) <i>Ettermiddag fra kl 15:00 til 18.00.</i> Vi begynner med suppe kl 15.00 15.30 Velkommen Presentasjon av prosjektet og idéene bak Hvorfor trenger vi å lære opp ungdom i cybersikkerhet? - Janne Hagen NVE - Jørgen Dyrhaug NSM - Bodil Ellen Grødem Godalen vgs Hva forventer næringslivet av sine fremtidige arbeidstakere? - Innlegg av Olav Espedal, Sikkerhetssjef Hatteland - Paneldebatt	Nettvett <i>Norsis</i> Grunnleggende ferdigheter med praktiske oppgaver (på PC) Slett meg Utfordringer knyttet til bruk av internett og sosiale medier. Dilemmatrening knyttet til utfordringene med nettkrenkelser Diskusjon i grupper i forhold til nettvett/sosiale medier Rollespill Case (Eik –bygget)	Kryptering/hacking <i>Anita Sondresen Atea</i> (samme opplegg som på Godalen) (Aud 1)	<i>Ca 45 minutter på hver stasjon</i> Evaluerings/ og avslutning med pizza og diplom ca kl 12.00 (2401)

Sommerskole i Ski 24/6-28/6 2019

Mandag 10.00 – 15.00 Ansvar: Kristin	Tirsdag 10.00 – 15.00 Ansvar: Maria	Onsdag 10.00 – 15.00 Ansvar: Espen	Torsdag 10.00 – 15.00 Ansvar: Egil	Fredag 10.00 – 14.00 Ansvar: Alle
Tema: Personvern og Kryptografi Kl. 10.00 Introduksjon og Presentasjon ved Janne Hagen NVE Kl. 12.00 Lunsj Kl. 12.45 Teori: Introduksjon til kryptografi Praktisk: Oppgaver 15.00 Slutt	Tema: Datasikkerhet Kl. 10.00 kryptofun Kl. 10.30 Teori: NSM Jørgen Dyrhaug Tema: datasikkerhet Kl. 12.00 Lunsj Kl. 12.45 «Capture The Flag» 15.00 Slutt	Tema: Programmering og sikkerhet Kl. 10.00 kryptofun Kl. 10.30 Teori: Lære om koding Innføring i programmering av Sphero Kl. 12.00 Lunsj Kl. 12.45 Praktisk: Sphero bolt 15.00 Slutt	Tema: Teknisk kryptografi Kl. 10.00 kryptofun Teori: Introduksjon Raspberry Pi Kl. 12.00 Lunsj Kl. 12.45 Praktisk: Raspberry pi og kodeknocking. 15.00 Slutt	Tema: Utprøving av opparbeidet kunnskap Kl. 10.00 kryptofun Kl. 10.30 Praktisk oppgave: Break-up box Kl. 12.00 lunsj m/pizza Kl. 13.00 Evaluering Utdeling av kursbevis. 14.00 Slutt

Vedlegg B – Deltakere

Navn	Rolle
Mona Strøm, NSM	Leder styringsgruppen
Bodil Ellen Grødem, Godalen videregående skole	Prosjektleder
Eldri Holo, NVE	Medlem styringsgruppen
Kirsi Helkala, CIS	Medlem styringsgruppen
Peggy Heie, Norsis	Medlem styringsgruppen
Audun Jøsang, UiO	Medlem styringsgruppen
Nils Kalstad Svendsen, NTNU	Medlem styringsgruppen
Christine Korme, Abelia	Medlem styringsgruppen (kun i starten)
Anne Helen Dahle, Godalen videregående skole	Medlem styringsgruppen
Omid Mirmotahari, UiO	Fagressurs
Lazlo Erdodi, UiO	Fagressurs
Jørgen Dyrhaug, NSM	Fagressurs
Trond Øvstedal, NSM	Fagressurs
Janne Hagen, NVE	Fagressurs
Kristin Kurtz, Ski ungdomsskole	Fagressurs ved Ski Ungdomsskole
Knut Gjerde, Politiet	Fagressurs
Anita Sondresen, Atea	Fagressurs
Sujeet Sheno, Universitetet i Tulsa	Fagressurs Cybersikkerhet
Kimberly Adams, Universitetet i Tulsa	Fagressurs GenCyber
Donna Farrior, Universitetet i Tulsa	Fagressurs GenCyber

