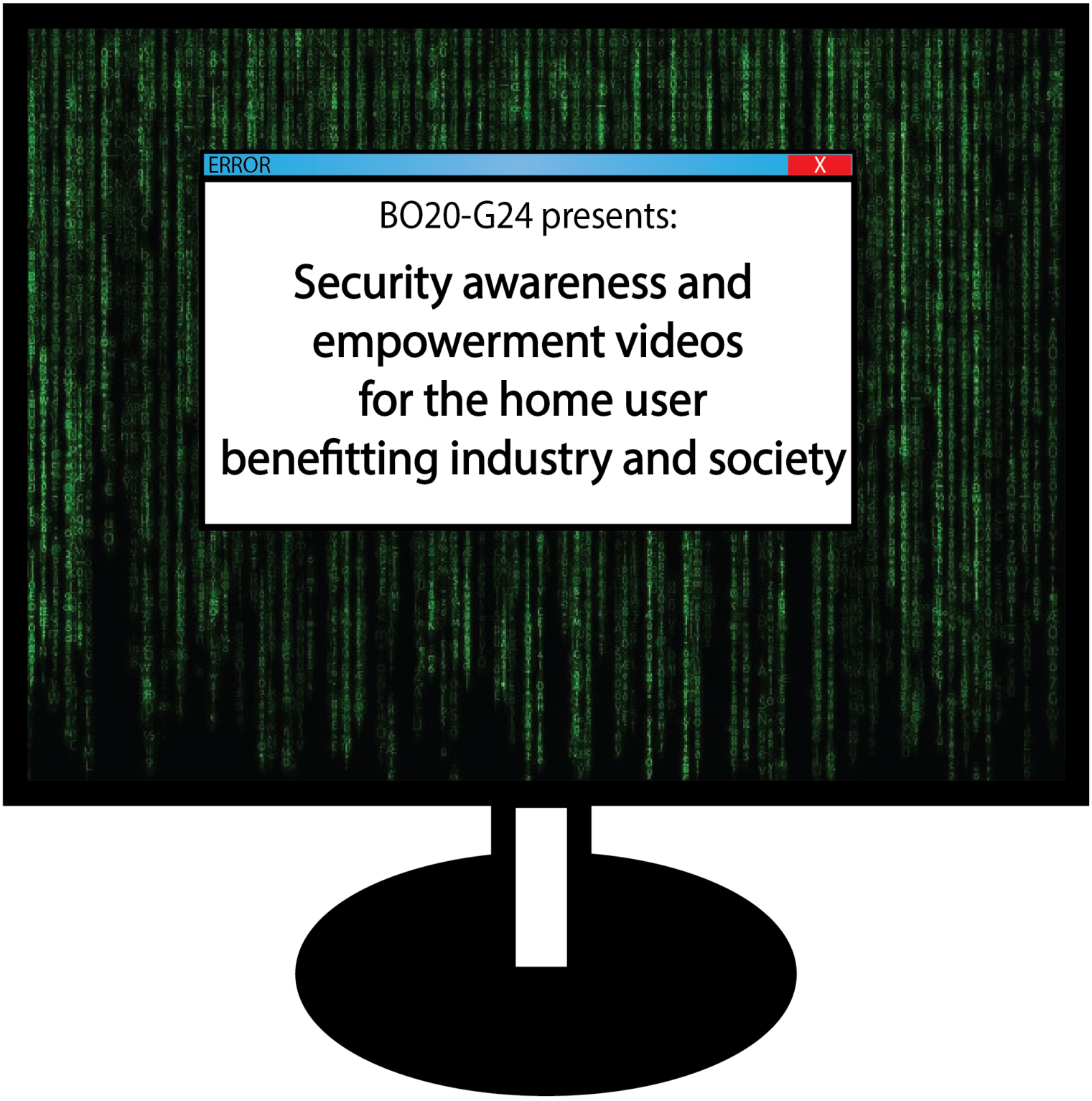


Bacheloroppgave 2020

28.05.2020

Christopher Romnæs

Tom Martin Roberg

Håvard Pettersen

Sindre Torgersen

Avdeling for Informasjonsteknologi
Høgskolen i Østfold

HØGSKOLEN I ØSTFOLD
Avdeling for Informasjonsteknologi
Remmen
1757 Halden
Telefon: 69 21 50 00
www.hiof.no

BACHELOROPPGAVE

Prosjektkategori: Bacheloroppgave	X	Fritt tilgjengelig
Omfang i studiepoeng: 20		Fritt tilgjengelig etter:
Fagområde: Datasikkerhet		Tilgjengelig etter avtale med arbeidsgiver

Rapporttittel: Security awareness and empowerment videos for the home user benefitting industry and society	Dato: 09 Mars, 2020
Forfattere: Tom Martin Roberg, Håvard Pettersen, Christopher Romnæs, Sindre Torgersen	Veileder: Gunnar Misund
Avdeling / linje: Avdeling for Informasjonsteknologi	Gruppenummer: BO20-G24

Oppdragsgiver: IFE, Institutt for energiteknikk	Kontaktperson: John E. Simensen, Sizarta Sarshar

Ekstrakt:
Institutt for energiteknikk (IFE) jobber med nukleært arbeid og de er opptatt av datasikkerhet. Gruppen sin oppgave er å lage videoer som kan brukes for å styrke kunnskapen om datasikkerhet blant hvermannsen. Ved instrukser av kontaktpersonene og hjelp fra veileder, skal gruppen lage relevante videoer som IFE kan få bruk for i senere tid. Gruppen har valgt å sende ut en spørreundersøkelse og med det få inn svar som kan være til hjelp for å lage relevante videoer. Gjennomføre intervju om datasikkerhet med relevant fokusgruppe og bruktertesting av videoer laget på basis av dette.

3 emneord:

Datasikkerhet
Samfunnet
Video

Sammendrag

Vi fikk i oppdrag å lage videoer for å styrke «mannen på gata» sine datasikkerhetskunnskaper. Oppgaven var relativt åpen og kunne løses på den måten som gruppen synes var best. Vi valgte å holde oss innenfor infotainment sjangeren, grunnet at innholdet i videoene skulle bli formidlet på en slik måte at «mannen på gata» kan selvstendig styrke sine datasikkerhetskunnskaper ved å se på videoene.

Tidlig i arbeidet startet vi med å finne ut hva vi trengte å finne ut om datasikkerhet, og arbeidet mot å finne ut lignende prosjekter som vi kunne hente ideer og tankegang fra. Vi la raskt for oss hvilket utstyr vi ville trenge for å lage filmene, og vi fikk lånt dette utstyret av Høgskolen i Østfold.

Gruppen valgte å sende ut en kvantitativ spørreundersøkelse for å finne ut hvor nivået til «mannen på gata» ligger. Dette gjorde vi ved å analysere alle svarene som vi fikk fra spørreundersøkelsen. Dette ga oss et bedre innblikk i situasjonen og var til stor hjelp for oss når vi skulle lage videoer for å treffe «mannen på gata» best mulig.

Det ble også valgt ut en fokusgruppe som skulle se på videoene før de ble ferdig, for å hjelpe oss med å lage videoer som treffer målgruppen best mulig. Etter at vi hadde analysert svarene fra den kvantitative spørreundersøkelsen, valgte vi å gjennomføre semistrukturerte intervjuer med fokusgruppen, for å gå enda mer i dybden enn den forrige spørreundersøkelsen. Fokusgruppen kom med tilbakemeldinger på videoene, slik at vi kunne endre de etter beste evne.

Det var som plan å filme på lokasjoner presentert i storyboards. Manus ble deretter lagd på vegne av storyboards. Det ble endringer i hele denne prosessen etter koronaepidemien. Nye lokasjoner måtte brukes, nye storyboards og nye manus.

Det ble produsert to filmer som skal styrke «mannen på gata» sine datasikkerhetskunnskaper. Den første videoen handlet om at en person ble et offer for en svindel og at en annen person forklarer hva offeret burde ha gjort for å forhindre dette. Den andre filmen handlet om at en person plukker opp en minnepenn fra bakken og setter den inn i pc-en. Det viser seg å være en orm i det dokumentet, noe som kan vise seg å være farlig. Her er det også en person som forklarer hva som kan være farlig ved å plukke opp en minnepenn fra bakken som noen andre eier. Etter flere brukertester av videoene så gjorde vi endringer på de for å bedre treffe «mannen på gata».

Helt i starten av prosjekttiden satte vi oss noen mål som vi skulle forsøke å oppnå. Etter en vurdering av gjennomføringen, kom vi frem til at vi hadde nådd målene. Etter at alt var gjennomført, fant vi noen forbedringspotensialer som kunne gjort at resultatet hadde blitt bedre.

Etter en prosess med spørreundersøkelse, semistrukturert intervju, to videoer og brukertester, kan vi ærlig si at vi har lært mye. Vi har måtte ta valg og reflektere over våre egne forventninger, for å komme med et så godt produkt som vi til slutt gjorde. Vi ønsker å ta med oss all læringen videre i livet.

Innhold

1 Introduksjon

1.1 Prosjektgruppen

Christopher

Jeg er født i 1996, er fra Trøgstad. har fagbrev i IKT, har tatt faget videoproduksjon, samtidig som jeg skal ta faget datasikkerhet vårsemesteret 2020. Jeg går nå digitale medier og design og er det jeg skal ta bachelor oppgave i.

Håvard

Jeg er født i 1995, Fredrikstad. Jeg startet på Gudeberg skole hvor jeg gikk i 2 år før jeg flyttet til Italia Der gjennomført jeg fire års skolegang ved International School of Naples (2003-2007). I denne tiden trente jeg mye. Jeg spilte fotball, drev med Tae Kwon Do, og i tillegg drev drev jeg med ridning og deltok i rideshow.

Da jeg flyttet tilbake til norge valgte jeg å fortsette med fotball. Jeg spilte på Østsiden fotballklubb i fem år før jeg jeg sluttet og begynte på Frederik ii Vgs(studiespesialisering).

Videre etter videregående begynte jeg å jobbe i Coop Goman Bakeriet Value Marketing Fredrikstad Kommune Showfabrikken. I dag holder jeg på med Bachelor i Digitale Medier og Design ved Høgskolen i Østfold samtidig som jeg trener regelmessig på treningsstudio.

Sindre

Jeg er født i 1998, født og oppvokst i Halden. Jeg gikk studiespesialiserende med realfag på videregående, med IT1 og IT2 som valgfag. Etter videregående begynte jeg rett på Høgskolen i Østfold. Jeg går nå 3.året på informasjonssystemer og jeg skal ta innføring i datasikkerhet dette semesteret.

Tom Martin

Jeg er født i 1998, er født og oppvokst i Halden. Jeg gikk IT i studiespesialiserende på videregående, og gikk videre rett etter videregående til høgskolen i Østfold. Jeg går nå Informatikk, design og utvikling av IT-Systemer. Jeg har hatt faget innføring i datasikkerhet, og jeg skal ta faget datasikkerhet i utvikling og drift i vårsemesteret 2020.

1.2 Oppdragsgiver

Institutt for energiteknikk (IFE) ble etablert i 1948 som Institutt for atomenergi (IFA), og fikk i 1980 dagens navn. IFE har sitt hovedkontor på Kjeller og en nesten like stor avdeling i Halden i Østfold. IFE er vertsorganisasjon for det internasjonale Halden prosjektet, med deltakere fra 19 medlemsland. IFE driver forskning på følgende områder: energi-, miljøteknologi og fysikk (Kjeller), nukleærteknologi (Kjeller), petroleumsteknologi (Kjeller), nukleær sikkerhet og pålitelighet (Halden), og tematikken «sikkerhet-menneske-teknologi-organisasjon» (Halden). IFE driver to forskningsreaktorer. JEEP II-reaktoren på Kjeller brukes til grunnforskning i fysikk og produksjon av legemidler, mens Haldenreaktoren brukes til forskning på materialteknologi og kjernebrensel sikkerhet. Instituttet har ca. 600 ansatte i Halden og på Kjeller. Instituttets administrerende direktør er Nils Morten Huseby[1].

[1] https://no.wikipedia.org/wiki/Institutt_for_energiteknikk

1.3 Oppdraget

Staying safe in a digital world is a challenge for private individuals and companies alike. In the modern advanced society, the technological lines between work and private (non-work) become meshed. At the work place the companies are continuously struggling with designing and implementing of countermeasures to ensure and support the secure digital behaviour of the workers, with an objective of turning their employees from being a possible vulnerability to becoming a strong first line of defence. Many companies are working systematically with security and cyber security and is employing best practices from e.g. NSM and societal tools such as "nasjonal sikkerhetsmåned". The typical learning material the employees go through is online informational slides consisting mainly of text. The advice is often basic and constrained by time and the type of communication. We believe there is a possibility to increase security further by instructing individuals to perform more advanced cyber security hardening, to become more informed and as a result more aware. A way to achieve this can be through the making of informational videos demonstrating the how's and why's of increasing private cyber security even further and in more detail. This would be beneficial to the broader society, private individuals and companies alike.

The overall goals for the project are:

A. Systematic assessment of the technological level of "the man in the street" (everyone and anyone).

B. Evaluate and find best practice approaches for increasing cyber security resilience of private individuals (given step A)

C. Create a set of informational videos empowering individuals to understand and act to increase their private cyber security.

D. In general, follow an approach that is systematic and repeatable so that videos can be added in the same format (contents, visuals, level of understandability, etc.) later, so that the changing landscape of cyber threats can be addressed similarly in the future.

The steps are of course up for discussion and if there are better methodologies or working steps, we invite the alternatives. (original oppgavetekst mottatt fra IFE)

Det blir vanskeligere og vanskeligere å holde seg trygg i dagens digitale verden. Vi vil derfor hjelpe privatpersoner og bedrifter med å styrke seg digitalt og dermed øke den generelle datasikkerheten.

A. Systematisk vurdering av det teknologiske nivået til "mannen i gata"(alle og enhver).

B. Evaluer og finn tilnærminger for å øke cybersikkerhet hos privatpersoner (gitt trinn A)

C. Lag et sett med informasjonsvideoer som gir enkeltpersoner mulighet til å forstå og handle selvstendig for å øke deres private cybersikkerhet.

D. Ha en systematisk og repeterbar tilnærming slik at videoer kan legges til i samme format (innhold, grafikk, forståelsesnivå osv.) senere, og slik at det skiftende landskapet til cybertrusler kan adresseres på samme måte i fremtiden.

E: Gruppen skal jobbe etter dokumentert metode/metodikk slik at det er mulighet for at andre kan videreføre arbeid i senere fremtid. *(revidert oppdrag etter møter med IFE)*

1.4 Hvorfor, hva og hvordan: Formål, leveranser og metode

1.4.1 Formål

Hovedmål:

- Øke datasikkerhets kompetansen blant privatpersoner

Delmål:

- Gjøre personer oppmerksomme på hva man burde tenke på
- Lage videoer som IFE kan få bruk for etter prosjekttiden
- Skaffe et overblikk over cyber kunnskapen til privatpersoner

1.4.2 Leveranser

Vi skal levere videoer som vi har laget, og jobbe etter en dokumentert metode/metodikk. Både video og framgangsmåte er dokumentert, slik at andre kan følge samme metodikk for å lage videoer ved en annen anledning med nyere data trusler som dukker opp

Nedenfor finnes en tabell av leveransene

Delmål	Beskrivelse av delmål	Ansvarlige	Dato
D1	Prosjektstart	Delt ansvar	12.12.2019
D2	Forprosjektrapport	Delt ansvar	20.01.2020
D3	Første versjon av hoveddokumentet	Delt ansvar	09.03.2020
D4	Andre versjon av hoveddokumentet	Delt ansvar	24.04.2020
D5	Innlevering av Bacheloroppgaven	Delt ansvar	15.05.2020
D6	Presentasjon av Bacheloroppgaven	Delt ansvar	29.05-4.06 2020

Figur 1.4-1. Tabelloversikt av leveranser

1.4.3 Metode

A. Systematisk vurdering av det teknologiske nivået til “mannen i gata”(alle og enhver).

B. Evaluer og finn tilnærminger for å øke cybersikkerhet hos privatpersoner (gitt trinn A)

C. Lag et sett med informasjonsvideoer som gir enkeltpersoner mulighet til å forstå og handle selvstendig for å øke deres private cybersikkerhet.

D. Ha en systematisk og repeterbar tilnærming slik at videoer kan legges til i samme format (innhold, grafikk, forståelsesnivå osv.) senere, og slik at det skiftende landskapet til cybertrusler kan adresseres på samme måte i fremtiden.

E: Gruppen skal jobbe etter dokumentert metode/metodikk slik at det er mulighet for at andre kan videreføre arbeid i senere fremtid.

1.5 Rapportstruktur

Kapittel 2, Analyse:

Analysekapittel som inneholder litt mer om oppgaven, om det finnes noen lignende prosjekter og verktøy som vi skal bruke i oppgaven.

Kapittel 3, Teori:

Relevant teori som handler om samarbeid, datasikkerhet og videoproduksjon.

Kapittel 4, Datainnhenting ved hjelp av spørreundersøkelse:

Omhandler spørreundersøkelsen, hvordan vi lagde den, metoden, hensikten, gjennomføringen og litt diskusjon rundt hva som kunne vært bedre.

Kapittel 5, Datainnhenting ved hjelp av semistrukturert intervju

Omhandler semistrukturert intervju som ble gjennomført for å undersøke hvorfor noen grupper er bedre enn andre.

Kapittel 6, Planlegging:

Her kommer vi til å gå mer i detalj inn på planleggings prosessen vi gjorde før vi begynte på arbeidet, og underveis i arbeidet.

Kapittel 7, Gjennomføring:

Her kommer vi til å gå inn på forarbeidet, hvordan vi har gjennomført selve videoene og etterarbeidet.

Kapittel 8, Evaluering:

Her kommer vi til å snakke om litt om hvordan vi har evaluert effektiviteten av videoene våre, og evaluert arbeidet vårt.

Kapittel 9, Diskusjon

Her kommer vi til å diskutere funnene i prosjektet og forbedringspotensialet til gruppen og prosjektet.

Kapittel 10, Konklusjon

Her kommer vi til å ta for oss resultatet av prosjektet, hva vi har diskutert tidligere i rapporten og ta en generell rask gjennomgang av det vi har presentert i rapporten.

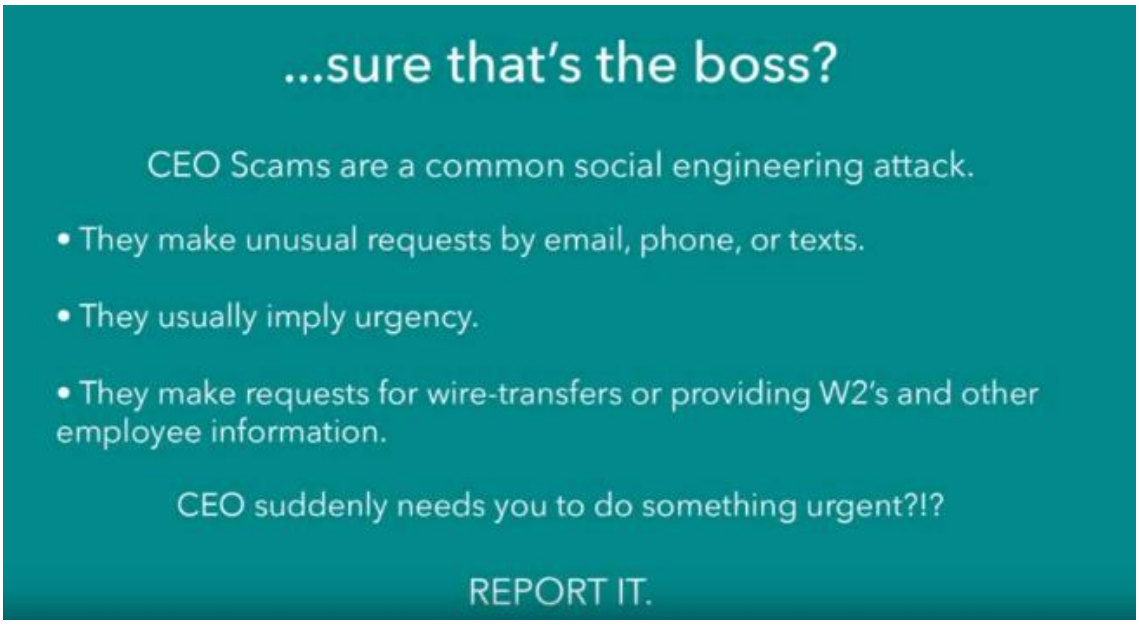
2 Analyse

2.1 Lignende prosjekt:

Et prosjekt som ligner vårt prosjekt, er Nasjonal Sikkerhetsmåned som er holdt av Norsk Senter for Informasjonssikring (NorSIS). Det er et prosjekt som blir holdt i oktober hvert år. Prosjektet inneholde flere moduler som bedriften kan sende ut til sine ansatte, eventuelt elever også om en skole/fylkeskommune bestemmer seg for å være en del av dette. Modulene inneholder videoer som viser hvordan man kan sikre seg mot forskjellige sikkerhetstrusler. På skolen brukes det også skjermer hvor det vises forskjellige videoer og animasjoner som viser ting man burde passe på i forhold til datasikkerhet[2], [3].

Figur 2.1-1 Youtube video om CEO-Scam[4]

[2] *https://www.nosif.no/aktivitet/apning-av-nasjonal-sikkerhetsmaned-2018/*
[3] *https://norsis.no/*

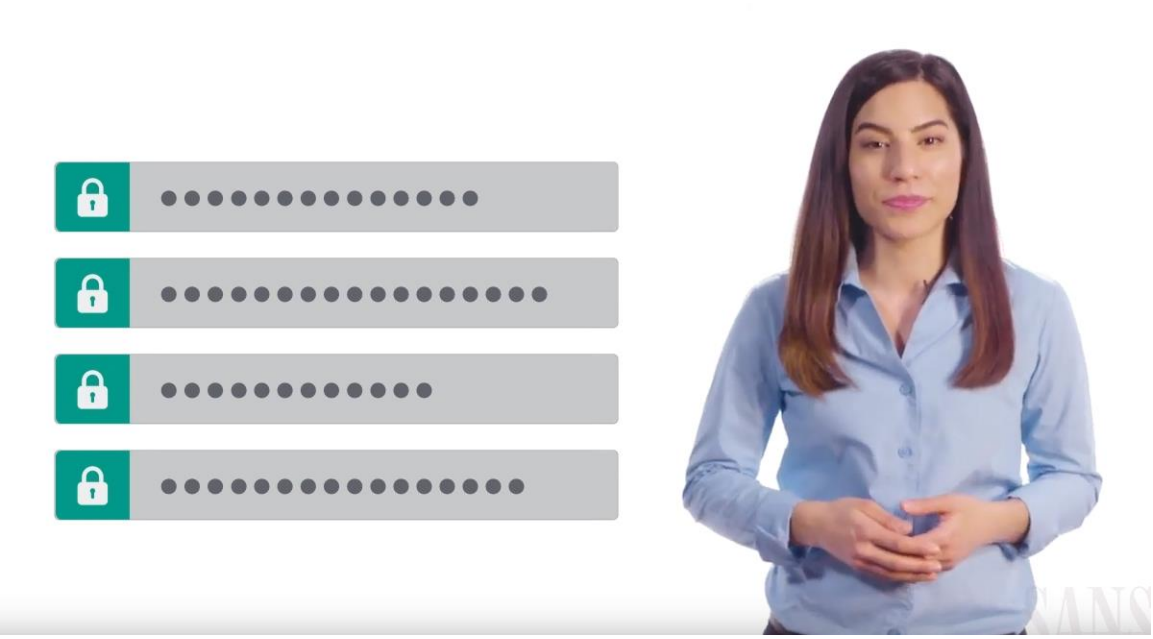


Figur 2.1-2 (Hentet fra Youtube video om CEO-Scam)[4]

Et annet lignende prosjekt er Youtube kanalen Habitu8, hvor de har laget faresituasjoner som man ser i cybersikkerhet som f.eks social engineering, for så å prøve og gjøre noe morsomt ut av det for å trekke til seg folks oppmerksomhet. Samtidig viser de at dette er en reell trussel som ofte blir brukt som taktikk av hackere[4]. De har brukt infotainment for videoene sine. Infotainment er en videosjanger som går ut på å slå sammen informasjonsgivning og underholdning (Entertainment). Figurene 2.1-1 og 2.1-2 er et utdrag fra videoene som Habitu8 har laget som går ut på en social engineering taktikk kalt CEO Scam, hvor man utgir seg for å være sjefen til en annen på mail/telefon eller lignende. Her har de tatt det fra perspektivet til svindleren, hvor vi ser han ringe til en antatt i et selskap. Han introduserer seg selv som sjefen hennes og sier at han trenger at hun overfører 25000 USD til hans konto. Videoen slutter så med en forklaring av det som nettopp skjedde og kjennetegn for det, samt hva man bør gjøre om man tror at man blir utsatt for det[5].

[4] *https://www.youtube.com/channel/UCic3Uwg5OiLQJokATY00zGQ*

[5] *https://www.youtube.com/watch?v=_oqXcx3bRD8*



Figur 2.1-3. "Jan 2020 Passwords: SSA Video of the Month" [6]

Videre er det et selskap som heter SANS Security Awareness. SANS jobber med å lage videoer og systemer for å lære opp mennesker i datasikkerhet og for å gjøre så flere mennesker er klar over farene på nettet og de teknikkene som blir brukt for å lure folk til daglig. De lager mer informative videoer med animasjon eller live-action for å vise hvordan hackere bruker disse teknikkene for å lure folk. Dette gjør at folk kan beskytte seg selv mer fra det ved å vite mer om hvordan de bruker teknikkene mot deg[7]. Figur 2.1-3 viser er fra en av videoene som SANS har laget, som omhandler passord. Her går de gjennom hvorfor det er viktig å ha bra og varierte passord, samt tips for hvordan man lager bra og varierte passord[8].

2.2 Verktøy

Vi brukte Google skjema for å lage vår datasikkerhet quiz. Med Google skjema kan vi som gruppe jobbe samtidig på quizen. Vi brukte rullegardiner, valgspørsmål og beskrivelse som alternativer. Skjema blir automatisk responsiv når det blir opprettet. Det er mulig å hoppe over spørsmål. Det er flere muligheter til å dele dokumentet på, som for eksempel å bygge den inn i et HTML-dokument, epost eller en link direkte.. I dokumentet kan vi se endringer gjort fra gruppe medlemmer og når. Det er også mulig å skrive med andre direkte i dokumentet som blir opprettet. Google skjema er gratis å opprette.

---

[6] https://www.youtube.com/watch?v=gUOnUW7cId4
[7] https://www.sans.org
[8] https://www.youtube.com/watch?v=gUOnUW7cId4

2.2.1 Kommunikasjonsverktøy

For kommunikasjon bruker vi som gruppe flere forskjellige verktøy. Vi bruker Facebook Messenger for å snakke med hverandre daglig om oppgaven og avtale møter mellom oss. Vi bruker Discord for å jobbe snakke sammen mens vi jobber.

Vi bruker en Facebook gruppe for å kunne snakke enkelt med Gunnar(veileder) og avtale møter mellom oss og Gunnar. Vi bruker Slack for å holde kontakt med IFE og sender viktige dokumenter vi vil de skal se over.

Om det er noen på gruppen som av ulike grunner ikke kan delta på et gruppemøte, eller ikke kan delta når vi skal jobbe, så bruker vi Discord/Skype for at personen fortsatt får vært med i jobbingen og at vi ikke skal havne noe bak på grunn av dette.

2.2.2 Redigeringsverktøy

For redigering har vi valgt å bruke Adobe Premiere Pro som hovedprogram da dette er et program et par av oss har litt bakgrunnskunnskap i. I tillegg til det, er det et program som skolen har noen lisenser på. Vi vil også bruke Adobe Audition som er et tilleggsprogram til Adobe Premiere Pro, som ofte brukes for å fjerne støy, eller legge effekter på lyd. I tillegg vil det bli brukt et annet Adobe-program som heter Adobe After Effects for å kunne legge på eventuelle tilleggseffekter. Vi vil også bruke Adobe Photoshop der vi ser at dette er nødvendig.

2.2.3 Filmutstyr

Kamera

Vi har fått låne et Canon EOS C kamera fra skolen. Dette er et kamera som kan ligne veldig på et speilreflekskamera, selv om det er et videokamera. Vi har også brukt webkamera for filming, grunnet skjermopptaksfilming. Da har vi brukt Microsoft lifecam studio. Vi har også brukt det det innebygde webkamera i HP pavilion 14 bf0xx.

Objektiv

Vi har fått låne 2 forskjellige objektiver fra skolen. Det ene objektivet er en Canon EFS 18-135mm linse og det andre er en Canon EFS 10-18 linse.

Mikrofon

Mikrofonen som vi fikk med kameraet er Røde NTG-1 som er en god mikrofon til å fange opp både stemmer, men også et område. Vi har også brukt Steelseries arctis 7 som mikrofon, grunnet at vi har tatt opp skjermopptak med lyd. Det er også brukt den innebygde mikrofonen i HP pavilion 14 bf0xx.

Stativ:

Vi har fått med oss et kamerastativ som fungerer til kameraet, stativet heter Manfrotto MVT502AM og er et fint og enkelt trebent stativ.

Skjermopptak

I filmen har vi tenkt på at det kan være greit å bruke skjermopptak. Til dette har vi valgt å bruke OBS (Open Broadcaster Software). Det er et program til pc som originalt ble utviklet for streamere så man kunne sende forskjellig innhold til streaming plattformer eksempel Twitch, Mixer, Facebook, og Youtube. Dette er et program som lar deg gjøre opptak av hva du vil på pcen din, som gjør at det vil være et enkelt og bra program for vårt bruk.

2.2.4 Storyboard

Verktøyet vi har valgt å bruke for storyboard er verktøyet til StoryboardThat. Dette er en enkel side å lage storyboard på, og en enkel måte å lage storyboard. Det går dessverre ikke an å lagre storyboardet underveis, så storyboardet må være ferdig før man eventuelt gir seg med å lage det. Dette er om man bruker gratis versjonen, man kan velge å gå for en betalingsløsning her også. Denne lar deg lagre, men uten at du eventuelt har flere med betalingsløsningen, er det fortsatt bare én som kan jobbe med storyboardet[9].

2.2.5 Manuskript

Verktøyet vi har valgt å bruke for manus er en nettside som heter studiobinder. Dette er en enkel og ryddig nettside å bruke. Man kan her bare lage ett manus per gratis bruker, og må ellers velge en betalingsløsning. Man vil også kunne lage storyboard her hvis man velger å bruke en betalingsløsning [10].

[9] https://www.storyboardthat.com/education/learn-more-about-classroom-edition
[10] https://app.studiobinder.com/

2.3 Spørreundersøkelsen

Spørreundersøkelsen ble sendt ut til alle studenter og ansatte ved Høgskolen i Østfold, både avdeling Fredrikstad og Halden. Vi valgte å lage en spørreundersøkelse som både består av kvantitativ og kvalitativ, men mest vekt på den kvantitative delen. Vi valgte å legge mest vekt på den kvantitative metoden, på grunn av at vi ønsket å få flest mulig respondenter. Vi hadde ikke hatt tid til å gjøre personlige intervjuer med alle 314 som har svart på spørreundersøkelsen. Alle respondenter i denne spørreundersøkelsen ble anonymisert, slik at respondenter skal være beskyttet i forhold til GDPR.

En lignende spørreundersøkelse til det vi vil undersøke, altså security awareness, fant vi i SANS' "security awareness survey". Det er en kvantitativ undersøkelse, og spør om kunnskapen til den som tar den rundt datasikkerhet, men også hvor oppmerksomme de er rundt datasikkerhet. Undersøkelsen finner også informasjon om misforståelser og feil inntrykk til de som tar undersøkelsen har rundt datasikkerhet[11].

2.4 Bruker spør bruker

I Stange kommune er fokusgruppeintervju, gjennom metoden Bruker Spør Bruker, brukt som en del av kommunens arbeid med å gjennomføre brukerundersøkelser som grunnlag for kvalitetsutvikling av tjenester. Intervjuene ble ledet av 2 brukere med spesiell kompetanse til dette. Det ble gjennomført i alt 9 gruppeintervjuer, hvorav en gruppe fra tjenesteapparatet og resten var brukere. I alt deltok 29 brukere, 8 brukerrepresentanter og 6 representanter fra de ansatte i undersøkelsen. Det ble også avholdt to informasjons- og diskusjonsmøter; ett blant dialogkonferanse der resultatene ble lagt fram og diskutert. Det er senere opprettet et Brukerråd som jobber med videre oppfølging av resultatene. For å gjennomføre intervjuene erfarte man at det var viktig med god informasjon og god tilrettelegging bl.a. i form av tilbud om transport[12].

2.5 Videoer

Vi skal lage videoer for å styrke "mannen på gata" sin datasikkerhetskompetanse. Det skal gjøres gjennom videoer som presenterer nyttig informasjon om datasikkerhet på en selvvalgt måte. Noen måter å strukturere videoer på kan være infotainment med musikk, og prøve og presentere informasjonen til publikum på en morsom måte, hvor det blir brukt mye vitser og overdriving av viktige temaer.

---

[11] https://www.sans.org/sites/default/files/2018-01/security-awareness-survey.pdf

[12] https://www.regjeringen.no/globalassets/upload/krd/kampanjer/ry/fokusgruppeintervju.pdf

2.5.1 Lyd

Lyd på en video blir ofte brukt for å lage en stemning eller for å formidle et budskap.

Musikk:

Musikk i en video kan bli brukt til flere formål. Det mest vanlige er bakgrunnsmusikk for å lage en stemning. Publikummet får da en stemning av hvordan personene i videoen føler seg og hvordan de har det med tanke på følelser.

I de fleste skrekkfilmer blir det ofte lagt til en litt skummel og dyster bakgrunnsmusikk for å skape en skummel stemning som passer til innholdet og sjangeren.

Voiceover:

Mange videoer blir laget uten noe form for lyd. Lyden blir lagt til i form av musikk, voiceover og andre effekter. Voiceover er en stemme/tale som man kan legge over videoen. I stedet for å snakke på filmen, kan man legge på voiceover for at det skal virke som at man snakker på filmen.

I de aller fleste animasjonsfilmene, blir lyden lagt til etter at selve animasjonen er ferdig.

Lydeffekter:

I mange filmer blir det lagt til lydeffekter etter at filmen er spilt inn. Lydeffekter er med på å skape en stemning. Det er ikke alle effekter som blir utført i filmen, derfor blir de lagt til senere.

Lydeffekter som ofte blir lagt til, kan for eksempel være et våpen blir avfyrt i en action film.

2.5.2 Sjanger

«Sjanger, eller genre, er en viss type tekster eller filmer basert på fellestrekk i form, innhold eller funksjon.» (Svennevig, 2019).
«Sjangeren skapes av visse normer og konvensjoner for hvordan tekster skal utformes, og dermed også for hvordan de leses og forstås (også kalt sjangerkrav)» (Svennevig, 2019).

Sjangere er en gruppe krav til hvordan en film, tekst eller annet medie skal være, eller visse ting som en film eller tekst må inneholde. Et eksempel på dette er en musikal, hvor for å passe inn i sjangeren musikal må det valgte mediet inneholde sang som et virkemiddel for å fremme handlingen. Sjangere kan da ha krav til innholdet, men også kommunikasjonsfunksjon. Samtidig kan det være konvensjoner knyttet til mediets form. Eksempler på slike konvensjoner finner man i en skreven artikkel, hvor den må inneholde en introduksjon, hvor man redegjør for hva man skal snakke om, en midtdel hvor man diskuterer hovedpoengene, og til slutt en konklusjon hvor man presenterer hva man kom fram til og det som ble diskutert i midtdelen. Samtidig tilsier sjangeren at disse må komme i en bestemt rekkefølge. Altså må man først ha en introduksjon, deretter midtdelen, og så til slutt en konklusjon. Man kan da ikke ha det i en annen rekkefølge for at det skal være en artikkel. Derimot finnes det undersjangere til artikkel hvor formen og rekkefølgen og mye av konvensjonene endres, men man forholder seg til enkelte overkonvensjoner som man finner i sjangeren artikkel.

En filmsjanger er ofte ikke like normativ som faktabaserte sjangere, men er ofte mer deskriptiv. Likevel inneholder en filmsjanger mange kjennetegn som viser hvilke sjangere en film har basert seg på. Et eksempel på et slikt kjennetegn kan man finne i sjangeren komedie, hvor et godt kjennetegn er at filmen bruker vitser og sarkasme for å få publikum til å le.

Vi har som oppgave å lage relevant videoer innenfor datasikkerheten til "mannen på gaten". Vi føler at en lang film ikke ville dekket alle problemene til disse menneskene og derfor gjør vi undersøkelse på kortfilmer. Filmer i dag som dreier seg om datasikkerhet eller hacking involverer, 1) tøffe damer, 2) tøffe menn, 3) pene mennesker, og sex. Dette er noe vi vil holde oss unna av, fordi filmen/filmene skal ha fokus på læring og ikke underholdning. Vi har som plan å undersøke filmer relatert til datasikkerhet med høy kvalitet og plukke gode elementer fra de, som vi føler kan bli videreført. Filmene våre kan ta i bruk ulike sjangere på hver film dersom budskapet vil bli bedre kommunisert ved å bruke en spesifikk sjanger.

Krim

«Kriminallitteratur, ofte bare kalt krim, er en samlebetegnelse for underholdende, spenningsfylt litteratur om etterforskning og oppklaring av forbrytelser.» (Skei, 2019).

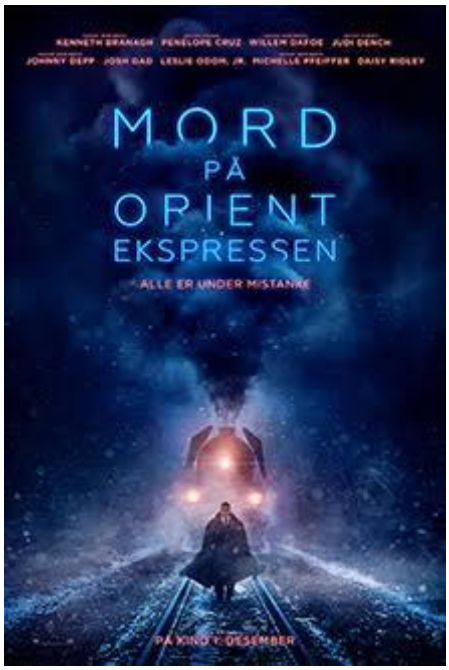
Den norske ordbok definerer kriminalhistorie som en «historie om kriminelle hendelser». Det kan også være en beretning om en kriminelles liv. Krim har mange undersjangere, for eksempel detektivkrim hvor ofte noen har begått drap og handlingen baserer seg rundt en hovedperson som leter etter hint og spor etter den som gjorde det. I en detektivkrim så står mysterie rundt hvem som har begått drapet og selve drapet sentralt i handlingen. Typiske kjennetegn på detektivkrim er at man har en detektiv som prøver å løse noe, et offer, og en kriminell som har begått en kriminell handling mot offeret. hovedpersonen har også ofte en partner som hjelper dem. Videre er et kjennetegn at det er mistenkte, noen som hovedpersonen mistenker at kan ha begått den kriminelle handlingen. (Skei, 2019).

Eksempler på denne type sjanger kan være filmer som:

Figur 2.5-1 (Offisiell plakat laget for filmen Mafia Brødre)

Mafiabrødrene: Er et amerikansk kriminaldrama fra 1990 regissert av Martin Scorsese. Hovedrollene som de tre «mafiabrødrene» spilles av Robert De Niro, Ray Liotta og Joe Pesci. Filmen er basert på en bok av Nicholas Pileggi, som også hadde manus. Mafiabrødre er den klassiske historien om løpegutten som jobber seg oppover mot toppen[13] . Typiske kjennetegn til krim i denne filmen er mord, våpen og mafia virksomhet.

[13] https://no.wikipedia.org/wiki/Mafiabr%C3%B8dre



Figur 2.5-2 (Offisiell plakat for filmen Mord på Orient Ekspressen)

Mord på orient ekspressen: «Tretten personer befinner seg på en overdådig togtur gjennom Europa. Et mord skjer og alle de tretten er mistenkte. Heldigvis befinner Hercule Poirot også seg på dette toget. Klarer han å løse mysteriet før det skjer flere mord?»[14]

Mord på orient ekspressen viser klare tegn til detektiv krim. Man ser her kjennetegn som at hovedkarakteren, Hercule Poirot, bruker logikk og snakker med de mistenkte for å prøve å finne ut hvem som har begått mordet om bord på toget «Orient Ekspressen». Her finner man også et offer, en kriminell som har begått handlingen, her et mord, mistenkte gjennom de andre som er ombord på toget, en partner som hjelper Poirot med å løse mysteriet, og en detektiv, her Hercule Poirot. Mysteriet om hvem som har begått mordet og Poirot som sakte prøver å løse mysterie står sentralt i handlingen.

[14] https://www.filmweb.no/film/article1253773.ece?location=Oslo#22.03.2020

Drama

Drama blir ofte betraktet som det motsatte av en komedie, men kan også betraktes som atskilt fra andre verk av en bred sjanger, for eksempel fantasi. Innen film og TV, er drama en sjanger av narrativ fiksjon (eller semifiksjon) ment å være mer alvorlig enn humoristisk i tone, med fokus på dyptgående utvikling av realistiske karakterer som må forholde seg med realistiske følelsesmessige kamper. Med denne sjangeren kan vi lage filmer som baserer seg på drama i en kritisk situasjon på hvordan man føler seg etter å ha blitt utsatt for dramanagrep.

Typiske kjennetegn er realistiske hovedkarakterer som beskrives og skildres dypt både fysisk og psykisk, som ofte settes i en situasjon hvor de prøves eller er i en form for konflikt, og som utvikler seg som personer gjennom filmen.

Eksempler på denne type film:

Figur 2.5-3 (Offisiell plakat for filmen Forrest Gump)

Forrest Gump

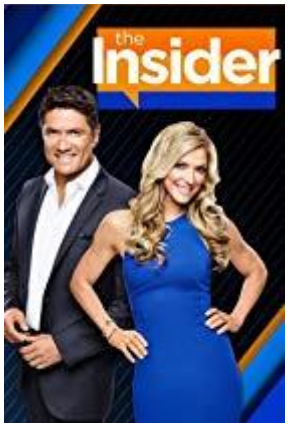
«Filmen handler om en mann med IQ på 75, der han forteller om sin reise gjennom livet, der han møter historiske personer, påvirker populærkulturen og opplever historiske begivenheter uten å være klar over hvor viktige de er på grunn av sin uvanlig lave intelligens.» [15]

Forrest gump viser kjennetegn til drama sjangeren, gjennom å ha en hovedkarakter som er grunnet i virkeligheten, og som finner seg i mange ulike situasjoner gjennom historien som skaper konflikter og prøver han på forskjellige måter, samtidig som at man ser hvordan han utvikler seg fra en ung gutt til en middelmådig man, både fysisk og psykisk.

Infotainment

Er en kombinasjon av informasjon og underholdning, også kalt myke nyheter, er en type medier, vanligvis TV, som gir en kombinasjon av informasjon og underholdning. Begrepet brukes vanligvis avvisende mot mer alvorlige harde nyheter. Infotainment brukes ofte i videoer hvor de vil lære publikum noe samtidig som at de holder oppmerksomheten til publikum i videoen ved å underholde.

Eksempler på denne typer film:



Figur 2.5-4 (Offisiell plakat laget for The Insider)

The Insider: Lager filmer om underholdningsnyheter, som gir dekning av hendelser og kjendiser, intervjuer og innvendige blikk på kommende film- og TV-prosjekter.

[15] https://no.wikipedia.org/wiki/Forrest_Gump

Figur 2.5-5 (Logoen til Habitu8)

Habitu8: Lager morsomme datasikkerhets filmer. De prøver å gjøre deg og firmaet ditt mer sikkert mot hackere. Her kan du lære alt fra passordsikkerhet, sosiale mediesikkerhet, personvern på sosiale medier, sikkerhet for bærbare datamaskiner og mobilenheter og mer.

Oppsummering

Det er altså mange ulike typer sjangere som kan brukes for å lage filmer. Disse sjangeren har ulike typer kjennetegn, fra enkle kjennetegn som bruk av konflikt i drama, til mer spesifikke kjennetegn som at hovedpersonen er detektiv i detektivkrim. For vår oppgave er det nok mest relevant med infotainment, siden vi skal lage videoer som informerer og styrker «mannen på gata» sin forståelse og kompetanse innenfor datasikkerhet. Infotainment passer oppgaven godt siden det går ut på å informere publikum, samtidig som at man prøver å gjøre det på en underholdene måte som holder publikums fokus på videoen, og dermed informasjonen som blir gitt. Samtidig blir videoene også litt krim, siden de handler om kriminelle handlinger som blir gjort mot et offer.

2.5.3 Casting

Original plan:
Vår casting prosess vil være å bruke “mannen på gata” mennesker til de ulike rollene for å få frem autentisiteten i situasjonen med unntak av en sterk hovedrolle som “hackeren”. Alderen til våre karakterer kan ha hvilken som helst alder med unntak av på vår antagonist, fordi “mannen på gata” er deg og meg. Annonsering til å være med på filmen vil bli gjort gjennom Facebook, venner og Hiof epost. Dette er fordi vi ikke søker noen relevant bakgrunn til personen. Personen trenger bare være seg selv.

Etter koronaepidemien:
Dette ble ikke en realitet med tanke på koronaepidemien. Vi valgte å bruke oss selv som skuespillere og en del skjermopptak hvor vi følte at dette var nødvendig.

2.5.4 Location scouting

Opprinnelig plan:
Omgivelsene vi ønsker å fokusere på for antagonisten vår er foran et digitalt medie. Det vil si foran en dataskjerm, tv, på telefonen eller nettbrett. Men de andre karakterene kan befinne seg hvor som helst. De andre karakterene kan befinne seg hvor som helst. Vi vil bruke steder som er offentlig for alle, samt steder som hjemme hos oss eller som vi har tilgang til.

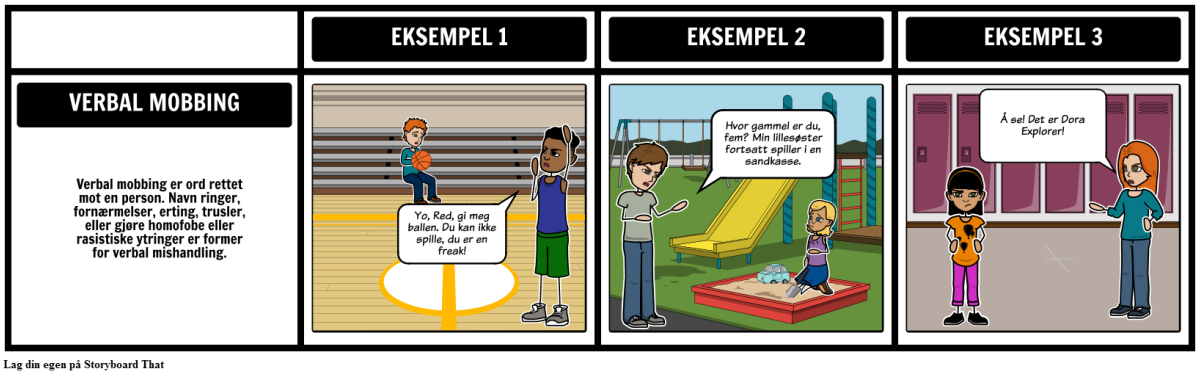
Etter koronaepidemien:
Vi har valgt å bruke noen offentlige lokasjoner, men steder hvor det ikke oppholder seg andre personer. Vi har valgt å bruke skjermopptak som er vår egen pc, slik at vi unngår å være så mye sammen som gruppe med tanke på fare for smitte.