Referanser

- Godalen videregående skole. (2019, 3 4). *Lærere på Godalen videregående skole har fått opplæring i cybersikkerhet av eksperter fra USA!* Hentet fra Godalen.vgs.no: <http://www.godalen.vgs.no/Aktuelt/Laerere-paa-Godalen-videregaaende-skole-har-faatt-opplaering-i-cybersikkerhet-av-eksperter-fra-USA>
- Grødem, B., & Dale, A. (2019, 4 26-27). *CyberSMART - pilotprosjekt med opplæring i cybersikkerhet i vgs*. Hentet fra Rogalandskonferansen: https://rogalandskonferansen.weebly.com/uploads/7/1/5/9/7159280/program_rogalandskonferansen_2019.pdf
- Hagen, J. (2019). *CyberSmart - educating the future workforce. Narrative and financial report. NVE-rapport 20:2019*. Oslo: NVE.
- Hagen, J., & Grødem, B. (2018, 6 14). *Folk flest forstår ikke hva som er bak skjermen - Dette burde bekymre mange*. Hentet fra Digi.no: <https://www.digi.no/artikler/kommentar-baerekraftig-digitalisering-trenger-bevisste-ungdommer/439866>
- Hagen, J., & Grødem, J. (2019). *CyberSmart - Teach the Teachers. Computerworld, Mars 2019*, 71.
- Justis- og beredskapsdepartementet og Kunnskapsdepartementet. (2019). *Nasjonal strategi for digital sikkerhetskompentanse. Satretgi, 30 Januar 2019*. Oslo: Departementene.
- Kunnskapsdepartementet. (2017). *Framtid, fornyelse og digitalisering. Digitaliseringsstrategi for grunnsopplæringen 2017-2021. Strategi*. Norge: Kunnskapsdepartementet.
- Malmedal, B., & Røislien, H. E. (2017). *Ungdom og digital sikkerhetskultur*. Gjøvik: Norsis.
- Norsis. (2017). *Nordmenn og digital sikkerhetskultur*. Gjøvik: Norsis.
- NSM. (2019, 5 7). *CyberSmart lærerkurs er gjennomført*. Hentet fra NSM: <https://www.nsm.stat.no/aktuelt/cybersmart-larerkurs-er-gjennomfort/>
- NTNU. (2018). *CyberSmart - mer kunnskap om sikkerhet*. Hentet fra NTNU CCIS: <https://www.ntnu.edu/ccis/cybersmart>
- NVE. (2018). *Lærere på skolebenken for å bli cybersmarte*. Hentet fra NVE: <https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/laerere-pa-skolebenken-for-a-bli-cybersmarte/>
- NVE og NSM. (2017). *Informasjonssikkerhetsilstanden i energiforsyningen, NVE-rapport nr 90: 2017*. Oslo: NVE. Hentet fra NVE.
- Sikkerhetsfestivalen. (2019, 8 27). *7 representanter fra offentlig sektor og utdanning. Digital sikkerhet som allmennkunnskap*. Hentet fra Sikkerhetsfestivalen.no: <https://sikkerhetsfestivalen.no/bidrag2019/7>
- Stavanger Aftenblad. (u.d.). *Stavanger Aftenblad, debatt*. Hentet fra Godalen vgs er med på dugnad i cyber-sikkerhet: <https://www.aftenbladet.no/meninger/debatt/i/bKBrAv/Godalen-vgs-er-med--pa-nasjonal-dugnad-i-cyber-sikkerhet-->
- Thon, R. (2018). *Teaching the teachers*. Hentet fra NSM-blogg: <https://www.nsm.stat.no/blogg/cybersmart2018/>
- TV-Vest, v. 1. (Regissør). (2018). *Elever for et tryggere samfunn* [Film].

Utdanningsdirektoratet. (2017). Rammeverk for grunnleggende ferdigheter - Revidert 2017. Til bruk for læreplangrupper oppnevnt av Utdanningsdirektoratet. *Strategi*. Utdanningsdirektoratet.



NVE

Norges vassdrags- og energidirektorat

.....

MIDDELTHUNSGATE 29
POSTBOKS 5091 MAJORSTUEN
0301 OSLO
TELEFON: (+47) 22 95 95 95

www.nve.no