2.5.5 Planlegging

Planlegging er et viktig aspekt av det å lage en video. Det kan være like viktig som filmingen i seg selv, jo bedre filmen er planlagt, desto bedre vil filmingen kunne bli. Det er flere aspekter i planleggingen av filmingen. Dette er «location scouting», casting, manuskript og lignende.

2.5.6 Storyboard

Et storyboard er en viktig ting i forhold til å lage en video. Et storyboard er en visuell presentasjon som en regissør og eventuelt en kameramann lager sammen for å vise hvordan filmen skal bli visuelt når den er ferdig. Hvor grundigere storyboard blir laget, jo bedre vil filmingen av videoen bli. Det vil være fordi at du kan rå klippe videoen før man starter filming, ved å vite hvilke vinkler man skal filme i, samtidig som man vet hvem skuespillere man skulle trenge til filmen.
Et storyboard er som oftest en illustratør, animatør, eller en tegneserietegner[16].



Figur 2.5-6 er et storyboard som handler om verbal mobbing[17]

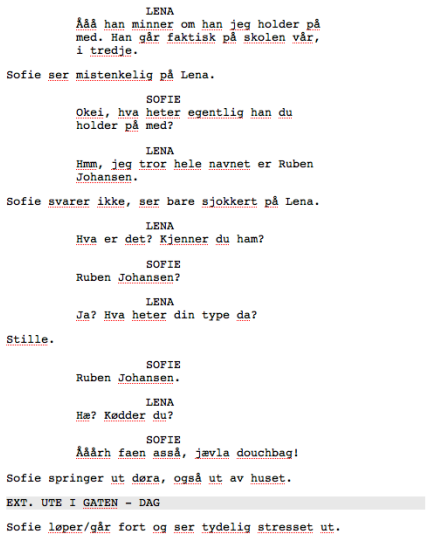
2.5.7 Manus

Et manus er et dokument satt sammen av flere ting som skuespillerne får når de skal jobbe på en film. Manuset vil være satt sammen av replikker (dialoger), og også bevegelser eller hendelser som skal skje i filmen. Manuset er noe av det første som må skrives inn for en film [18].

[16] https://no.wikipedia.org/wiki/Storyboard

[17] https://www.storyboardthat.com/no/storyboards/no-examples/eksempel-pa-verbal-mobbing

[18] https://no.wikipedia.org/wiki/Filmmanus



LENA
Åååå han minner om han jeg holder på med. Han går faktisk på skolen vår, i tredje.

Sofie ser mistenkelig på Lena.

SOFIE
Okei, hva heter egentlig han du holder på med?

LENA
Hmm, jeg tror hele navnet er Ruben Johansen.

Sofie svarer ikke, ser bare sjokkert på Lena.

LENA
Hva er det? Kjenner du ham?

SOFIE
Ruben Johansen?

LENA
Ja? Hva heter din type da?

Stille.

SOFIE
Ruben Johansen.

LENA
Hæ? Kødder du?

SOFIE
Åååårh faen asså, jævla douchbag!

Sofie springer ut døra, også ut av huset.

EXT. UTE I GATEN - DAG

Sofie løper/går fort og ser tydelig stresset ut.

Figur 2.5-7 er et eksempel på et manus[19]

[19] http://eline2mkb.blogspot.com/2013/10/manus-og-storyboard.html

3 Teori

3.1 Samarbeid

Bacheloroppgaven blir løst i gruppe. Det vil si at samarbeid er en meget sentral faktor. For å kunne oppnå de beste mulige resultatene, og i tillegg gjøre det så effektivt som mulig, er det nyttig å lese seg opp på relevant teori. Diverse retningslinjer rundt samarbeid valgte vi å tilegne oss via boken "Management Information Systems". Boken definerer samarbeid som følgende:

"Collaboration is working with others to achieve shared and explicit goals. Collaboration focuses on task or mission accomplishment and usually takes place in a business or other organization and between businesses" (Kenneth C. Laudon, 2018).

I tillegg til å vite hva definisjonen på samarbeid er, vil forskjellige måter å gjøre et samarbeid suksessfullt på være sentralt.

"Successful collaboration requires an appropriate organizational structure and culture along with appropriate collaboration technology" (Kenneth C. Laudon, 2018).

3.1.1 Verktøy for samarbeid

"A collaborative, team-oriented culture won't produce benefits without information systems in place to enable collaboration and social business. Currently there are hundreds of tools designed to deal with the fact that, in order to succeed in our jobs, we are all much dependent on one another, our fellow employees, customers, suppliers and managers." (Kenneth C. Laudon, 2018).

Virtuelle møte systemer er en av de multifunksjonelle systemene som tar over bruken av samarbeid da nåtids samarbeid ikke er mulig (Kenneth C. Laudon, 2018). Innenfor dette feltet finnes det systemer som er tilgjengelig for enhver person, eksempler på disse er Skype, Google+ Hangouts, Zoom. I disse systemene kan de involverte personene snakke sammen samtidig ved at de kan se hverandre.

Skybaserte samarbeidsløsninger som Google Docs og Word/office365 legger til rette for at personene som samarbeider kan opprette og redigere dokumenter selv da de befinner seg på forskjellige lokasjoner.

Bruken av slike systemer vil effektivisere prosessen i et samarbeid ved at involverte personer kan arbeide sammen fra forskjellige lokasjoner. Det vil i tillegg spare bedrifter for eventuelle reiseutgifter (Kenneth C. Laudon, 2018).

3.2 Metode

3.2.1 Kvantitativ metode

> *«Kvantitativ metode er forskningsmetoder som brukes ved innsamling og analyse av kvantitative data. Dette er data som foreligger i form av tall eller andre mengdetermer, i motsetning til kvalitative data, som vanligvis uttrykkes i form av tekst»* (Grønmo, 2014).

En kvantitativ undersøkelses fordeler er lettere behandling av store informasjons/datamengder, ved å bruke diverse statistikk og-presentasjonsverktøy. Data kan bli analysert statistisk, konkretisert i variabler og samvariasjoner. Gruppering av enheter vil bli mer strukturelle, både i analysen og spørreundersøkelsen. Det finnes flere forhold som kan undersøkes i denne oppgaven. Bruk av en kvantitativ metode resulterer at strukturering av analysen og spørreundersøkelsen vil bli mer effektiv. Man unngår også at enkeltindivider blir involvert, som skaper en avstand som gir styrket objektivitet (Jacobsen, 2015).

Kvantitativ metode går ut på å skaffe mindre detaljert informasjon, men i veldig store mengder. Dette kan da brukes ofte for å studere hva virkeligheten er. Ved å for eksempel lage en kvantitativ spørreundersøkelse om mat kan man finne ut hvilken matrett som er mest populær per land, men ikke hvorfor det er sånn.

3.2.2 Kvalitativ metode

> *«Kvalitativ metode er forskningsmetoder som brukes ved innsamling og analyse av kvalitative data. Dette er data som vanligvis foreligger i form av tekst, i motsetning til kvantitative data, som uttrykkes i form av tall eller andre mengdetermer»* (Grønmo, 2009).

Kvalitativ metode går ut på å skape mindre mengder av veldig detaljert informasjon. Her er det viktigere med kvalitet enn kvantitet. Dette brukes ofte for å finne mer ut om hvorfor noe er som det er. For eksempel hvis man vil vite hvorfor noen mennesker liker fårikål mer enn Grandiosa, kan man ta et kvalitativt intervju for å undersøke det og finne mer ut om hvorfor det er sånn.

3.3 Datasikkerhet begreper

3.3.1 Phishing

Phishing er en samlebetegnelse på alle svindelforsøk der målet vil være at personen vil få tak i brukernavn og passord, betalingskort informasjon eller lignende, med å sende ut falske e-poster eller å lage falske nettsider. Mange av disse svindlene blir sendt fra nettsider du kanskje bruker som for eksempel Apple, Facebook, Instagram, eller lignende. Disse mailene inneholder ofte meldinger som *"noen har prøvd å komme seg inn på brukeren din, for å sikre deg for at du ikke skal bli hacket vil vi anbefale at du går inn å bytter passord"* etter dette vil det da ofte være en link til nettsiden hvor du da kan logge inn. Ved å logge inn der gir du da fra deg brukernavn og passord, også blir du sendt til den ekte nettsiden etterpå. En annen veldig vanlig mail å få er for eksempel at du har vunnet en konkurranse, for å motta pengene så må du gi dem kortnummer, pin kode, og cvc nummer til bankkortet ditt (Tom Heine Nätt, 2017).

3.3.2 Sosial engineering

Sosial hacking er når en person finner ut informasjon om deg ved hjelp av sosiale medier (Facebook, LinkedIn, titter, etc.), eller googler opp informasjon, det vil også bli sett på som sosial hacking hvis en person du ikke kjenner ringer deg og ber om eventuell informasjon, for eksempel som *"Hello sir, I come from Microsoft and our systems tells us that your computer systems have been infected with a virus."* Dette er en veldig vanlig måte å gjøre sosial hacking på hvor de vil prøve å få deg til å gi dem tilgang til pc en din. sånn at de kan finne ut informasjon om deg.

3.3.3 Skadevare

Skadelig programvare, ofte kalt skadevare, er en samlebetegnelse på programmer som gjør handlinger med en brukers systemer eller informasjon uten tillatelse fra brukeren. Skadevare betegner mange typer skadelig programvare. Virus, orm, trojaner og spionvare er noen eksempler på slik skadevare (Nätt, 2019).

3.3.4 Virus

Virus kjennetegnes med at hver gang infiserte filer blir åpnet av brukeren eller systemet, senere at den vil spre seg til andre filer den kan finne som ikke allerede er infisert, enten på din maskin eller på tilkoblede lagringsmedier du bruker (nettverksdisker, minnebrikker, osv.) (Tom Heine Nätt, 2017).

3.3.5 Orm

En orm kan minne veldig mye om et virus, men en orm er ikke avhengig av å infisere filer som offeret selv distribuerer. En orm kan distribuere seg selv, den finner ofte egne måter å kontakte nye ofre på, ofte gjennom for eksempel e-post listen koblet til din e-postadresse, venner på sosiale medier, systemets lister over personer du har kontaktet (Tom Heine Nätt, 2017).

3.3.6 Trojaner

Det finnes skadevare som kan se ut som de er andre programmer, dette er skadevare vi kaller for trojanere. Programmet fungerer på samme måte som det egentlig skal, men det vil i tillegg gjøre ting på datamaskinen som man ikke er klar over, og kanskje ikke merker selv. Da trojanere ikke er selv distribuerende, med mindre de er kombinert med en orm eller virus, så vil det måtte trenge menneskelig hjelp for å kunne flytte seg. Dette gjøres ofte via såkalt «social engineering» (sosial hacking) (Tom Heine Nätt, 2017).

3.3.7 Antivirus

Antivirus er et sikkerhetsprogram som skal hjelpe en datamaskin eller mobil med å identifisere, motarbeide og fjerne skadevare, ofte kalt datavirus, samtidig som det skal sikre maskinen mot angrep fra både innsiden og utsiden. Antivirus beskytter maskinen mot skadevare på to måter. Den første metoden antivirus bruker er å skanne maskinen etter kjennetegn til skadevare. Den skanner filer og programmer etter kjente tegn til skadelig oppførsel. Finner den et program som viser kjennetegn til et kjent virus, så vil den prøve å fjerne og nøytralisere programmet før det kan gjøre skade på maskinen. Problemet som oppstår i denne metoden er for at antiviruset skal finne et virus må det gjenkjenne det, altså hvis antiviruset ikke har sett dette viruset før eller lignende virus, så vil det ikke kjenne det igjen, og vil derfor heller ikke stoppe det fra å skade maskinen.

Det er her den andre metoden antivirus bruker kommer inn. Samtidig som den leter etter kjente virus, så følger den med på om noen av programmene på maskinen holder på med skadelig oppførsel. Altså følger antiviruset med på oppførselen til programmene. Prøver et program å for eksempel få tilgang til en sensitiv fil, så vil antiviruset se på det som skadelig oppførsel for så å prøve å stoppe programmet fra å gjøre det. Problemet som oppstår her er at antiviruset kommer med mange falske advarsler, siden den tror mye ikke-skadelig oppførsel er skadelig. Dette fører ofte til at brukeren blir usikker på hvilke programmer de bør godta, og noen godtar da alt, noe som legger systemet åpent for virus. Samtidig så må program startes for at antiviruset skal kunne se at programmet oppfører seg mistenksomt, og da vet man ikke hva viruset kan ha gjort får antiviruset oppdaget skadelig oppførsel (Williams, 2014).

3.3.8 Passordhåndterer

En passordhåndterer eller «password manager», er et program som er laget for å hjelpe brukere med å sikre passordene sine, lage gode passord, samtidig som at de lagrer passordene sikkert så man ikke trenger å huske de selv. En passordhåndterer fungerer litt som en safe, hvor man legger passordene sine inn i safen, og så trenger man en nøkkel, ofte et til passord, for å åpne safen og få tilgang til de lagrede passordene. Den genererer sikre og unike passord for hver av stedene man lager en bruker, og så håndterer den logg inn informasjon for brukeren, og man lager et ekstra passord for å logg inn i passordhåndtereren for å få tilgang til alle brukerne. Dette gjør så man har sikrere passord og ikke trenger å huske de selv. Et problem med dette er at hvis passordet til passordhåndtereren blir stjålet, kan en hacker logge seg inn i den og hackeren vil da få tilgang til alle brukerne som blir håndtert av programmet. (Bakos, 2013)

3.3.9 VPN

VPN står for «Virtual Private Network» og er en type program som lar deg sette opp sikre koblinger over nettet. VPN blir ofte brukt for å komme rundt nettside restriksjoner satt av nettselskapet eller myndigheter. Det brukes også ofte til å skjule nett trafikk fra andres øyne. VPN fungerer ved at programmet setter opp en sikker kobling mellom en server og brukeren sin enhet. Dermed blir serveren som en slags mellom mann for all nett trafikk, noe som lar VPN kryptere all trafikk som går mellom enheten og VPN-et, noe som gjør at ingen andre kan lese nett trafikken.[20]

3.4 Undervisningsteori

3.4.1 Pedagogikk

Pedagogikk er et begrep som omfatter læren om oppdragelse og undervisning. Pedagogikk tar blant annet for seg teknikker som er hensiktsmessige for overføring av kunnskap, verdier og mestringsevne. Man finner hovedsakelig pedagogisk virksomhet innenfor familien og ulike organisasjoner. Her handler det som hovedsak om å forme individer etter verdier og interesser bestemt av en forelder, organisasjon eller annen myndighet.

[20] https://vpnportalen.no/hva-er-vpn

Det er flere ulike tradisjoner og syn på pedagogikk. I antikke Hellas finner man pedagogisk essensialisme, som ble opprinnelig fremstilt av Platon. Kjennetegn på pedagogisk essensialisme er stor vekt på individuelle forskjeller, og at evnen til å ta til seg kunnskap og abstrakt tenking var hierarkisk. Herunder går tanken at ikke alle har evnen til abstrakt kunnskapstilegning, og utdanning skal da tilbys til de som har bestemte evnemessige, sosiale og kulturelle forutsetninger. Utdanning som blir strukturert etter pedagogisk essensialisme kjennetegnes i hovedsak av få fag, hvor idealet er å lære fagene så grundig at det former individets karakter til å ha høy moral og klokskap.

I nesten strakmotsetning til essensialismen finner vi ensyklopedismen. Pedagogisk ensyklopedisme sine hovedtrekk var at alle i et samfunn skulle få utdanning, og utdanning skulle skje med premissene «alle skal lære alt». Utdanningssystemer som følger ensyklopedismen kjennetegnes av læreplaner med mange fag. Dette var også tiltenkt at skulle styrke et demokratisk samfunn. Ved å lære opp alle i alt skulle de ha nok kunnskap til å gjøre et godt valg i et demokratiskvalg. (Tjeldvoll, 2018)

3.4.2 Didaktikk

Didaktikk er et begrep for læren om undervisning. Didaktikk har som fokus innholdet i undervisning. Hva er viktig å lære, hvorfor er det viktig, og hvordan skal kunnskapen formidles og overføres. Det omhandler i hovedsak hvordan man skal forbedre kunnskapen til en som lærer, og da hvilken kunnskap som skal være i fokus. Kunnskap og begreper fra didaktikken skal hjelpe lærere med å begrunne og ta gode valg for undervisningen sin. Det finnes også ulike typer didaktikk, som omhandler mer spesifikke fag, nivåer, alderstrinn og målgrupper. (Sjøberg, 2020)

3.5 Filmteori

Det er flere forskjellige måter å filme en film på, og det vil si at det er mye å tenke på. Skal det brukes skjermopptak? Skal vi filme bare med kamera?

Skal deler av filmingen filmes med kamera som filmer en pc skjerm? Dette er noe av tingene som må tenkes på når man skal filme en film som dette. Alle delene er egentlig riktig, deler med skjermopptak, deler med kamera som filmer personer og som filmer en pc, er en bra måte å kunne få frem budskapet på. Vi vil lage en film som folk på gata kjenner seg igjen i, og dette vil gjøre at vi behøver å sette oss litt i deres situasjon.

Tekniske ting er også viktig å tenke på når man skal filme, som for eksempel rommet du skal filme i er for lyst eller for mørkt? Hvordan skal du sette opp zebra innstillingene på kameraet? Dette er jo ting man ikke kan planlegge, før man eventuelt setter opp kamera på filming lokasjonen. Alt dette vil man jo se på i forhold til hva slags film man skal lage, skal man lage en skrekkfilm så vil det vel kanskje være mer relevant å lage en skremmende effekt ved å filme deler av filmen inne i et mørkt rom.

Hva er det egentlig som gjør en film bra? Jo, det er mange aspekter i det å lage en film som skal bli bra, hvor alt kommer ned til hva slags film man egentlig prøver å lage. For eksempel det å sitte og se på en lang forklaringsdel på 10-15 minutter, er det veldig få som faktisk syntes er interessant å se på. Derimot det å se på en lang dokumentar som varer i oppimot en time, er faktisk noe som folk ser på som interessant, hvorfor er det akkurat sånn? Dette kan det være flere grunner til, en av disse grunnene vil være hva man faktisk ser på skjermen. Det er en stor forskjell på om du sitter og ser på en person som forklarer noe, mot at du sitter og ser på et bilde som beveger seg. da for eksempel et dyr eller noe lignende (kommer an på hva slags dokumentar dette da er snakk om). Andre ting som kan gjøre filmer mere spennende er visuelle effekter, eller lyder/musikk. Dette er noe som fanger seernes oppmerksomhet på en annen måte enn bare hva som blir forklart/hva som blir vist i filmen.

3.6 Konsekvenser

Det å ha god datasikkerhet er en viktig ting i dagens samfunn. Dette kan fort være en enkel jobb for noen, mens for andre kan dette være en vanskelig jobb. Det finnes flere konsekvenser for det å ha dårlig sikkerhet, men alle disse konsekvensene er forskjellige i forhold til hvilken datatrussel som dukker opp. For eksempel om man ikke har totrinnsverifisering, så gjør dette en enklere jobb å eventuelt få kontoene dine hacket. Her kan folk hente ut forskjellig informasjon, som for eksempel på en klient som heter Steam. Steam er et spill klient, hvor man lett kan bytte ting inne på spill mellom brukerkontoer som gjør at totrinnsverifisering er en veldig viktig ting i forhold til datasikkerhet.

En annen veldig vanlig måte for hacking er phising. Dette er en hacker metode som en konsekvens fort kan være tap av kredittkortinformasjon, eller at man oppgir passord og brukernavn til noen andre. Flere konsekvenser er at om du ikke har et antivirus program som fungerer bra på pcen din, så kan du ende opp med å få virus på pcen din. Et virus på pcen din kan komme i mange former, som for eksempel keylogger, en orm som blir sendt videre til andre fra pcen din, og ad virus.

4 Datainnhenting ved hjelp av spørreundersøkelse

Det som er skrevet i dette kapitelet tar utgangspunkt i spørreundersøkelsen som vi sendte ut til studenter ved Høgskolen i Østfold og på Facebook. Spørreundersøkelsen ligger som vedlegg 1, sammen med alle svarene som vi fikk inn. Vi valgte bare å ta med noen av resultatene, som vi følte at vi fikk mest ut av, i denne delen.

4.1 Valg av metode

Prosjektgruppens primære metode i denne oppgaven er en kvantitativ metode. En kvantitativ metode er en undersøkelse som analyserer et stort antall enheter, som i dette tilfellet er kunnskap som mannen på gata har (Dahlum, 2019).

Vi valgte å lage en spørreundersøkelse som både består av kvantitativ og kvalitativ, men mest vekt på den kvantitative delen.. Vi valgte å legge mest vekt på den kvantitative metoden, på grunn av at vi ønsket å få flest mulig respondenter.

4.2 Spørreundersøkelsen

Spørreundersøkelsen ble sendt ut til alle studenter og ansatte ved Høgskolen i Østfold, både avdeling Fredrikstad og Halden. Vi hadde ikke hatt tid til å gjøre personlige intervjuer med alle 314 som har svart på spørreundersøkelsen.

En kvantitativ spørreundersøkelses fordeler er lettere behandling av store informasjons/datamengder, ved å bruke diverse statistikk og-presentasjonsverktøy. Data kan bli analysert statistisk, konkretisert i variabler og samvariasjoner. Gruppering av enheter vil bli mer strukturelle, både i analysen og spørreundersøkelsen. Det finnes flere forhold som kan undersøkes i denne oppgaven. Bruk av en kvantitativ metode resulterer at strukturering av analysen og spørreundersøkelsen vil bli mer effektiv. Man unngår også at enkeltindivider blir involvert, som skaper en avstand som gir styrket objektivitet (Jacobsen, 2015).

4.3 Hensikten med spørreundersøkelsen

Formålet med spørreundersøkelsen var for å finne ut hvor mye kunnskap «mannen på gata» har om datasikkerhet. Grunnen til at vi valgte å sende spørreundersøkelsen både til studentene og ansatte ved Høgskolen i Østfold og på Facebook, var for å treffe flest mulig «mannen på gata». Det blir brukt mye mer digitale medier nå enn det gjorde for en god stund tilbake.

Ved å få respondentene til å svare på generelle spørsmål knyttet til datasikkerhet, vil vi få svar på hvor mye de kan om datasikkerhet. Ved å finne ut kunnskapen til «mannen på gata», kan vi lage mer spesifikke videoer som seerne kan få utnytte av i form av ny kunnskap. Samtidig får vi mer kunnskap om hvilke grupper som står bedre og verre stilt overfor den digitaliserte verdenen vi lever i.

4.4 Respondenter

Spørreundersøkelsen ble sendt ut til alle studenter og ansatte ved Høgskolen i Østfold og til våre venner på Facebook. Respondentene som svarte på mail sendt til HiOF eposten, vil alderen være fra man starter på høgskolen, som er 18/19 og til alderen man er ferdig på høgskolen, altså alt fra 21/22 eller til endt studieløp. Noen kan begynne på høgskolen også i senere alder. Ettersom at spørreundersøkelsen også ble sendt ut på Facebook, vil alderen her være alt fra 13 og opptil 70/80+. Målgruppen vil da være fra 13 og til 70/80+ for å finne kunnskapsnivået til «mannen på gata».

Kunnskapsnivået vil derfor variere veldig. De unge som går på høgskolen nå vil ha kunnskap om generell datasikkerhet, mens de som ikke er vokst opp med digitale medier, vil kanskje ha mindre kunnskap. Spørreundersøkelsen ble også sendt til IT avdelingen på høgskolen, og de vil etter alt å dømme ha bedre kunnskap om datasikkerhet og hvordan man kan sikre seg mot eventuelle angrep. De er de eneste som i utgangspunktet har hatt faget datasikkerhet.

Ettersom at alder -og kunnskapsforskjellen er så stor, føler vi at dette representativt nok for å finne den generelle kunnskapen «mannen på gata» har om datasikkerhet.

4.5 Valg av spørsmål

Vi innledet spørreundersøkelsen med et spørsmål om at personen godtok at vi samlet inn informasjon som ble spurt etter i de neste spørsmålene. Den generelle informasjonen det ble spurt etter, var hva personen jobber med/studerer og alder på personen.

Deretter hadde vi med noen spørsmål om ekte og svindel. Personen fikk opp ett eller flere bilder og skulle da svare om bildet var ekte eller svindel. Vi valgte å ha med slike spørsmål på grunn av at det kan vise oss hva folk ikke hadde kunnskap om. Etter at personen hadde svart om bildet var ekte eller svindel, fikk personen opp et underspørsmål om hvorfor personen mente at bildet var ekte eller svindel. Her hadde vi med et svaralternativ som var at personen selv kunne skrive hva personen tenkte. De fleste ekte eller falsk spørsmålene inneholdt temaet phishing. Phishing er en metode for å samle inn personlig informasjon på.

I den siste delen hadde vi generelle spørsmål om datasikkerhet. Her hadde vi med temaer som forskjellige typer virus, totrinnsverifisering og hvordan man kan forebygge dataangrep.

4.6 Gjennomføring av spørreundersøkelse

Vi brukte Google Form til å lage spørreundersøkelsen. Her kunne vi designe spørreundersøkelsen slik vi ville ha det. Vi valgte å sende ut spørreundersøkelsen til alle studenter og ansatte ved Høgskolen i Østfold, både avdeling Fredrikstad og Halden. Grunnen til at vi sendte den ut til alle studentene og ansatte, var for å få flest mulig svar og en blanding av de forskjellige studieretningene. Spørsmålene ble formulert slik at alle kunne svare på spørsmålene, uansett utdanning og kunnskap.

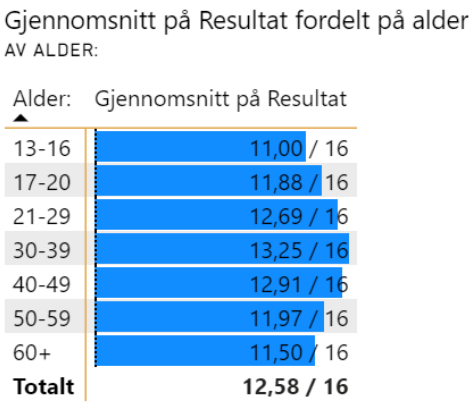
Vi valgte også å legge spørreundersøkelsen ut på Facebook. Grunnen til at vi valgte å legge den ut på Facebook, var for å få spredning i alder, men også kunnskap om datasikkerhet.

Alle respondenter i denne spørreundersøkelsen ble anonymisert, slik at respondenter skal være beskyttet i forhold til GDPR

4.7 Hypoteser

Vi har valgt å lage noen hypoteser knyttet mot datasikkerhets quizzen. Grunnen til at vi valgte å lage hypoteser var for at vi hadde noen teorier om noen av spørsmålene og valgte å finne ut om de stemte eller ikke.

4.7.1 Aldersgruppen 20-29 er den beste på datasikkerhet



Figur 4.7-1. Tabellen viser gjennomsnitt av resultat fordelt på alder

Grunnen til at vi antar 21-29 er de beste på datasikkerhet, er at de er oppvokst med digitale medier og moderne kommunikasjon. Moderne kommunikasjon omhandler alt som har med kommunikasjon over internett å gjøre. I senere tid er det vanlig å bruke sosiale medier blant unge, men også flere og flere voksne bruker det nå for tiden. De som er i aldersgruppen 21-29 kan ha tilegnet seg relevant kunnskap og har/har hatt fag på skolen som omhandler datasikkerhet.

Ut ifra figur 4.7-1 kan man se at det er aldersgruppen 30-39 som er den beste aldersgruppen innenfor datasikkerhet. Etter aldersgruppen 30-39, kommer aldersgruppen 40-49, også kommer 21-19. De som er dårligste på datasikkerhet er aldersgruppen 13-16.

Dette viser at hypotesen ikke stemmer.

Aldersgruppen 21-39 ligger over snittet

Gjennomsnitt på Resultat fordelt på alder
AV ALDER:

Alder:	Gjennomsnitt på Resultat
13-16	11,00 / 16
17-20	11,88 / 16
21-29	12,69 / 16
30-39	13,25 / 16
40-49	12,91 / 16
50-59	11,97 / 16
60+	11,50 / 16
Totalt	**12,58 / 16**

Figur 4.7-2. Tabellen viser gjennomsnitt av resultat fordelt på alder

Grunnen til at personer som er innenfor aldersgruppen 21-39 er over gjennomsnittet, er at de er oppvokst med digitale medier og kan ha tilegnet seg kunnskap ved hjelp av dette. De personene er kanskje nettopp ferdig med studier, som gjør at de har tilegnet seg relevant kunnskap eller så har de jobbet med IT over en viss periode. Denne aldersgruppen er også oppvokst med moderne kommunikasjon, som gjør at de kanskje blir mer oppmerksom angående datasikkerhet.

Ut ifra figuren 4.7-2 kan man se at aldersgruppene 21-29(12,69), 30-39(13,25) og 40-49(12,91) som har gjennomsnittsresultat over snittet på 12,58.

Dette viser at hypotesen stemmer.

4.7.2 De som studerer eller jobber innenfor IT-sektoren er bedre på datasikkerhet

Gjennomsnitt på Resultat fordelt på sektor
AV SEKTOR

Sektor	Gjennomsnitt på Resultat
IT	13,48 / 16
Annet	12,52 / 16
Økonomi	12,07 / 16
Helse	12,02 / 16
Næringsdrift	11,43 / 16
Totalt	**12,59 / 16**

Figur 4.7-3. Tabellen viser gjennomsnitt av resultat fordelt på sektor som ble representert i spørreundersøkelsen

Grunnen til at de som studerer eller jobber innenfor IT er bedre på datasikkerhet, er at de har hatt opplæring av IT programvare. Mange har også hatt om datasikkerhet i løpet av studietiden. Dette gjør at de blir mer oppmerksomme når de surfer rundt på internett. Det at de jobber eller studerer IT, gjør at de har stor forståelse og interesse av datamaskiner og programvare.

Ut ifra figur 4.7-3 kan man se at det er personer innenfor IT sektoren som er de beste innenfor datasikkerhet. Deretter kommer annet, også kommer Økonomi. De dårligste innenfor datasikkerhet er Næringsdrift.

Dette viser at hypotesen stemmer.

Aldersgruppen 30-39 innenfor IT sektoren vet mest om datasikkerhet

Alder:	IT	Totalt
30-39	14,44 / 16	**14,44 / 16**
40-49	13,67 / 16	**13,67 / 16**
50-59	13,60 / 16	**13,60 / 16**
17-20	13,50 / 16	**13,50 / 16**
21-29	13,39 / 16	**13,39 / 16**
60+	10,00 / 16	**10,00 / 16**
Totalt	**13,47 / 16**	**13,47 / 16**

Figur 4.7-4. Tabellen viser gjennomsnitt av resultat innenfor IT sektoren fordelt på alder

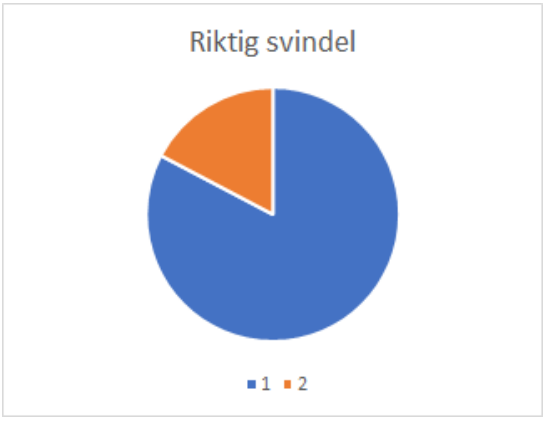
Grunnen til at aldersgruppen 30-39 innenfor IT sektoren vet mest om datasikkerhet, er på grunn av at de har mye erfaring innenfor IT. Noen av personene studerer kanskje IT, mens andre har jobbet innenfor IT sektoren over lenger tid. Ettersom at de har jobbet innenfor IT sektoren over lenger tid, gjør at de har mye erfaring innenfor IT, som igjen handler om datasikkerhet. Noen av personene kan ha blitt utsatt for en type svindel før, og har etter det tilegnet seg mer kunnskap om å beskytte seg selv.

Ut ifra 4.7-4 kan man se at det er aldersgruppen 30-39 som er de beste innenfor datasikkerhet i IT sektoren. Deretter kommer 40-49, også kommer 50-59.

Dette viser at hypotesen stemmer.

4.7.3 Folk er bedre i stand til å se at noe er ekte enn at det er svindel

Figur 4.7-5. Figuren viser svarandel når fasiten er ekte

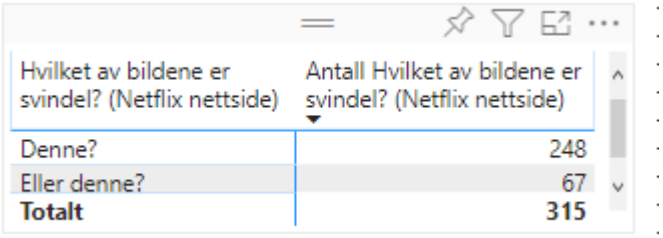


Figur 4.7-6. Figuren viser svarandel når fasiten er svindel

På figur 4.7-5 er den blå fargen riktig svar og oransje farge feil svar. På figur 4.7-6 er den blå fargen riktig svar og oransje farge er feil svar. Folk bruker telefonen/pc mye som gjør at de kommer bort i forskjellig type svindler. Dette gjør at de blir mer oppmerksomme når de surfer rundt på internett. Svindelforsøkene blir raskt delt på sosiale medier for folk fraråder andre til å gjøre en handling. Medier er også flinke til å gjøre folk oppmerksomme på svindler. Noen av spørsmålene ble laget litt enkle, slik at alle skulle ha en mulighet til å svare riktig uten å ha forkunnskaper om datasikkerhet. Ofte kan det være enklere å se om noe er ekte enn at noe er svindel, men svarene som vi har hentet inn fra spørreundersøkelsen viser at folk klarer å avsløre svindel enklere enn ekte.

Dette viser at hypotesen ikke stemmer.

4.7.4 Når de fleste svarer riktig så er det pga. riktig grunn



Hvilket av bildene er svindel? (Netflix nettside)	Antall Hvilket av bildene er svindel? (Netflix nettside)
Denne?	248
Eller denne?	67
Totalt	**315**

Figur 4.7-7. Tabellen viser antall riktige og feil svar på spørsmålet om hvilken av innloggingene til Netflix som var ekte

Ut ifra figur 4.7-7 kan man se at 248 som svarte riktig. Av de 248 som svarte riktig, var det 164 som begrunnet svaret sitt med at man ikke kan logge inn på Netflix med Facebook. Det er noe som faktisk er mulig. Ved å ha to svaralternativer, vil det si at man har 50% sjanse for å svare riktig. Deretter handler det om å begrunne svaret med riktig grunn.

4.8 Oppsummering og konklusjon

Vi har fått inn 314 svar, noe som vi er veldig fornøyde med. Vi sendte spørreundersøkelsen ut til alle studenter og ansatte ved Høgskolen i Østfold og på Facebook.

Ettersom at dette er en datasikkerhets quiz, kan det være at folk er mer skeptiske enn de ville har vært ute på nettet. Her vet de at noe er svindel og noe er ekte, men på nettet så vet de ikke helt sikkert hva som er svindel og hva som er ekte.

Det vi er mest overrasket over, er spørsmålet som handler om meldingen fra Spenst. Her svarte 170 personer at meldingen var svindel og 144 personer svarte at meldingen var ekte. Denne meldingen var ekte og kom fra Spenst. Vi trodde ikke at det var så mange som mente at den meldingen var svindel.

Noe som ikke var så overraskende var at det bare var 1 person som svarte feil på spørsmålet om Facebook melding fra en ukjent. Her var det altså 313 som svarte riktig og 1 person som svarte feil.

Vi er generelt fornøyde med gjennomføringen av spørreundersøkelsen, men vi har fått noen tilbakemeldinger på at noen av bildene var uklare. De bildene som var uklare, var de bildene som vi hadde til noen av alternativene.

Til en annen gang kan det være lurt å ikke ha med bilder i alternativene, men heller lage flere spørsmål hvor bildene blir mer tydelige.

5 Datainnhenting ved hjelp av Semistrukturert intervju

Det som er skrevet i dette kapitelet tar utgangspunkt i intervjuet som vi hadde med fokusgruppen. Intervjuspørsmålene ligger som vedlegg 2, sammen med alle svarene som vi fikk inn. Vi valgte bare å ta med noen av resultatene, som vi følte at vi fikk mest ut av, i denne delen.

5.1 Valg av metode

Vi har valgt å bruke kvalitativ metode for intervjuet. En kvalitativ metode brukes for å analysere kvalitative data. En kvalitativ metode går mer i dybden enn en kvantitativ undersøkelse, som uttrykkes i form av korte setninger eller bare ved få ord. Ved å ha kvalitative intervjuer, kan gruppen få færre svar, men mer utfyllende.

5.2 Gjennomføring av intervjuer

Formålet med intervjuene er å få fokusgruppen vår til å svare på spørsmål knyttet til datasikkerhet for å finne den generelle kunnskapen "mannen på gata" har om datasikkerhet. Dette intervjuet kommer til å foregå i kontrollerte omgivelser. Intervjuet kommer til å bli gitt ut til seks mennesker. Vi valgte fokusgruppen vår basert på jobb og alder, dermed ble det seks forskjellige aldere med hver av dem med en forskjellig jobb. Det som blir notert under intervjuet er svaret vi får, deretter fulgte vi opp med spørsmål rundt hva dem svarer for å mest ut av hvert svar. Før intervjuet begynner så må fokusgruppen fylle ut en avtale om anonymitet. Etter det får de en orientering om intervjuet. Brukeren skal få et innblikk i intervjuprosessen. Etter intervjuet får de tid til å gå over det vi har notert for å få en sjanse til å omformulere, hjelpe oss med å forstå, samt sikre seg at de er enig i det vi har notert. Intervju spørsmålene ble laget i samarbeid med bachelorgruppen, IFE og veileder.

5.3 Valg av spørsmål

Ut ifra de svarene som vi fikk fra den kvantitative spørreundersøkelsen, valgte vi å gjennomføre flere semistrukturerte intervjuer. Det var noen ting som vi følte at vi ikke fikk svar på fra den kvantitative spørreundersøkelsen, og valgte derfor å gjennomføre de semistrukturerte intervjuene.

Første delen handlet om at respondenten skulle vise sine kunnskaper innenfor datasikkerhet. Respondenten skulle for eksempel nevne noen former for hacking, mekanismer/metoder for å forbedre datasikkerheten og hvordan man kan beskytte seg mot dataangrep. Denne delen hadde som mål å oppklare hva som gjorde en gruppe sterkere enn en annen, samtidig som at vi skulle få mer innsikt i hva respondentene forstår som

sikkert, og hva de selv vet om truslene.
Etter den første delen, hadde vi en oppfølgingsdel. I denne delen spurte vi om respondenten for eksempel visste hva totrinnsverifisering er, noen antivirus programmer, og litt om bruk av passord. Dette var også for å oppklare hvor sikre respondentene er digitalt, men vi ønsket å se om respondentene kunne like mye som de ga utrykk for i den forrige delen.
Som avslutning hadde vi med noen generelle spørsmål som handler om koronaepidemien. Her spurte vi om respondenten har arbeidet annerledes etter krisen, og noen programmer som blir brukt mer etter krisen. Vi ønsket å vite litt mer om hvordan den situasjonen som respondentene befinner seg i nå, har endret hvordan de oppfører seg på internett, og som følge av det kan ha oppstått nye trusler.

5.4 Respondenter

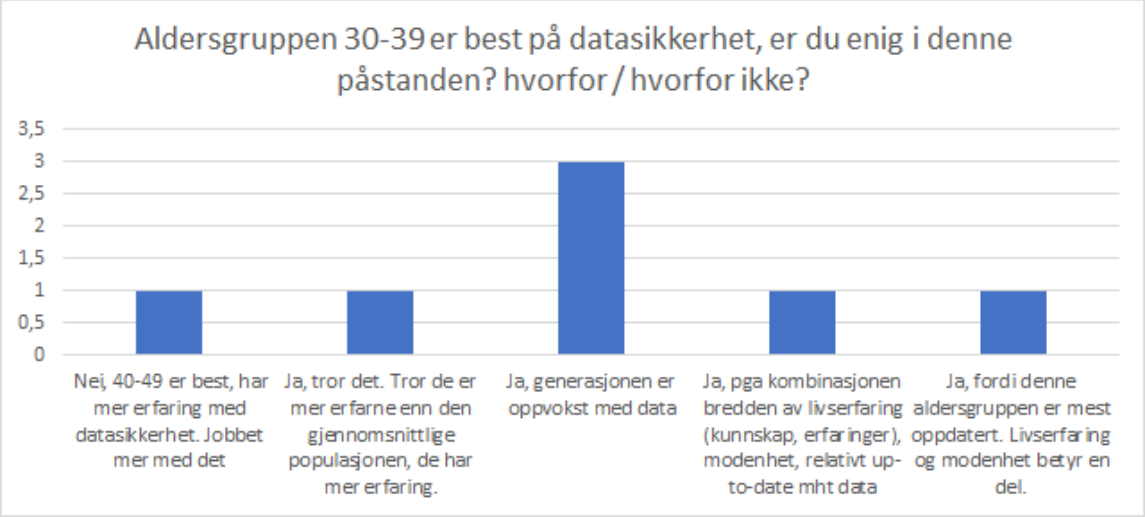
Gruppen sendte ut et dokument som respondenten måtte lese nøye igjennom og godta om de ønsket å bli intervjuet eller ikke. Dokumentet inneholdt rettighetene som respondentene har i forhold til hvordan dataen blir behandlet og anonymitet blant annet. Dokumentet ble sendt ut per epost og fikk svar der.

Respondentene ble valgt ut ifra studieretning/jobbsektor, kjønn og alder. Studieretningene/jobbsektorene som ble representert var IT, logistikk, pensjonist, sykepleier, oberst i militæret og distriktssjef. Alderen som ble representert var fra 21 → 76 år.

5.5 Resultater

Det som er skrevet i kapittel 5.5 tar utgangspunkt i de semistrukturerte intervjuene som vi hadde med fokusgruppen. Alle svarene fra de semistrukturerte intervjuene, ligger som vedlegg 3. Vi valgte bare å ta med noen av resultatene, som vi følte at vi fikk mest ut av, i denne delen.

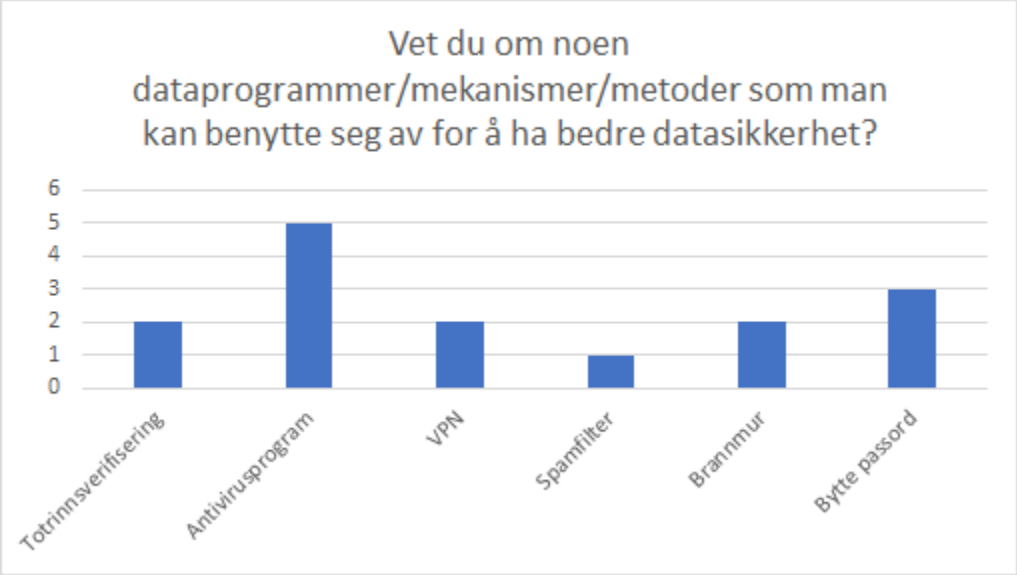
5.5.1 Aldersgruppen 30-39 er best på datasikkerhet, er du enig i denne påstanden? hvorfor / hvorfor ikke?



Figur 5.5-1. Diagrammet viser hva respondentene svarte på spørsmålet om aldersgruppen 30-39 er best på datasikkerhet

Ut ifra figur 5.5.1 kan man se at 6 av totalt 7 personer trodde at det var aldersgruppen 30-39 er best på datasikkerhet, noe som faktisk stemmer. Av de 3 respondentene som svarte Ja, argumenterte de med at aldersgruppen er oppvokst med data. flere mente også at de har mer erfaring innenfor datasikkerhet. Noen mente at det handler om en kombinasjon av erfaring og kunnskap.

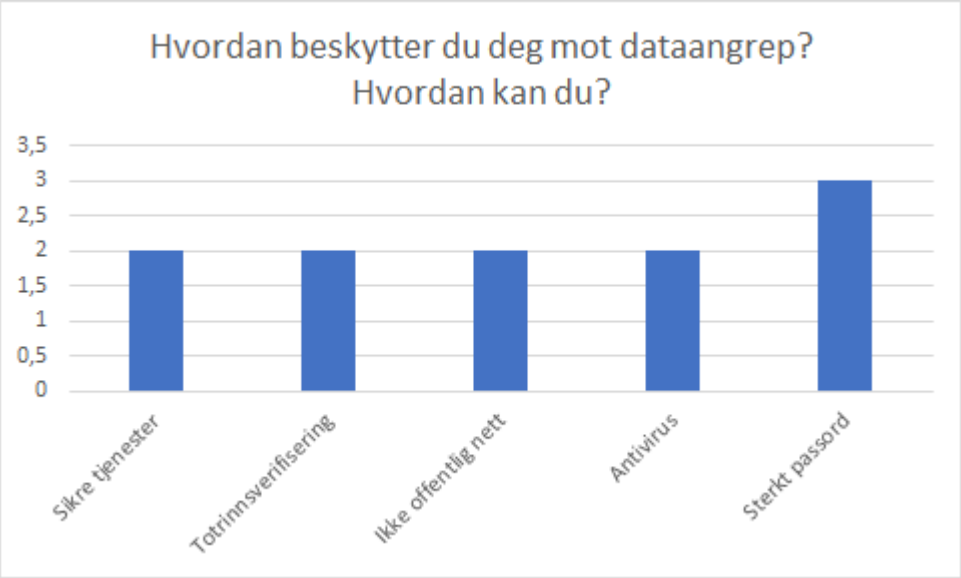
5.5.2 Vet du om noen dataprogrammer/mekanismer/metoder som man kan benytte seg av for å ha bedre datasikkerhet?



Figur 5.5-2. Diagrammet viser hva respondentene svarte på spørsmålet om respondenten vet noen metoder for å ha bedre datasikkerhet

Ut ifra figur 5.5-2 kan man se at flesteparten mener at antivirus program er det viktigste for datasikkerheten din. To nevnte ulike metoder som å sette opp vpn og bruke brannmur dette er veldig bra. Bytting av passord er også et bra svar selv om mange sier de sjeldent bytter passordene sine og vanligvis bruker samme passord på flere steder. Det var også to personer som nevnte totrinnsverifisering, som er en smart mekanisme som kan hindre folk i å hacke andre. Andre ting som også ble nevnt er å dobbeltsjekke eposter som mottas, unngå potensielt farlige nettsider, bruke et operativsystem som er velkjent, bruke en nettleser som støtter funksjoner når ting ikke er kryptert, og vite hvordan tjenester som blir brukt behandler dataen som blir innhentet.

5.5.3 Hvordan beskytter du deg mot dataangrep? Hvordan kan du?



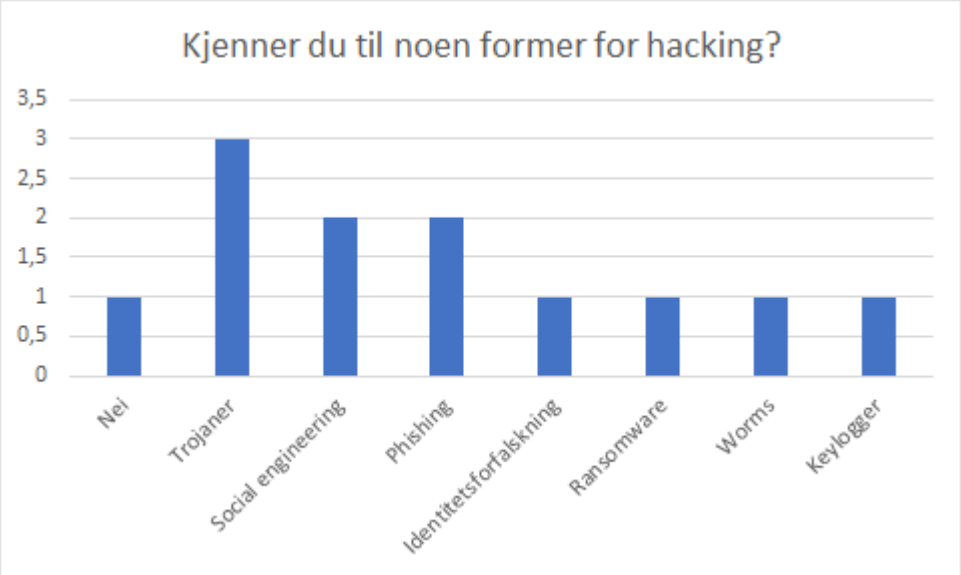
Figur 5.5-3. Diagrammet viser hva respondenten svarte på spørsmålet om hvordan man kan beskytte seg mot dataangrep

Her spurte vi om hvordan du beskytter deg mot dataangrep og hvordan det er mulig.

Ut ifra figur 5.5-3 kan man se at de fleste svarte at de benytter seg av tjenester som VPN, brannmur, antivirus programmer, totrinnsverifisering, viktig å ha et bra passord, være varsom på mail, unngå å bruke offentlig wifi, og holde seg unna nettsider som potensielt kan være farlige. Andre svarte at de holder maskinvare oppdatert, selektiv med personlig informasjon, og prøver å holde seg til få plattformer som mulig.

Ingen av respondentene svarte at dobbeltsjekke ting man skal laste ned kan være lurt, ikke åpne linker man får fra personer som man ikke stoler på, og for mye personlig informasjon ute på internett. Dette er ting som respondentene kunne svart.

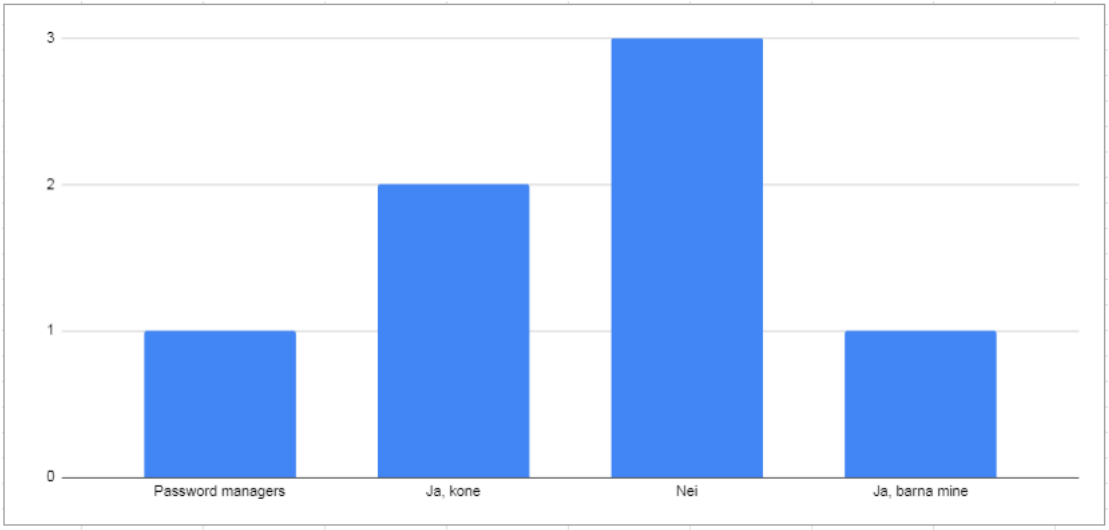
5.5.4 Kjenner du til noen former for hacking?



Figur 5.5-4. Diagrammet viser hva respondenten svarte på spørsmålet om respondenten kjenner til noen former for hacking

Ut ifra figur 5.5-4 kan man se at de fleste svarte at de har hørt om trojanere, social engineering, og phishing. Noen nevnte at de har hørt om ransomware, worms og identitetsforfalskning. En nevnte at han har hørt om keylogger, ddos angrep, og cross site scripting, og varsom ved å benytte seg av offentlig wifi. En person kunne ikke nevne noen former for hacking.

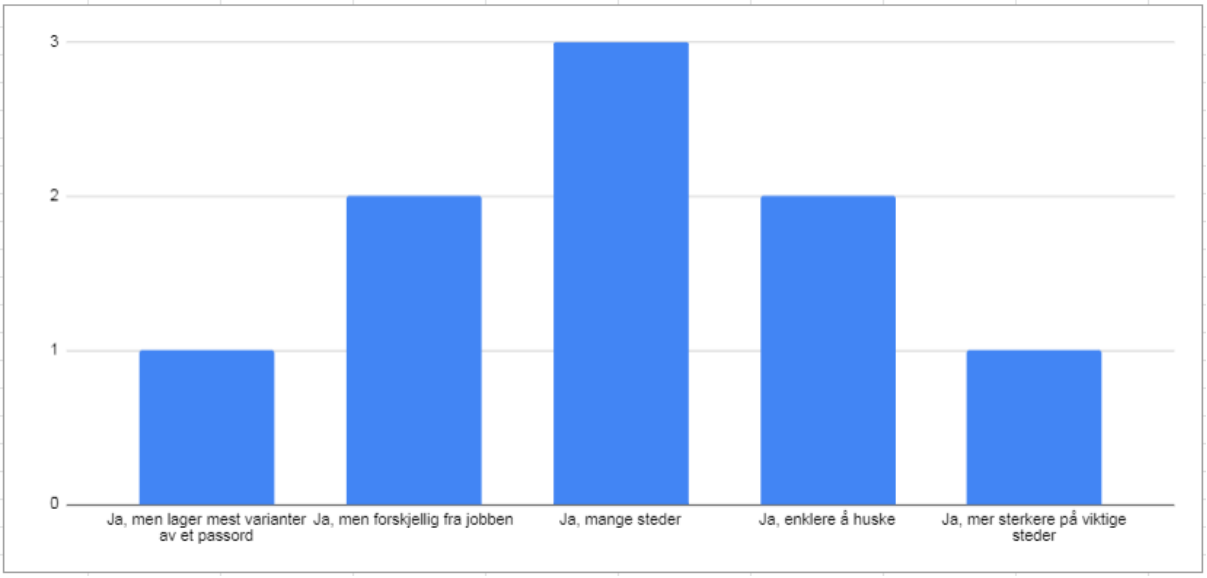
5.5.5 Kjenner flere enn deg passordet/passordene dine?



Figur 5.5-5. Diagrammet viser hva respondenten svarte på spørsmålet om flere enn respondenten kjenner til passordet

Ut ifra figur 5.5-5 svarte tre personer at ingen andre enn dere selv vet om passordene som de bruker. Et par svarte at konen vet passordet noen steder, for da kan det bli enklere å huske til neste gang passordet blir brukt. En person svarte at barna til personen vet passordet/passordene. En annen person svarte nei på spørsmålet, men at password manager kan vite passordet, på grunn av at passordet blir lagret der.

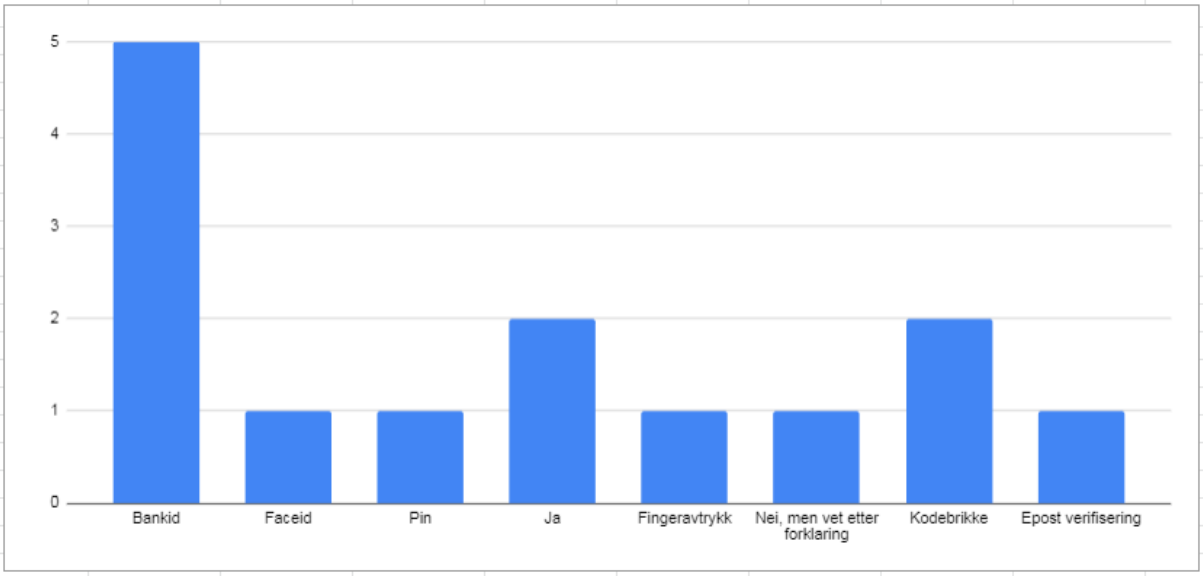
5.5.6 Bruker du samme passord flere steder?



Figur 5.5-6. Diagrammet viser hva respondenten svarte på spørsmålet om respondenten bruker samme passord flere steder

Ut ifra figur 5.5-6 kan man se at alle respondentene svarte at de bruker samme passord flere steder, men av forskjellige grunner. Noen mener at passordet blir enklere å huske hvis det blir brukt flere steder, andre mener at det er viktig å skille private passord fra passord som blir brukt på jobben, at det er viktig med sterkt passord på viktigere steder, og at man bruker «samme» passord, bare med forskjellige varianter

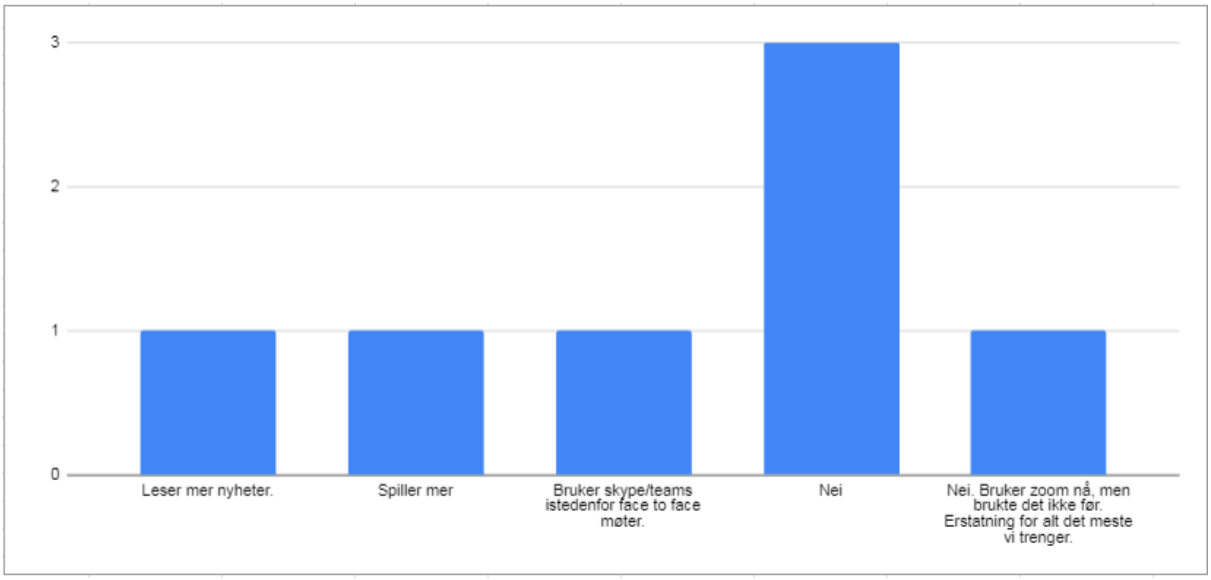
5.5.7 Kjenner du til noen former for totrinnsverifisering? Hvilke?



Figur 5.5-7. Diagrammet viser hva respondenten svarte på spørsmålet om respondenten kjenner til noen former for totrinnsverifisering

Ut ifra figur 5.5-7 kan man se at de fleste nevnte at de vet om/bruker bankID som totrinnsverifisering. Av de fem personene som svarte bankID, var det tre av personene som bruker det når de skal logge seg inn i banken. Det var to personer som svarte at de vet hva totrinnsverifisering er, uten å utdype det mer. Det var to personer som svarte kodebrikke, begge svarte at de bruker det for innlogging i banken. En person svarte at det er flere variasjoner, som for eksempel bankID på mobil + pin, bankID + pin og faceID + pin.

5.5.8 Bruker du noen programmer mer etter krisen?



Figur 5.5-8. Diagrammet viser hva respondenten svarte på spørsmålet om respondenten bruker noen programmer mer etter koronaepidemien

Ut ifra figur 5.5-8 kan man se at under Corona epidemien så blir det mer bruk av Skype/Teams/Zoom (programvarer hvor du kan se og høre på andre digitalt) ettersom helsevesenet har sagt vi ikke burde være i nærheten av hverandre. En sa hun spiller mer ettersom det ikke er jobb. En annen leser på nyheter ettersom hun vil holde deg oppdatert på koronaepidemien.

5.6 Oppsummering og konklusjon

Ut ifra de semistrukturerte intervjuene fikk vi vite litt om hva respondentene kan og ikke kan om datasikkerhet.

I spørsmålet om ulike mekanismer og metoder de kan bruke til å forbedre datasikkerheten sin svarte de disse metodene og programvarene: Totrinnsverifisering, antivirus, vpn, spamfiltre, brannmur og bytte passord ofte. Dette viser at de kan simple ting for å forbedre datasikkerheten sin.

I intervjuene våre sa de at de kan beskytte seg mot dataangrep med dette; Totrinnsverifisering, sikre ulike tjenester, bruke antivirus, ha et sterkt passord og ikke bruke offentlig nettverk. De svarene er bra og viser noen kunnskap på hvordan de kan beskytte seg mot dataangrep. På offentlig nettverk er du ikke eier og personen som har satt det opp kan ha tullet med koblingen og kan lese all trafikk som går igjennom det. Dermed er dine personlige opplysninger utsatt. Dersom du må bruke offentlig nettverk er det tryggere med bruk av vpn fordi trafikken din da blir kryptert av vpn-et.

Et spamfilter er et smart program som håndterer uønsket epost og forhindrer at disse meldingene kommer i innboksen din. En brannmur overvåker og styrer hvem som får tilgang til nettverket og pcen din. En sikker datamaskin burde ha sterke brannmur restriksjoner for å hindre uønsket tilgang. Antivirus er også et viktig program ettersom det identifiserer og fjerner virus og skadevare på datamaskinen din. Dette er da viktig å bruke på datamaskinen og andre enheter. I følge Dataprot så har bare halvparten av mobilbrukere et antivirus på mobilen sin, samt at mer en halvparten av Windows 7 maskiner ikke har antivirus beskyttelse i det hele tatt[21]. Dette vil da si at mer enn halvparten av enheter ikke har noe form for virusbeskyttelse og står da åpen for angrep. Faren er da at disse enhetene kan bli brukt til å spre virus videre. Dataprot viser også at 55% av all programvare ikke er oppdatert mot virus[22]. Å ikke oppdatere maskin og apper er en stor trussel for angrep ettersom oppdateringer fjerner og løser sikkerhetshull gjennom oppdateringer

Med totrinnsverifisering er kontoen din veldig sterk. En hacker vil ikke få tilgang til en konto selv om de har brukerinformasjonen dersom man bruker en totrinnsverifisering, ettersom hackeren trenger brukerens engangskode til innlogging.

Det som kanskje var mest overraskende er at så mange som 6 av respondentene bruker passordet sitt flere steder. Noen skriver at de har det samme passordet, bare i forskjellige varianter. Konsekvensen av å bruke samme passord flere steder er at hvis du blir hacket får hackeren tilgang flere steder. Man kan si det er å gi en nøkkel som låser opp alle dører.

«Mannen på gata» sitt nivå ligger der hvor de fleste enkle angrep blir stoppet av de sikkerhetsgrunnlagene som har blitt lagt rundt dem, samtidig som at noen av de blir stoppet av skeptisisme. Derimot viste respondentene at mindre enn halvparten av de visste kjennetegn for angrep eller hvordan man skal skille angrepsforsøk og vanlig kommunikasjon. Samtidig var det nesten ingen som nevnte dokumenter eller åpning av filer som en fare.

[21] https://dataprot.net/statistics/antivirus-statistics/
[22] https://dataprot.net/statistics/antivirus-statistics/

Fra intervjuene viser det seg at «mannen på gata» ikke sikrer seg mot mer fysiske angrep som usb angrep. Dette er urovekkende siden det åpner «mannen på gata» eller med andre ord, folk flest, til angrep i form av usb og dokumenter sendt til dem på mail eller programmer de laster ned. Samtidig åpner det for at de ikke kjenner igjen et angrepsforsøk som kan gjøre at de blir lurt av et slikt forsøk. Dette styrker opp nødvendigheten i å lære opp «mannen på gata» og styrke deres egen evne til å beskytte seg selv, spesielt siden de da står dårlig stilt til å beskytte seg selv mot angrep når beskyttelsesgrunnlaget som er bygget opp rundt dem svikter.

6 Planlegging

6.1 Innledning

Etter gjennomgang av intervjurunde og spørreundersøkelse har vi fått et klarere innblikk i nivået til «mannen på gata», og de farene de står overfor. Vi ser nå at «mannen på gata» har bygget opp noe kunnskap rundt det datasikkerhetsgrunnlaget som er bygget opp for å beskytte de, samt at de bruker dette grunnlaget som hjelp for dem. Derimot, ser vi også at «mannen på gata» har manglende kunnskap rundt selvbeskyttelse som hvordan man kan skille angrep fra vanlig kommunikasjon, samt en misforståelse rundt at man i hovedsak er under angrep over nettet. Dette hindrer de fra å beskytte seg mot mer fysiske usb angrep og såkalt «social engginering», samt angrep som kommer gjennom beskyttelsesgrunnlaget som nye epost og nettsidesvindel, eller virus som ikke har blitt laget beskyttelse mot enda.

Vi ser da igjen nødvendigheten i dette prosjektet. Vi endrer planleggingen vår til å rette seg mot mannen på gata og situasjoner de finner seg i, og mer dirkete angrep for å vise viktigheten med å kunne beskytte seg selv når beskyttelsen rundt svikter. Vi vil styrke «mannen på gata» ved å gi de kunnskap til å skille mellom angrep og vanlig kommunikasjon, samt gjøre de mer kjent med fysiske angrep som usb, og filangrep.

6.2 Location Scouting

På location scouting handler om det å finne steder som egner seg for å filme. Det er viktig å tenke på hvilke lokasjoner som skal være med i filmene. Forskjellige miljøer kan skape forskjellig stemning. Dette er mulige lokasjoner som vi kan ha med i filmene.

Her har gruppen kjørt rundt til forskjellige lokasjoner i Halden for å finne passende steder å filme. Foreløpig har vi bare kjørt rundt i Halden, men har også vurdert å kjøre en tur til Fredrikstad.

Etter alt som har skjedd med koronaepidemien, har noen av lokasjonene blitt valgt bort. Grunnen til dette er at vi setter helsen vår og til husstanden først.

Figur 6.2-1. Et bilde av en bil som står på en parkeringsplass

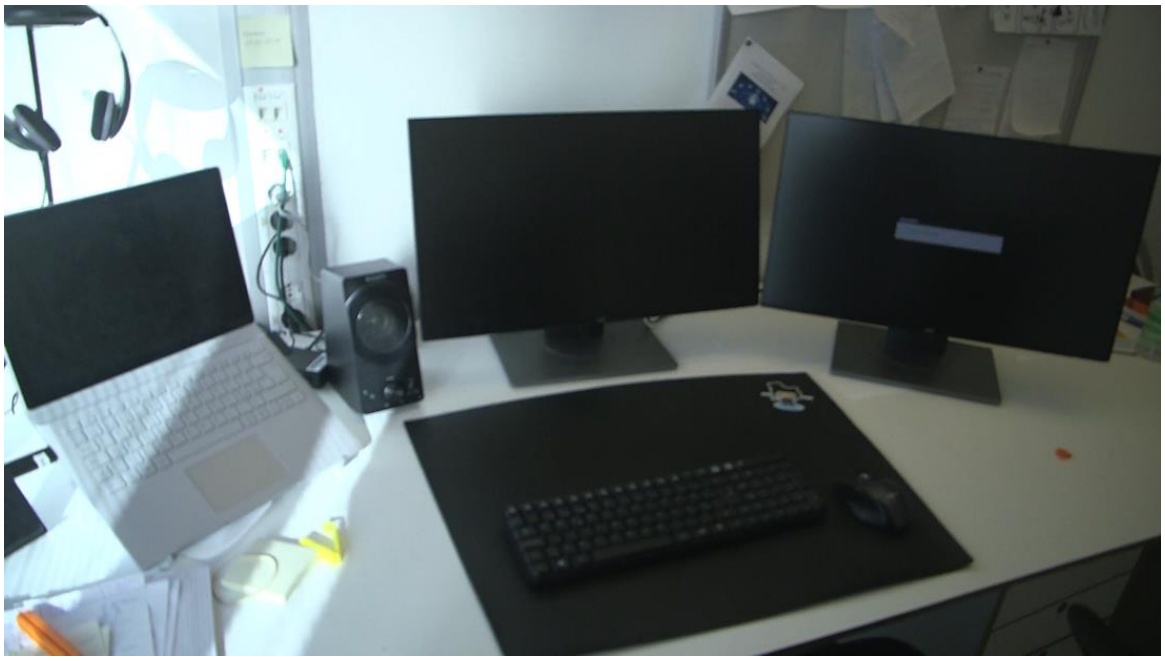
Figur 6.2-1 er et bilde av en bil. Det vi har tenkt er at vi kan filme i bilen hvis vi har tenkt til å bytte lokasjon i løpet av filmen. I bilen kan vi da ha korte samtaler mens vi forflytter oss til en annen lokasjon. Vi ser da etter en lokasjon som lar oss filme og simulere større avstander, samtidig som at det kan brukes for å bygge opp situasjoner som at en karakter som kjører andre fra et sted til et annet.

Figur 6.2-2. Et bilde av noen trær på en gresslette

Figur 6.2-2 er det et bilde av en gresslette med trær og litt ulent terreng. Bildet er tatt utenfor Fredriksten kro på Fredriksten festning. Det vi har sett etter her er et «park»-område som kan brukes for filming om litt diskre eller mistenksomme møter ute, hvor hacker kan møte en annen hacker, eller lignende. Samtidig ville vi ha et sted hvor vi kunne filme at et offer møter hacker. Den tredje tingen vi så etter var et sted hvor vi kunne ha litt mer rolige situasjoner slik som venner i en park, skolelever, og telefonbruk ute. Skogen ved festningen på utsiden av Fredriksten kro passet godt til alle tingene, siden det er stille, noe som betyr at det vil være enkelt å filme der, samtidig som at det er mulig å simulere en bakgård av en skole og en park der.

Figur 6.2-3. Et bilde av stuen i en leilighet

Figur 6.2-3 er et bilde av stuen hjemme hos en av gruppemedlemmene. Her ønsket vi et rom for å kunne simulere et vanlig hjem, for å vise at alle kan bli utsatt for svindel og hacking. Vi ønsket da et rom som var ganske normalt, samtidig som at det var stort nok til å kunne simulere et hjem for både yngre studenter, samt eldre mennesker og evt. en familie. Dette rommet oppfylte disse kriteriene siden det er god størrelse på det, uten at det er for stort til å kunne simulere et studenthjem.



Figur 6.2-4. Et bilde av et kontor hvor en hacker kan sitte

Figur 6.2-4 er et bilde av kontoret til en av våre lærere. Dette kontoret skulle fylle rollen av lokasjon for hackeren. Vi valgte dette kontoret for det, siden det hjelper med å få hackeren til å virke teknologisk avansert og erfaren, siden skrivebordet fremstår profesjonelt, samtidig som det blir brukt innenfor profesjonell informasjonsteknologi arbeid. Samtidig kunne kontoret bli brukt til å simulere et kontor kompleks, for å vise til hacking og datasikkerhetstrusler i et arbeidsområde.

Figur 6.2-5. Et bilde av en bil som står parkert utenfor en skole

Figur 6.2-5 er et bilde av en bil som står parkert utenfor en skolegård. Bildet er tatt utenfor Folkvang skole, som nå er Os skole. Denne lokasjonen var tiltenkt bruk for å filme en ung karakter som går på skole. Dette er for å vise at yngre også blir utsatt for datasikkerhetstrusler som kan ha effekt på barnet og de som er ansvarlige for dem. Samtidig vil det gi fyll til å vise at en karakter gjør noe og tiden går, før offer får tilbakemelding om hacking,

Figur 6.2-6. Et bilde av en videregående skole

Figur 6.2-6 er et bilde av samme bilen utenfor en skole. Skolen som er avbildet er Halden videregående skole, avdeling Porsnes. Denne lokasjonen var tiltenkt lignende som i figur 7.1-5, at en eldre karakter kan ta med en yngre karakter til skolen, men her for eldre mennesker, i aldersgruppen 16-19. Vi ville også ha et område som viser et bygg som kan simulere et kontorbygg. Det fant vi her, siden det er en skole samtidig som at det er stort nok til å simulere et kontor for et middelmådig til større selskap.

Figur 6.2-7. Et bilde av en korridor i en av studentblokkene på HIOF

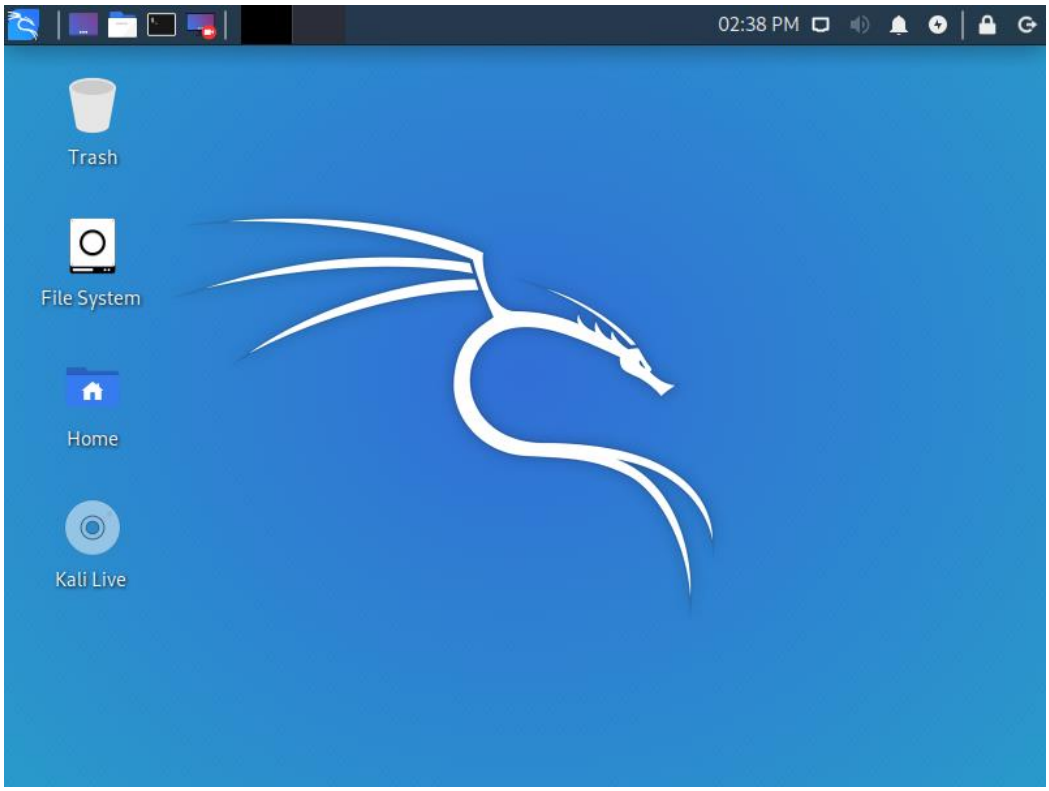
Figur 6.2-7 er det et bilde av en korridor. Korridoren er i en av studentblokkene på HIOF hvor en av gruppemedlemmene bor. Her kan for eksempel en gruppe personer bli filmet mens de går igjennom korridoren. Denne lokasjonen oppfylte ønsket vårt om å kunne filme og simulere en gruppe studenter i et kollektiv. Lokasjonen trengte å være stille nok til å filme, samtidig som at det var stort nok til å vise at tiden går, mens studenter går nedover gangen, samtidig som en annen student blir offer for et hackingsforsøk.

Figur 6.2-8. Et bilde av et kontor hvor en hacker kan sitte

Figur 6.2-8 er et bilde av kontoret til et av gruppemedlemmene. Denne lokasjonen ble brukt i vår USB video. Vi ville ha en lokasjon hvor vi kunne simulere rommet til en student, som kunne bli et offer for en svindel eller datasikkerhetstrussel. Samtidig ville vi ha en alternativ lokasjon for filming av hacker som gjør ting på en maskin. Dette er grunnet at vi ikke kunne være sikker på at vi alltid kunne låne kontoret til en lærer på skolen for det. Dette passet godt siden det er eid av en i gruppen, noe som ville si at vi alltid hadde tilgang til lokasjonen.

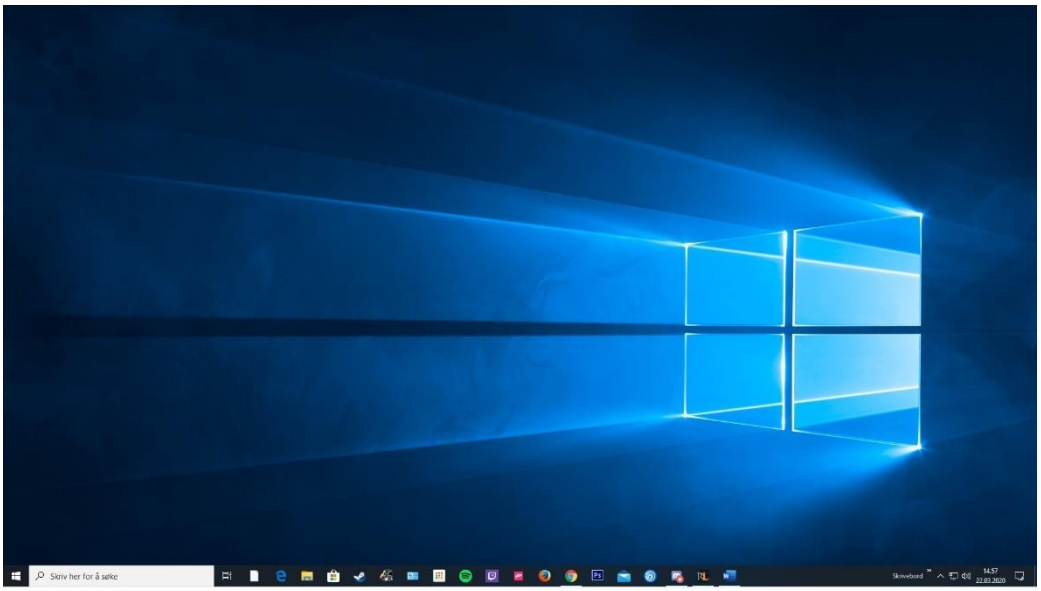
Figur 6.2-9. Et bilde av biler som står parkert på en parkeringsplass

Figur 6.2-9 er det et bilde av en parkeringsplass. Parkeringsplassen som er tatt bilde av her er ansattparkeringen på HIOF. Denne lokasjonen skulle vi bruke til parkering ved et kontorbygg, for å simulere at vi flytter oss store distanser i videoene. Samtidig var det for en av situasjonene vi opprinnelig ville bruke, hvor en far kjører familien til kontor og skole, hvor dette da ville bli brukt for å kjøre til kontor.



Figur 6.2-10. Et bilde av Kali Linux operativsystem

Figur 6.2-10 er et skjermbilde av Kali Linux operativsystem. Dette er et program som er kjent for bruk av hacking og andre datatrusler. Vi ville ikke simulere for mye av hackingen og truslene, siden vi ville at de skulle virke så ekte som mulig. For å oppnå det så ville vi bruke kali for å vise hackingen nærmere slik det faktisk er, også da for å beholde en følelse av virkeligheten i videoene. Det ville da bli brukt gjennom filming av skjermen med et eksternt kamera, for eksempel bak hackeren, samtidig som å filme skjermen med programmer på maskinen. Etter koronaepidemien begynte ble dette også mer relevant siden vi flyttet oss mer mot filming av skjermen og filming gjennom webkamera, lignende en videosamtale, for å sikre oss i gruppen mot coronaviruset, samtidig som vi får en video som var nærmere den situasjonen folk flest fant seg i etter hyppigere hjemmekontor som ble en konsekvens av koronaepidemien



Figur 6.2-11. Et bilde av Windows 10 operativsystem

Figur 6.2-11 er bilde av et Windows operativsystem. Her ville vi ta opptak av skjermen lignende det som er beskrevet over. Dette ble også brukt i video 1 om phishing, hvor vi filmer skjermen for å vise at et offer blir lurt av en epost som blir sendt til de, samtidig som at vi brukte filming av skjerm for å lettere forklare hva i eposten man bør se etter for å se om det er svindel eller ikke. Vi ville også kunne filme med eksternt kamera, som i video 2 om usb, for å vise at et offer blir lurt.

6.3 Casting

Casting handler om hvem som skal være med i de forskjellige videoene. Dette kan være alt fra skuespillere til statister. Statister er personer som ikke har en rolle med særlig stor betydning. Etter semistrukturert intervju og spørreundersøkelse har vi fått vite mer om hvilke grupper som sliter mest med datasikkerhet, hvorfor de sliter mer, og hva de sliter med. Vi vet nå at det de blir mye utsatt for, samt sliter med, er phishing forsøk, og da epost og nettside svindel. Videre vet vi nå at aldersgruppen 30-39 står best stilt mot datasikkerhetstrusler. Vi vil da prøve å finne cast i variert aldersgruppe, også den som står best stilt, for å best treffe «mannen på gata». Vi trenger en regissør og en kameramann, for å hjelpe med å lage filmen.

6.3.1 Opprinnelig plan

Som nevnt tidligere, ville vår casting prosess vært å bruke "mannen på gata" personer til de ulike rollene for å få frem autentisiteten i situasjonen med unntak av en sterk hovedrolle som "hackeren". Alderen til våre karakterer kan ha hvilken som helst alder fordi "mannen på gata" er deg og meg.

Vi ønsker flere skuespillere av forskjellige alder, så vi kan dekke mannen på gata, ved å lage flere videoer hvor vi varierer hovedperson basert på hvilken aldersgruppe som er mest sårbar for hver trussel. På denne måten får vi publikum som er i den aldersgruppen som er mest sårbar til å relatere mer til hovedpersonen, noe som så forsaker at de gir mer oppmerksomhet til filmen.

Vår metode for å finne personer som hadde vært villige til å stille opp som skuespillere for oss, var å legge ut et innlegg på Facebook. Hver av gruppemedlemmene har Facebook og flere personer i forskjellige aldersgrupper.

6.3.2 Plan etter endring

Etter at koronaepidemien har spredd seg eksponentielt, har vi kommet frem til noen andre løsninger. Med tanke på smitte, kan vi ikke ha med eksterne personer.

Vi har kommet frem til en mulig løsning ved at vi selv er skuespillere i filmene. Dette gjøres ved at en av oss er hackeren og noen andre er andre personer som skal være med.

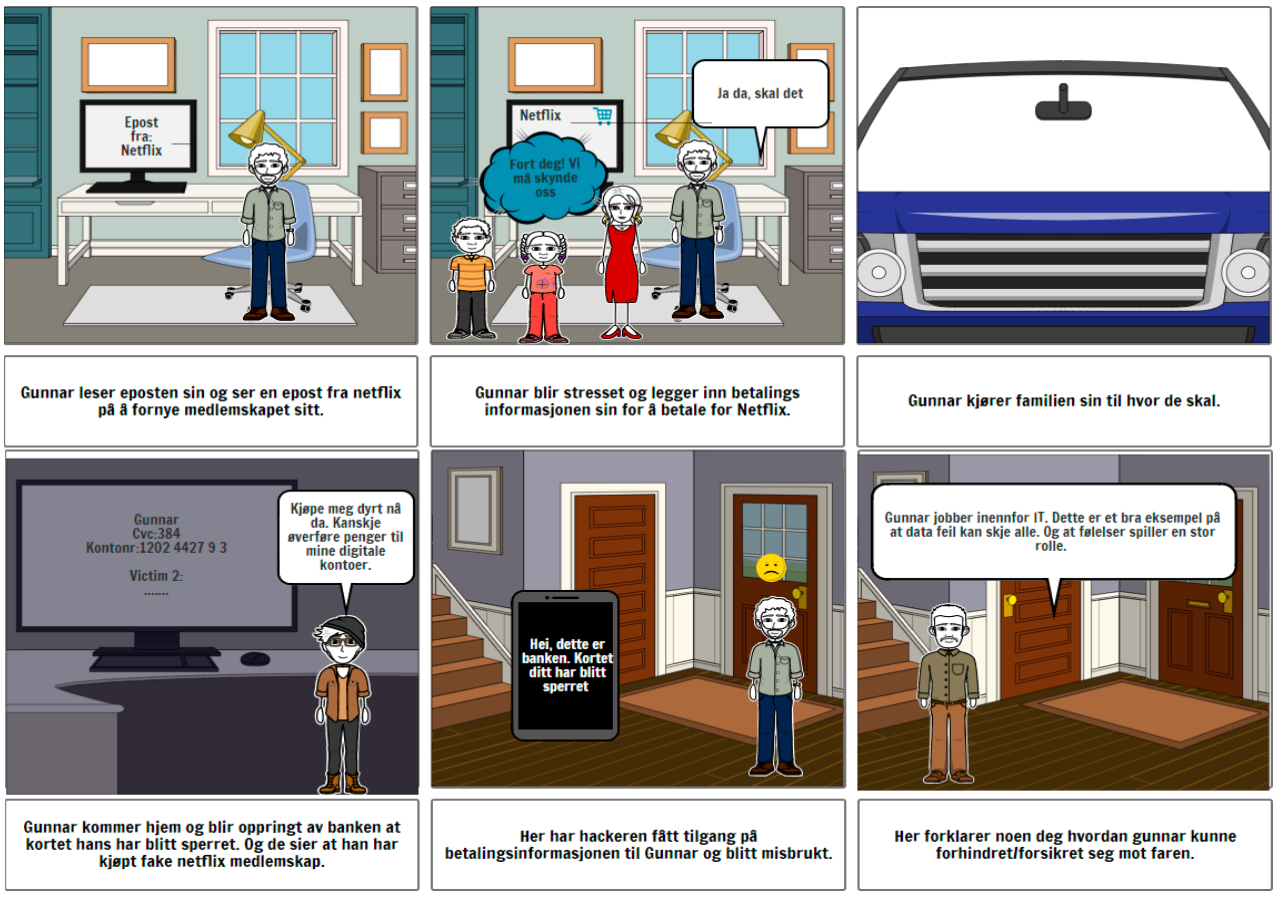
En annen løsning er om vi planlegger videoene helt ferdig for så å filme om en god stund. Hvis vi venter lenge nok, kan smittefaren ha blitt inkrementert og dermed kanskje mulig å filme med personer som ikke er medlemmer av gruppen.

Det viktigste er å sette helsen først, en løsning er da å bruke skjermopptak. Skjermopptak er et program som brukes for å ta opptak av det som skjer på skjermen. Her kan vi da ta opptak av hackeren som utfører angrep mot en annen person og personen som blir angrepet.

6.4 Storyboard

Som nevnt tidligere, er storyboard en viktig ting når det gjelder å lage videoer. Desto grundigere arbeid med storyboard, desto bedre kan videoene bli. Et storyboard inneholder elementer som skal være med i videoene. Elementer som ofte er med i et storyboard er skuespillere, miljøet hvor videoen skal bli filmet og handlingen som skal skje. Ved å lage storyboard før videoen blir laget, går filmingen fortere ettersom at man vet hva som skal filmes, hvem som skal være med og hvordan det skal filmes med tanke på for eksempel vinkler.

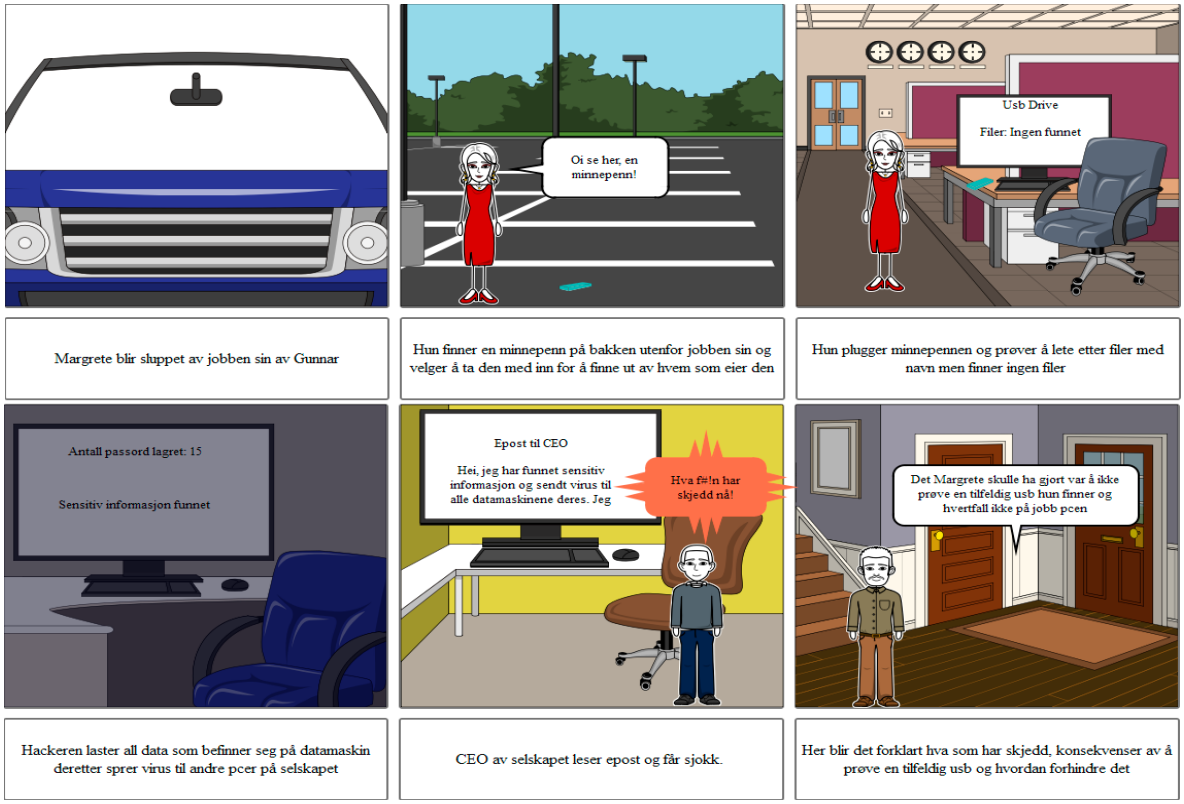
Vi har et overtema som er at vi følger en familie gjennom hverdagen, og viser dem i situasjoner de kommer i hvor de gjør en datasikkerhetsfeil og den konsekvensen den har. Vi følger først far i familien, hvor han snart må levere ungene på skolen og kjøre kona til jobb, så får han en epost fra «netflix» om å fornye medlemskapet sitt. Det han ikke vet er at dette er en fake epost som er designet for å lure han. Siden han er stresset, så tenker han ikke over det før han fyller inn betalingsinformasjonen sin og drar for å levere familien sin der de skal. Han får så etter 10 minutter en melding fra banken om at de har sperret kontoen hans siden den har blitt hacket av noen andre. Deretter forklares hva som skjedde og hvordan han kunne oppdaget dette. Dette illustreres i figur 6.4-1.



Figur 6.4-1. Bilde av er storyboard som viser at en litt stresset familiefar kan bli lurt

Vår neste situasjon var bygget for å illustrere faren med USB og fysiske angrep. Her følger vi Margrete, som er konen til Gunnar fra forrige story og mamma i familien. Gunnar slipper av Margrete på jobb, hvor hun fort finner en USB på bakken ved parkeringen. Hun tar med seg denne inn og setter den i pc-en sin, hvor det viser seg at ingenting er på den. Det hun ikke vet er at dette er en spesiell type USB som utfører ting når den blir satt i en datamaskin. USB-en har nå installert virus som gir hackeren tilgang til maskinen, uten at Margrete vet det. Siden hun satt det i jobb datamaskinen sin, så har hackeren nå tilgang til hele det interne systemet til jobben, og kan da gjøre hva de vil med det, noe som gjør at Margrete får problemer på jobben, siden hun slapp viruset inn. Til slutt forklarer vi hvorfor dette skjedde, hva som skjedde, og hvordan dette kunne vært forhindret. Dette er illustrert i figur 6.4-2.

Etter koronaepidemien var det dessverre ikke mulig å caste lenger, siden man ikke vil være mange på samme sted. Vi ville derimot fortsatt fullføre denne situasjonen, siden den viser godt faren med fysiske angrep slik som USB angrep. For å beholde situasjonen så endret vi den noe. I stedet for Margrete så har vi en gjennomgående person som er Sindre. Vi bruker gruppemedlemmene som cast istedenfor andre. Sindre finner USB-en på bakken, tar den med hjem, og åpner et dokument på den. Dokumentet slipper en orm inn på maskinen og det forklares så via webkamerafilming for å simulere Skype og videochat som brukes mer i disse tider, siden det er mer hjemmekontor arbeid og mindre mulighet for fysiske møter. Dette er den situasjonen og versjonen av den som ble brukt i video 2 om USB.

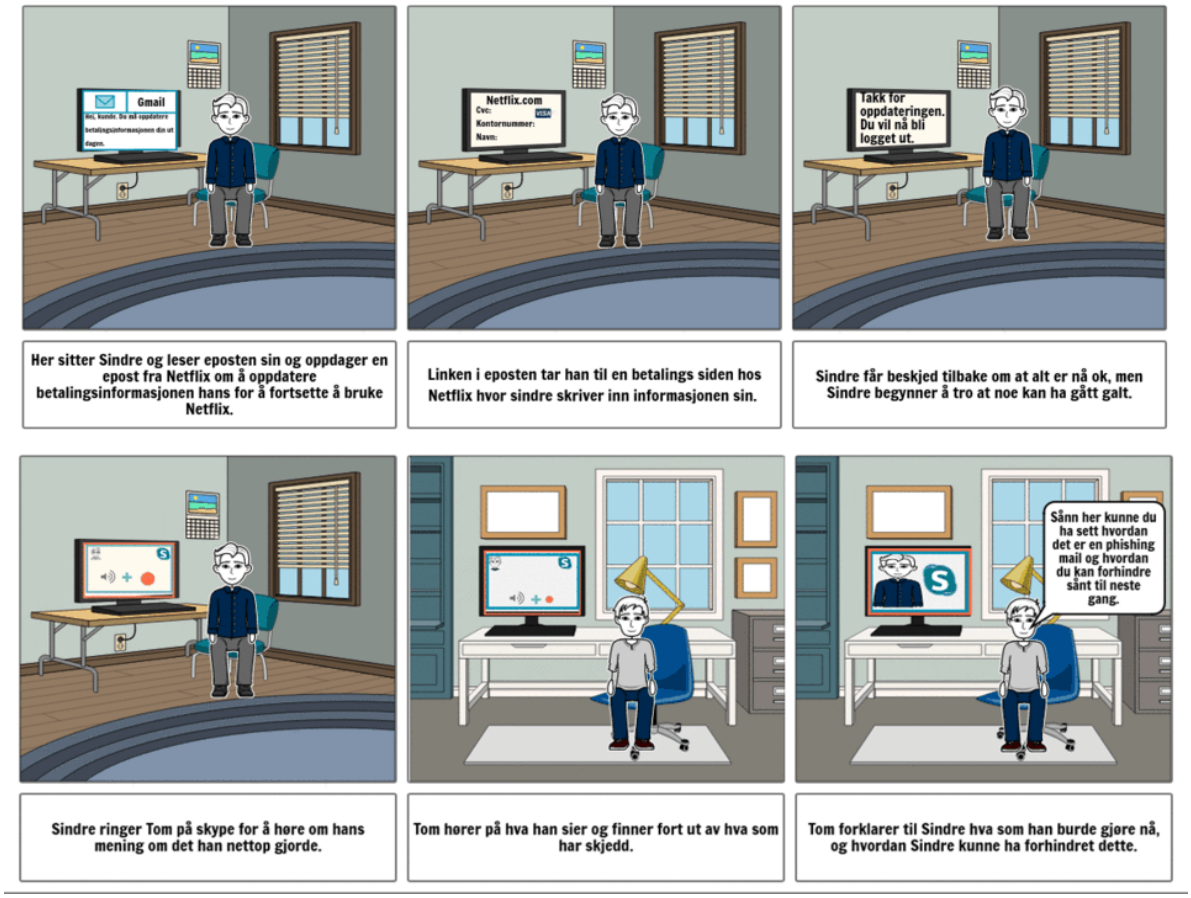


Figur 6.4-2. Bilde av et storyboard som viser at en person plukker opp en usb og setter den inn i pcen

Vårt siste storyboard er det som ble brukt i video 1 om phishing forsøk. Denne situasjonen ble laget for å tilpasse videoen til de nye forutsetningene som fulgte med koronaepidemien. Vi ville nå at hele videoen skulle filmes gjennom skjermopptak og webkamera for å redusere fysisk kontakt og risikoen for å spre viruset.

Situasjonen her begynner med Sindre karakteren som leser en epost. Her ser vi da skjermen hans og eposten, samt han gjennom webkameraet hans. Han får en epost sendt til han av «netflix» om å følge en link for å oppdatere betalingsinformasjonen hans. Det Sindre ikke vet er at denne eposten ikke har blitt sendt av netflix, men noen som prøver å lure han. Linken vil heller ikke føre han til netflix, men heller netflux, som er en side som ser lik ut men som er laget for å lagre det han skriver inn. Han følger linken, skriver inn informasjonen sin, og blir sendt tilbake til den originale siden. Han blir så bekymret om at han har gjort noe dumt, og ringer så Tom for å oppklare hva han har gjort galt. Dermed forklarer Tom hva som skjedde og hva Sindre kunne ha gjort for å unngå det. Illustrasjonen finnes i figur 6.4-3.

Etter brukertester endret videoen seg noe. I videoen som ble produsert, så ble delen hvor Sindre ringer Tom på Skype fjernet, siden den ikke ga noe uttelling for forklaring eller situasjon. Videre så fyller Sindre også ut brukerinformasjon istedenfor betalingsinformasjon, for å vise at selv dette er under angrep.



Figur 6.4-3. Et storyboard som viser at en person blir svindlet via en falsk nettside

7 Gjennomføring

7.1 Idémyldring

Vi som gruppe satte oss ned for å komme på ideer som kunne være temaer for videoene som vi skulle produsere. Dette var en prosess som skulle vise seg å gå ganske greit ettersom at gruppen var stort sett enige. Det første vi gjorde var å bestemme hvilken sjanger som passet best for den første videoen. Vi kom frem til denne sjangeren ved at vi satte oss ned som gruppe for å diskutere de forskjellige sjangerne som passet vår problemstilling. Gruppen kom frem til at en instruksjonsvideo/forklaringsvideo passet best.

Videre satte vi oss ned for å komme på ideer som passet til vår første video. Vi fikk en idé av veilederen vår, som var noe han selv har blitt utsatt for. Vi tenkte at det kan være flere som befant seg i samme situasjon og kan ha blitt utsatt for det samme svindelforsøket. Ideen som vi kom frem til var at en person fikk tilsendt en epost hvor det stod at personen måtte oppdatere kontoinformasjonen sin. I dette tilfellet var det «Netflix» som hadde sendt ut en epost, men det finnes også hackere som utgir seg for å være andre aktører, som for eksempel HBO og Viaplay. I den eposten var det en link som førte offeret til en falsk nettside hvor hackeren fikk kontoinformasjonen til offeret. Den opprinnelige planen for den første videoen var at vi skulle finne skuespillere som passet til den ideen som vi hadde kommet frem til. Etter at koronaepidemien kom til Norge, måtte vi finne andre løsninger. Vi valgte å bruke oss selv som skuespillere og gå fra å filme mye sammen til å filme mye hver for oss ved hjelp av skjermopptak.

Etter at gruppen hadde kommet frem til sjanger og ideen for den første videoen, satte vi oss ned for å diskutere sjanger og idé for den andre videoen. Vi bestemte oss for å ha samme sjanger som i den første videoen, bare på en litt annen måte. Den andre ideen som vi kom frem til var at et offer plukket opp en minnepenn på bakken og tok den med hjem for å finne ut hva som er på den. Etter det har vi valgt å ha med en forklaringsdel som forklarer hva som kan skje hvis det ligger skadevare på minnepennen.

7.2 Redigering

Vi har valgt å bruke Adobe After Effects for å lage effekter som vi bruker i filmene. Adobe Premiere Pro bruker vi for å redigere de forskjellige filmene og sette de sammen, slik at de blir til en film. Vi har også valgt å bruke Adobe Audition for å fikse på lyd i videoene for å fjerne bakrunnstøy i videoer. Filmen ble redigert sammen gjennom discord samtale og skjermdeling slik at alle fikk muligheten til å være delaktige i redigeringen.

7.3 Gjennomføring av videoer

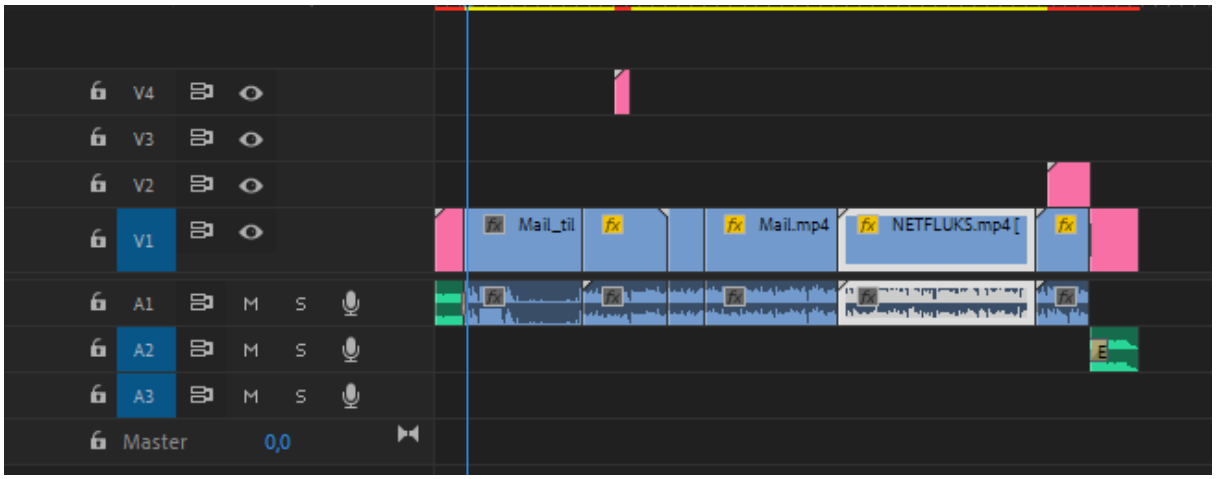
7.3.1 Film nummer en. Phishing

Manus

Manuset ble laget i gruppe gjennom discord samtale med skjermdeling slik at alle hadde mulighet til å være delaktige i arbeidet. Manuset ble skrevet ved hjelp av studiobinder. Vi satte oss ned og begynte å gå igjennom ideene som vi hadde funnet på forhånd, og valgte en av ideene. Deretter begynte vi å skrive ned hva de forskjellige rollene i filmen skulle formidle.

Redigeringsprosessen

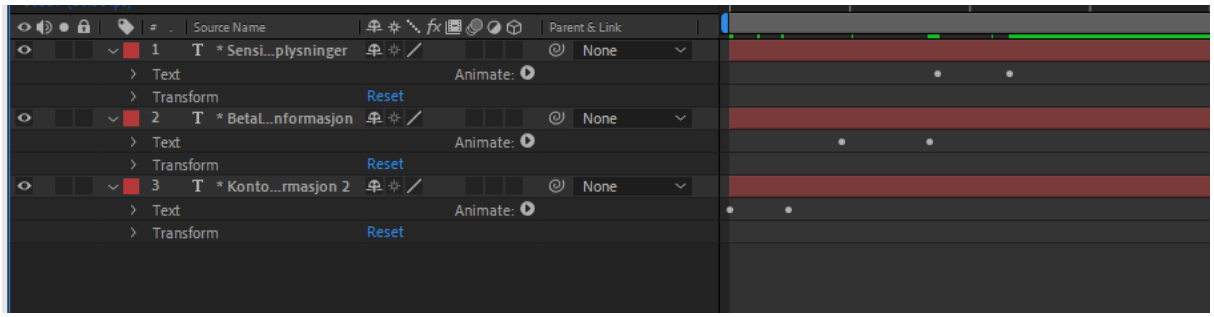
Når filmingen for film 1 var ferdig, så startet vi med å se over klippene, for å se hvilke klipp som var tatt opp best, var det endringer vi ville ha så klippene måtte spilles inn på nytt? Når vi følte oss fornøyde med klippene våre, så la vi de inn i Adobe premiere pro. Her la vi inn bare filene vi følte så best ut, så vi valgte her å ikke sortere noe særlig inne i programmet.



Figur 7.3-1 Bilde av timeline fra film1 i Adobe premiere pro

På figur 7.3-1 kan man se oppsettet i Adobe premiere pro på film 1. I motsetning til film 2 så har vi her ikke brukt mye forskjellige lydklipp, som har gjort at mye av dette har kunne blitt brukt på samme kanaler. Her har vi da også brukt flere effekter på selve videoen i seg selv, samt at vi har lagd egne effekter med tekst over skjermen, for å kunne få frem budskapet vårt på en enklere og mer effektiv måte.

Vi har også lagd noen egne visuelle effekter i filmen. På figur 7.2-1 så er alle de rosa boksene visuelle effekter vi har lagt inn. Dette er effekter som intro, rulletekst, og eventuelle tekster som har kommet over skjermen i løpet av filmen.



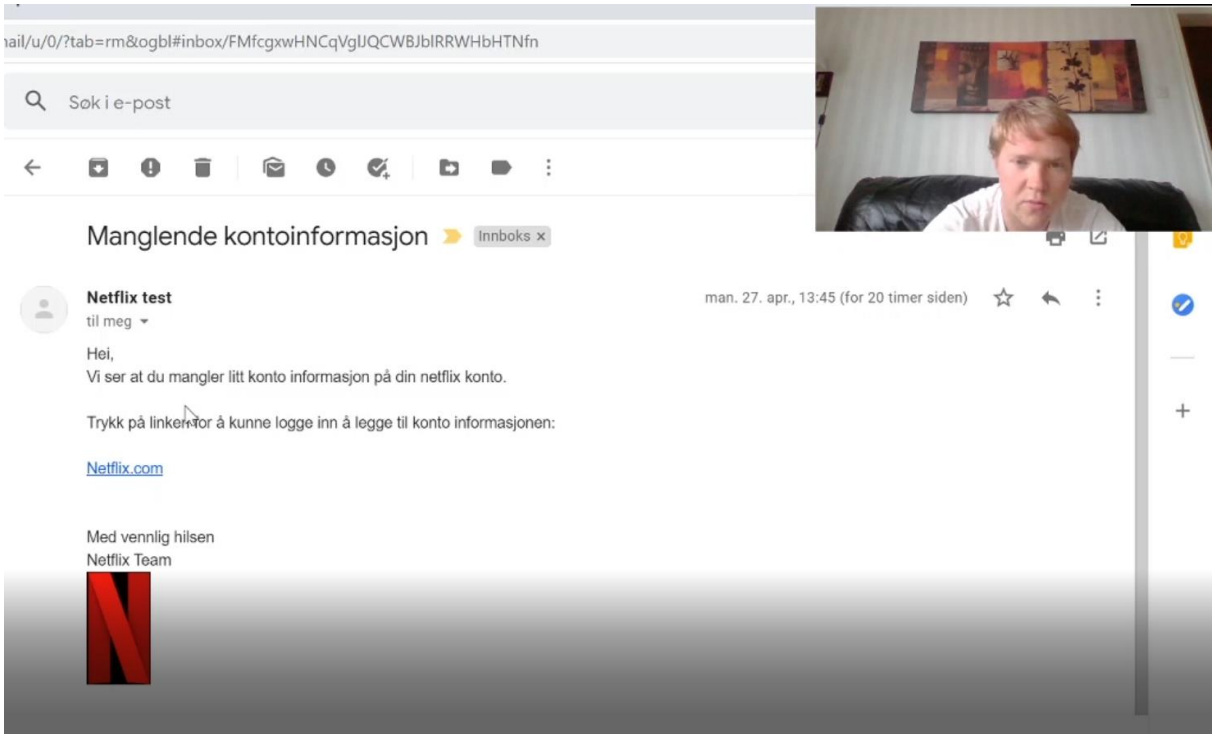
Figur 7.3-2 Bilde av timeline og keyframes i Adobe After Effects

Disse effektene er laget i Adobe sitt program som heter After Effects, På figur 7.3-2 ser man hvordan vi har jobbet med dette programmet. Det har her blitt jobbet en del med finpussing for å få effektene slik vi ønsket, selv om vi har hatt en plan på hva slags effekter vi vil ha med i filmen fra starten.

Filming

Gjennomføring av film nummer en ble i utgangspunktet lagd på basis av en ide. Ideen ble presentert i et storyboard for å illustrere ideen visuelt. Deretter jobbet vi med manuset, det ble bygd på basis av teksten som ble vist i storyboardet. Dagen ved filmingen hadde alle samme ide og oppgavene sine klare. Vi startet med å laste ned de riktige programvarene for opptak av egne skjermer. Vi brukte OBS (open broadcasting software) til opptak av lyd og skjerm. Det ble filmet hver for seg på egen pc med OBS. I denne filmen startet Sindre med å lese epostene sine hvor han finner en melding fra Netflix. Meldingen ble skrevet på en måte slik at den illustrerer et vanlig fiskingsforsøk. Den inneholder lite informasjon og ulik struktur fra en ekte epost fra Netflix. I eposten står det at han må oppdatere kontoinformasjonen med link til påloggingssiden. Siden for pålogging ble laget med Kali Linux. For å opprette den falske påloggingssiden tok vi kildekoden til Netflix sin påloggingsside og endret forespørselen på logg inn til Netflix sitt påloggingsskjema. Dette gjør da at når du trykker logg inn på vårt skjema, blir du tatt til Netflix sitt skjema. I filmen ser vi Sindre trykke på linken og forsøker å logge seg inn. Videre blir Sindre usikker siden han ikke ble logget inn på Netflix likevel. I neste scene forklarer Tom Martin til seerne om alle forholds tiltakene Sindre kunne ha gjort for å ha forhindret i å bli fisket.

Filmen, tilbakemeldinger og endringer underveis



Figur 7.3-3 Bilde fra filmen

I figur 7.3-3 så ser man bilde av Sindre, og av mailen som Netflix hadde sendt sindre. Dette bilde er tatt fra første utkast, og vi har her etter hvert tatt den opp på nytt, flere ganger, for å kunne få fikset oppi problemer, som lyd og hastigheten sindre går igjennom mailen.

Figur 7.3-4 Bilde av Sindre og Martin i et tidlig utkast

I Figur 7.3-4 ser man et tidlig utkast av filmen, her ser man at Sindre har ringt Martin på Skype etter at han har sett at mailen han hadde fått fra Netflix kanskje ikke var en ordentlig mail. Dette er en sekvens som er tatt ut av filmen da vi etter hvert etter samtaler med test brukere, og IFE forstod at denne ikke hadde noe sammenheng med filmen egentlig, å gjorde egentlig bare filmen lenger.

Figur 7.3-5 Bilde etter at intro animasjonen er ferdig

I Figur 7.3-5 så ser man hvordan vi har valgt å legge inn animasjonen til film 1, denne var opprinnelig veldig lang, og endte etter hvert med å bli kuttet ned, sånn at det ikke skulle være en veldig kjedelig start på filmen, og at folk derfor kanskje ikke hatt lyst til å se på den.

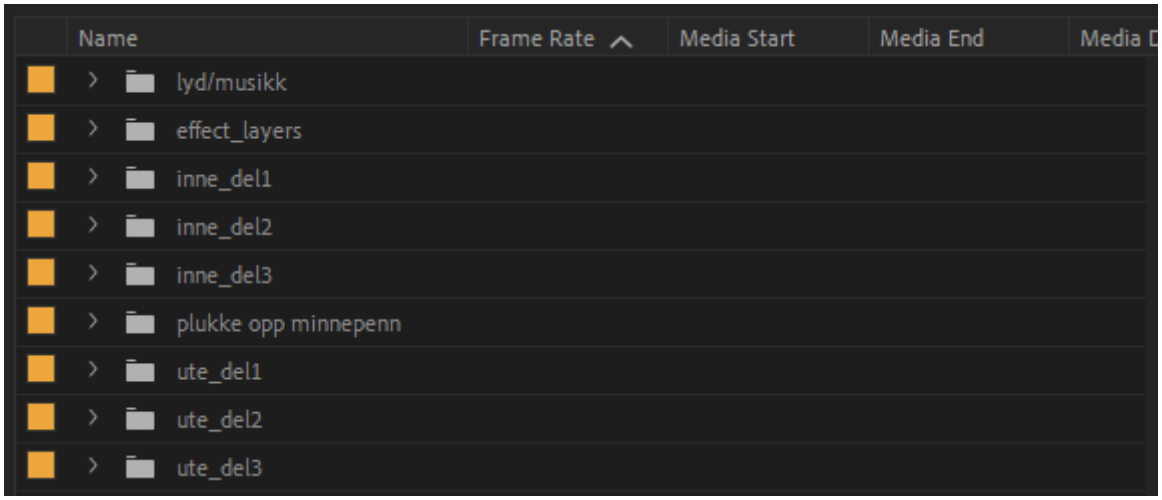
7.3.2 Film nummer to. Minnepenn

Manus

Ble laget i gruppe gjennom discord samtale med skjermdeling. Med studio binder ble manus skrevet. Vi satte oss ned og begynte å gå igjennom ideene som vi hadde funnet på på forhånd, og valgte en annen fra den vi valgte i film nummer en. Deretter begynte vi å skrive ned hva de forskjellige rollene i filmen skulle formidle.

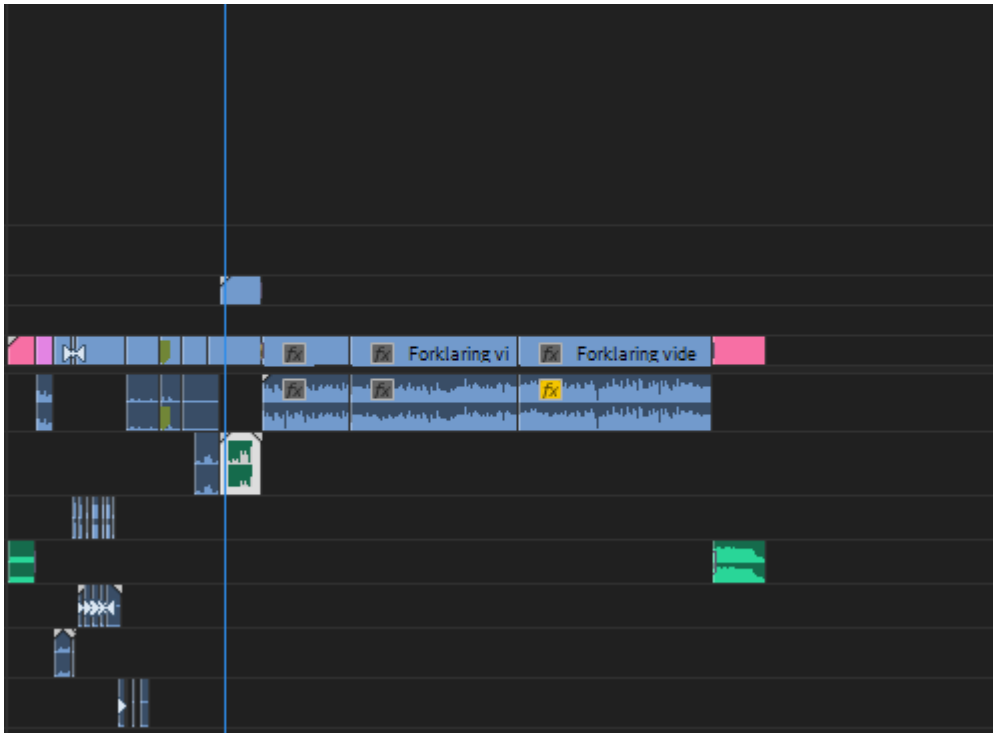
Redigeringsprosess

Redigeringsprosessen startet med at vi samlet opp alle klipp vi hadde gjort i løpet av filmingen, både skjermopptak som ble gjort, lydklipp som var tatt, og filming med kamera i en systematisk orden.
Når dette var ferdig så kunne vi starte med og se over alle klippene vi hadde fra del til del, siden hvordan vi ville ha filmen var planlagt, så delte vi den opp i deler for at det skulle være enklere å redigere.



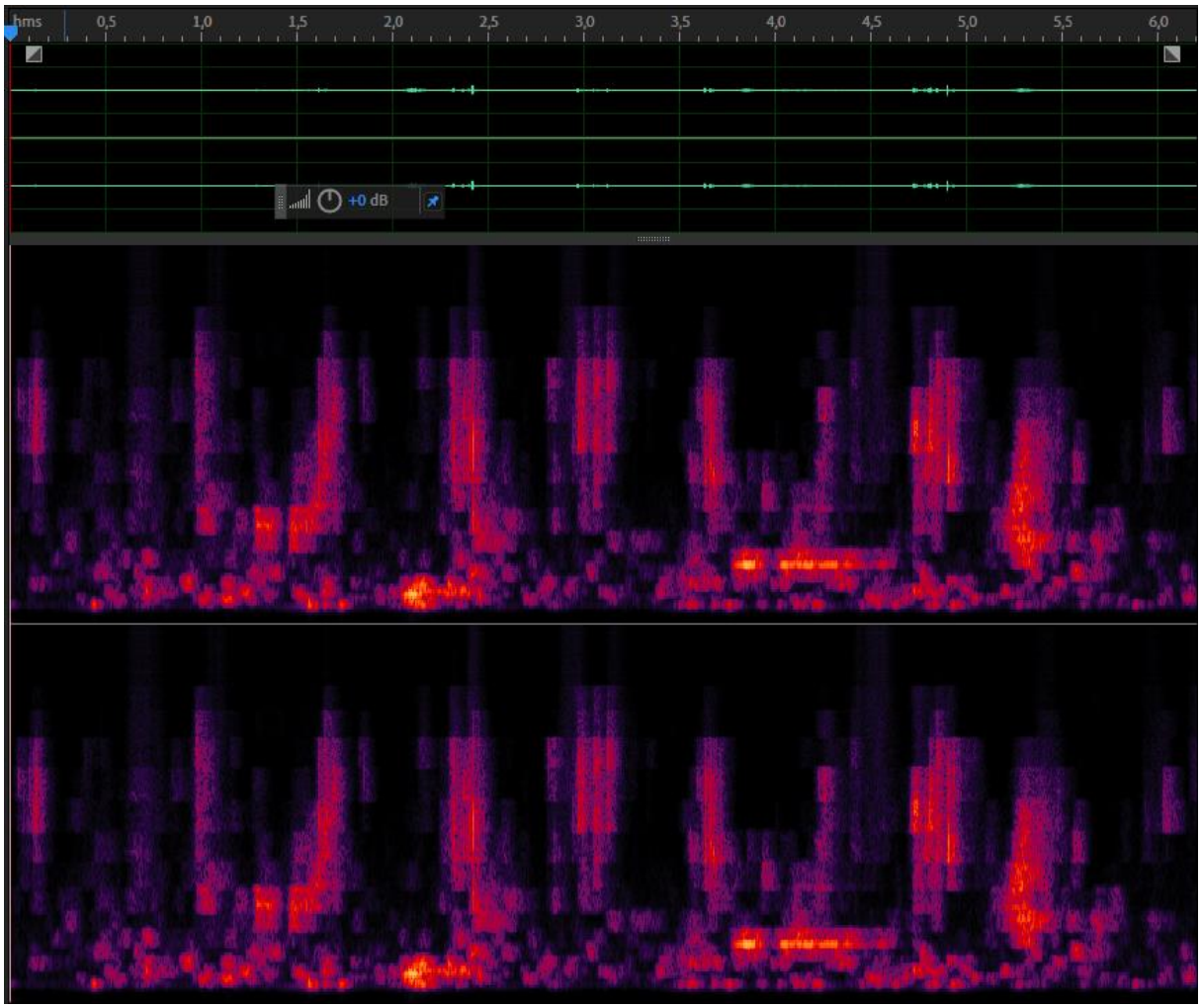
Figur 7.3-6 bilde av mappestruktur inne i Adobe Premiere Pro

På figur 7.2-6 så ser man mappestrukturen som er lagt inn i Adobe Premiere Pro. Dette var måten vi valgte å dele opp filmen på, for at det skulle være lettest for oss å holde orden i filene våre, samt for å finne ut hva som var hvor.



Figur 7.3-7 bilde av timeline inni Adobe Premiere Pro

På figur 7.3-7 ser vi nærmere på hvordan videoen har blitt satt opp. Vi har brukt flere lydspor, men også noen ekstra filmspor, for at ting skulle bli ordentlig. Lydsporene er brukt slik som det er her, grunnet at under redigering fant vi ut at noe av lyden ikke hadde blitt så bra vi trodde det ble, og vi endte dermed opp med å endre på lyden, og legge på litt effekter for å kunne gjøre lyden i filmen bedre. Får å fikse på lyden er det lagt på effekter som reverb, denoise, og parametric equaliser. I tillegg til at da det var mye støy i noen av lydklippene hvor vi hadde problemer med vind, så har vi brukt programmet Adobe Audition for å kunne fjerne lyd som vi ikke skulle ha med.

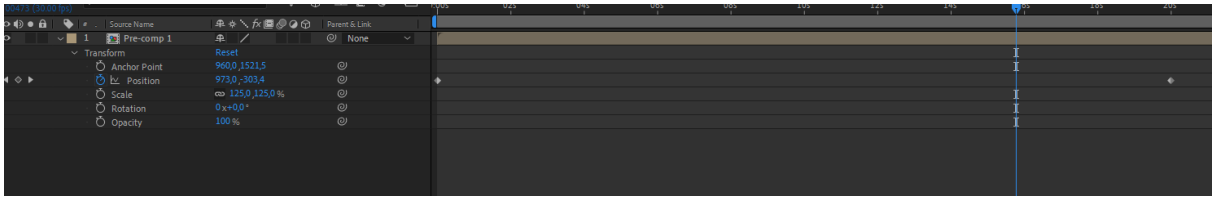


Figur 7.3-8 Bilde av lydbølger inni Adobe Audition

På figur 7.3-8 ser du et utkast av Adobe Audition. Her kan man skru ned, og fjerne spesifikke lydbølger, samt man kan gå mere i dybden i programmet for å kunne fjerne mye støy.

I filmen er det også lagd noen effekter. Her har vi ikke brukt mye visuelle effekter, vi har heller valgt å gå for rulletekst og intro bare som ekstra visuelle effekter. Rulleteksten er lagd i en composition som vi valgte å pre-compose for å animere hele rulleteksten etterpå. Dette var for å lage rulleteksten enklere og kunne endre om vi ville ha endringer i rulleteksten etter at den var ferdig lagd.

Figur 7.3-9 bilde av hele rulletekst teksten.



Figur 7.3-10 Bilde av pre-compose animasjonen av rulleteksten

På figur 7.3-9 ser vi selve rulletekst teksten inni pre-composen sin hvor all teksten står alene, mens i figur 7.3-10 ser man keyframsene i animasjonen. Det man også ser her er at vi har lagt inn logoen fra Høgskolen i Østfold. Da vi lagde rulleteksten, fant vi logoen i svart, selv om den skulle på svart bakgrunn. Da vi satt den inn i rulleteksten, satt vi på en change color effekt, som kan endre fargen ved bruk av chroma colors og da endre fargen til den fargen vi ville ha, som i dette tilfelle var hvit.

Filming

Filmingen av film 2 ble gjort under koronaepidemien. Da denne skulle filmes litt ute, måtte vi ta forhåndsregler for å gjøre denne filmingen på en ordentlig og bra måte. Vi begynte med å legge en plan på hva vi skulle filme, hvor vi skulle filme, og hvem som skulle være skuespillere i filmen. Etter dette bestemte vi oss hvem som da skulle styre kamera, også ble det bare disse som dro til lokasjonen vi skulle filme på.

Da vi kom til lokasjonen, visste vi allerede hva som skulle filmes, hvem som skulle filmes, og hvordan det skulle filmes. For å være sikker på at det ble filmet på en god måte, endte vi opp med å ta opp 3-4 opptak av hver del, slik at vi visste at vi hadde fått med flere opptak som kunne brukes. Vi hadde også sett over flere av klippene for å se at de så bra ut.

Filmen, tilbakemeldinger og endringer underveis

Figur 7.3-11 Bilde av Sindre og Martin i filmen

I figur 7.3-11 ser man Sindre og Martin i filmen, etter brukertester så fant vi ut her at lyden var veldig dårlig, og måtte endres på, grunnet for mye bakrunnstøy som var i original klippet så valgte vi her å ta opp lydopptak av begge skuespillerne i etterkant, å bruke dette som voiceover, samt at vi da la på litt bakgrunnsstøy sånn at man fortsatt skulle merke at de stod ute.

Figur 7.3-12 Bilde fra et utkast av filmen

I figur 7.3-12 så ser man en gå sekvens som var med i et tidlig utkast av filmen, denne sekvensen har blitt tatt ut av filmen grunnet tilbakemeldinger om at den ble alt for lang, og at det ikke gav noe til filmen. Dette var noe vi ble enige om å fjerne etter tilbakemeldinger fra brukertester og fra vår oppdragsgiver IFE.

8 Evaluering

Nedenunder ser du en evaluering og gjennomføring av vår brukertesting på våre filmer. Vi kommer til å vise videoene vi lager, og presentere prosessen vår til vår oppdragsgiver IFE, fokus gruppene våre, og evt andre selvstendige selskaper som jobber med datasikkerhet i forhold med utdanning. Gruppen sendte ut en Youtube link til filmene til våre respondenter, IFE og fokusgruppe. Vi brukte den samme fokusgruppen fra intervju prosessen. Hensikten med vår brukertesting er for å forbedre filmene, finne ut om de hjelper eller ikke og om det er rom for forbedringer. Respondentene ble valgt ut ifra studieretning/jobb sektor, kjønn og alder. Studieretningene/jobb sektorene som ble representert var IT, logistikk, pensjonist, sykepleier, oberst i militæret og distriktssjef. Alderen som ble representert var fra 21 → 76 år.

8.1 Film 1 (Phishing)

8.1.1 Tilbakemelding på brukertesting fra fokusgruppe

Dette er en samlet tilbakemeldingene fra vår fokusgruppe vi fikk på filmen om phishing: Det var flere skrivefeil i filmen, filmen virker troverdig, den er tydelig og klar med hensikten sin, dette var veldig nyttig informasjon, filmen har en veldig lang intro, en kort film og et viktig tema, og Lærte mye, kommer ikke til å gå på denne feilen som Sindre gjør.

8.1.2 Tilbakemelding på brukertesting fra oppdragsgiver

Fra vårt først utkast ga IFE denne tilbakemeldingen. IFE ønsket mer informasjon på skjermen under forklaring. IFE ønsket at vi viser til at filmen er basert på en spørreundersøkelse. Dø tid måtte fjernes, dette var under alle scener som hvor, «eh», «øh» og «åh» blir sagt. Større skjermbilde. Innlednings tittel og avslutningstittel må legges inn. Samtalen mellom forklarer og personen (Sindre og Tom Martin) som blir hacket kan bli fjernet og gå rett på forklaringsdelen. Fra vårt andre utkast som ble sendt til IFE fikk vi denne tilbakemeldingen. Sindre må snakke roligere og tydeligere. Likte punktlistene, men fiks skrivefeil. Likte at vi tok med at vi filmen forbeholder alle regler fra koronaepidemien. Filmen må kortes ned. Fra vårt siste utkast til IFE fikk vi denne tilbakemeldingen: Intro og outro lyd burde fase ut. Les mer klart og tydelig. Lyden er fortsatt dårlig. Skrivefeil må fikses.

8.2 Svar fra brukertesting film 2 (usb)

Dette er en samlet tilbakemelding fra vår fokusgruppe vi fikk på filmen om usb: Tom Martin mumler under forklarings delen. Det var veldig mye bakgrunnsstøy. Kan ikke se hva Sindre plukker opp (usb). Figur 8.2-1 viser at Sindre plukker opp minnepennen fra bakken.

Figur 8.2-1. Klipp fra film 2 hvor Sindre plukker opp USB.

Samtalen mellom Martin og Sindre var lav og kan ikke bli hørt godt nok. Filmen var informativ. Forklaringen til Tom var bra. Det var kjedelig å se på Tom forklare. Filmen var redigert bra.

8.2.1 Tilbakemelding på brukertesting fra oppdragsgiver

Dette er tilbakemeldingene på filmen fra IFE. Det er færre tilbakemeldinger på filmen om usb ettersom alle forbedrings endringene som ble gjort i filmen om phishing ble forbeholdt i denne. Fra vårt første utkast som ble sendt til IFE fikk vi denne tilbakemeldingen. For lang intro, det går nesten 1 minutt og 30 sekunder fra minnepenn er plukket opp til den puttes i maskina. Manus/replikker begynner å bli veldig bra. Finpuss kan være: prøve å være enda tydeligere i artikulasjon, nesten kunstig tydelig. Det er unormalt for den som snakker, men det oppfattes ikke slik av mottakeren. I tillegg kan man kanskje snakke litt saktere/roligere og da får man bedre tid til å lese replikkene helt korrekt også. Pusting i mikrofonen er forstyrrende; forslag: sett mikrofonen til side for pusteretning og øk følsomheten. Kort sagt: tydeligere tale og holde seg til teksten. Kutte ned alt som er dødtid (gåsekvenser etc.)

Fra vårt andre utkast som ble sendt til IFE fikk vi denne tilbakemeldingen. Fint at dere har kuttet gå-scenen, kutt gjerne fra 40 sek til 60 sek. Vi skjønner at han er kommet hjem.- lyden fra 1.20 til 1.30 må spilles inn på nytt. Generelt sett er lyden dårlig og skurrete, dersom jeg skulle ønske EN forbedring må det være lydkvalitet. "Hackeren vil kunne gå igjennom PC'n" --> mener dere : "Hackeren vil få tilgang til informasjon på datamaskinen din"

8.3 Konklusjon

Vi konkluderer med at vi har fått noen bra og noen dårlige tilbakemeldinger. Vi må rette skrivefeil, fikse bakgrunnsstøy, lyd og fargekorrigere. Dette vil bli fikset før vi leverer vårt sluttprodukt. Denne filmen er lagd under Koronaepedemien, alle rettningslinjer fra Norsk stat og FHI er overholdt. Nye scener kan ikke spilles inn, så scene hvor usb blir plukket opp vil ikke bli fikset.

9 Diskusjon

Diskusjonen går ut på at vi går igjennom målene som vi har hatt siden starten, metodene som vi har valgt å bruke, det som skal leveres, hva vi kunne gjort forskjellig fra det vi gjorde, og hva som ville vært videre arbeid.

9.1 Måloppnåelse

Målene for prosjektet ligger i kapittel 1.4 og er som følger:

Hovedmål:

- Øke datasikkerhets kompetansen blant privatpersoner

Delmål:

- Gjøre personer oppmerksomme på hva man burde tenke på
- Lage videoer som IFE kan få bruk for etter prosjekttiden
- Skaffe et overblikk over cyber kunnskapen til privatpersoner

Vårt hovedmål var å styrke privatpersoner sin datasikkerhetskompetanse. Dette gjorde vi ved å lage videoer basert på svarene vi fikk fra spørreundersøkelsen. Ved å lage videoer som viser og forklarer forskjellige typer svindler, kan være med å styrke «mannen på gata» sin datasikkerhetskompetanse. Ut ifra de tilbakemeldingene vi fikk fra fokusgruppen, var det noen konstruktive, men også noen positive. Vi har forsøkt å fikse videoene ut ifra de konstruktive tilbakemeldingene slik at vi skulle lage videoer som «mannen på gata» skulle få best utnytte av. Ut ifra de positive tilbakemeldingene var det flere som mente at filmene var bra og til hjelp. Dette viser at videoene er til hjelp og vi har nådd vårt hovedmål.

Det første delmålet vårt var å gjøre personer oppmerksomme på hva man burde tenke på. Dette gjorde vi ved å tilpasse innholdet i videoene til å forklare hva personene burde tenke på. Det kommer frem i form av tale, men også punkter som kommer på skjermen under videoen.

Det andre delmålet vårt var å lage videoer som IFE kan få bruk for etter prosjekttiden. Vi har valgt å lage to videoer som blir vårt produkt. Planen var at vi skulle prøve å lage fem videoer, men vi fant ut at dette ville ta lang tid og at vi ikke ville rekke å lage fem gode og informative videoer. Vi har skrevet hvordan vi har valgt å gå frem for å lage videoer, som IFE kan få bruk for senere.

Det tredje delmålet var å skaffe et overblikk over cyber kunnskapen til privatpersoner. Dette gjorde vi ved å gå igjennom svarene som vi fikk fra spørreundersøkelsen og de semistrukturerte intervjuene. Ved å analysere alle svarene, kunne vi lage videoer basert på det.

9.2 Leveranser

Hovedleveransene for dette prosjektet var instruksjonsvideoer, hoveddokumentet og nettsiden. Planen var at vi skulle lage fem instruksjonsvideoer med fem forskjellige temaer. Videoene skulle produseres slik at de som ser på den skal få bedre kunnskaper om datasikkerhet. Vi fant ganske fort ut at det å lage 5 gode videoer ville ta lang tid og derfor valgte vi å lage to gode videoer i stedet for fem videoer som bare hadde blitt middels. Vi ønsket å lage en bedre spørreundersøkelse og intervju for å finne ut kunnskapen «mannen på gata» har om datasikkerhet, før vi begynte på planleggingen av videoene. Planleggingen av hver video tok lenger tid enn det vi hadde trodd på forhånd. Alt fra skuespillere til lokasjoner måtte planlegges før vi kunne starte med filmingen.

Hoveddokumentet startet vi med så fort vi hadde mulighet. Vi startet med å skrive forprosjektrapport som skulle leveres tidlig i prosessen. Deretter fortsatte vi med å skrive om de elementene som hoveddokumentet skulle bestå av. I hoveddokumentet ligger fremgangsmåten på hvordan å lage en video. Dette kan IFE bruke videre for å lage flere videoer som står i stil til de vi har laget.

Nettsiden er en wordpress side som vi har lagt inn alle dokumenter som vi har utarbeidet i løpet av prosjekttiden i. Møtereferatene fra møtene mellom gruppen og veileder, mellom gruppen og IFE har blitt lagt ut her underveis.

9.3 Metodevurdering

Metodene som er valgt for prosjektet ligger i kapittel 1.4.3 og er som følger:

A. Systematisk vurdering av det teknologiske nivået til “mannen i gata”(alle og enhver).

B. Evaluer og finn tilnærminger for å øke cybersikkerhet hos privatpersoner (gitt trinn A)

C. Lag et sett med informasjonsvideoer som gir enkeltpersoner mulighet til å forstå og handle selvstendig for å øke deres private cybersikkerhet.

D. Ha en systematisk og repeterbar tilnærming slik at videoer kan legges til i samme format (innhold, grafikk, forståelsesnivå osv.) senere, og slik at det skiftende landskapet til cybertrusler kan adresseres på samme måte i fremtiden.

E: Gruppen skal jobbe etter dokumentert metode/metodikk slik at det er mulighet for at andre kan videreføre arbeid i senere fremtid.»

Som nevnt tidligere, valgte vi å sende ut en spørreundersøkelse for å finne ut kunnskapen «mannen på gata» har om datasikkerhet. Vi følte at det å sende ut en spørreundersøkelse ville gjøre det vi ønsker, uten at vi skulle bruke for mye tid på det. Vi kunne da jobbe med andre ting samtidig som personer svarte på spørreundersøkelsen.

Som nevnt tidligere, skulle vi produsere videoer for å styrke kunnskapen «mannen på gata» har om datasikkerhet. Vi har valgt å lage videoer som er informative i form av instruksjonsvideoer. Videoene inneholder en person som blir ett offer for en svindel og en person som forklarer hva offeret gjorde, og tiltak som offeret burde ha gjort.

Gruppen har dokumentert alt som har blitt gjort i forhold til planlegging og filming i hoveddokumentet. Ved å lese igjennom dette, kan andre personer få samme tankegang som vi har hatt og lage videoer som står i stil til de vi har laget.

9.4 Forbedringer

9.4.1 Spørreundersøkelsen

Det vi har snakket om i ettertid er at vi burde laget en egen spørreundersøkelse for Facebook. Det vi tenkte på var at vi kunne kopiere den spørreundersøkelsen som vi sendte ut til studentene og ansatte ved HIOF, slik at vi kunne få en egen link og funnet ut hvor mange respondenter vi fikk fra Facebook kontra studenter og ansatte fra HIOF. Dette hadde gitt oss svar på hvor mange som svarte fra hver plattform. Ettersom at de fra Facebook kanskje har annerledes bakgrunn enn de som studerer nå, kunne vi laget med spesifiserte videoer.
Et annet spørsmål som vi kunne hatt med er kjønn. Ved å finne ut kjønnet til respondenten kan vi finne ut svar basert på kjønn. Ut ifra det kan vi finne ut hvilket kjønn som er de beste innenfor datasikkerhet. Vi kunne delt inn aldersgruppene forskjellig fra hva vi har gjort nå.

Ved å for eksempel legge til aldersgruppen 19-25 kan man finne ut om personen er studenter eller ikke. De som er i aldersgruppen 19-25 er ofte studenter. De yngste som går på høgskolen, er 19/20 år. Noen har vært i militæret før de har begynt å studere høyere utdanning, og da er de 20/21 år. Etter at de har fulført er de tidligst 23/24 år, men noen må kanskje ta opp et fag og da er de 24/25 år.

Helt på slutten av spørreundersøkelsen, kunne vi hatt med et spørsmål om respondenten fikk noe ut av denne spørreundersøkelsen. Hvis respondenten hadde svart at respondenten hadde fått noe ut av denne spørreundersøkelsen, hadde vi gjort en god jobb i forhold til målet vårt.

9.4.2 Filming

Det viste seg at de fleste av opptakene ikke ble som vi hadde tenkt, slik at vi ikke kunne bruke de. Vi endte opp med ett opptak som viste seg å være helt grei, men noe uklar lyd. Hvis det er en ting som vi burde ha endret, hadde det vært å få en klarere lyd. En annen ting som vi også burde ha gjort var å gå igjennom alle opptakene som vi hadde gjort den dagen og eventuelt filmet de scenene som trengtes på nytt.

9.5 Videre arbeid

Videre arbeid ville vært å lage flere videoer ut ifra den fremgangsmåten som vi har valgt å bruke. Ved å lage flere videoer med andre temaer, ville det etter alt å dømme styrke datasikkerhetskunnskapen til «mannen på gata».

Sammen med å lage flere videoer, vil det være smart å ha mer brukertesting. Dette kan gjøres ved å sende et påbegynt produkt til en fokusgruppe, slik at de kan komme med tilbakemeldinger på hva som burde gjøres bedre og eventuelt hva som var bra.

Noe som hadde vært smart for oss og gjort videre, ville vært å finne ut om filmene faktisk hjalp «mannen på gata». Vi fikk ikke testet om filmene hadde hjulpet de med å forbedre datasikkerhetskompetansen deres bortsett fra det vi fikk vite fra brukertestene. Det vi kunne gjort var å gjennomføre en ny spørreundersøkelse for alle respondentene, for å kunne se om de svarte bedre denne gangen.

10 Konklusjon

Arbeidet med bacheloroppgaven har vist seg at «mannen på gata» står ovenfor digitale trusler av ulike typer og har manglende kunnskaper innenfor datasikkerhet. De ulike aldersgruppen står ovenfor dette. Vårt opplegg retter seg mot å forbedre «mannen på gata» sin forståelse og for å forebygge datatrusler, og våre videoer viser at de er målrettet «mannen på gata» og forbedrer datasikkerhets kunnskapene.

Gjennom spørreundersøkelse og semistrukturert intervju ble våre videoer rettet mot målgruppen «mannen på gata». Våre respondenter sier at videoene kunne vært mer gøy og de videoene er hensiktsmessige for og forbedrer datasikkerheten sin.

I denne oppgaven ble det brukt to metoder for innhenting av data. Den første metoden vi startet med var en kvantitativ metode som var en spørreundersøkelse. Denne spørreundersøkelsen ble laget med google forms. Spørreundersøkelsen ble sendt ut til alle studenter og ansatte ved Høgskolen i Østfold og til våre venner på Facebook. Grunnen til at vi sendte ut en spørreundersøkelse var på grunn av at det var en enkel og effektiv måte å finne «mannen på gata» sin datasikkerhetskompetanse. Totalt fikk vi inn 314 respondenter som vi ser som bra og mange nok til å representere «mannen på gata». Grunnen til at vi sendte ut en spørreundersøkelse var på grunn av at det var en enkel og effektiv måte å finne «mannen på gata» sin data sikkerhetskompetanse. Totalt fikk vi inn 314 respondenter som vi ser som bra og mange nok til å representere «mannen på gata».

Den andre metoden brukte vi kvalitativt metode. En kvalitativ metode går mer i dybden enn en kvantitativ undersøkelse, som uttrykkes i form av korte setninger eller bare ved få ord. Ved å gjennomføre semistrukturerte intervjuer, kan gruppen få færre svar, men mer utfyllende.
Semistrukturerte intervjuene ble gjennomført med en fokusgruppe på seks personer som er satt sammen basert på alder og teknisk bakgrunn. Grunnen til at vi valgte å gjennomføre de semistrukturerte intervjuene var for å finne ut hva de kan og hva de ikke kan. Videre ble det laget videoer basert på resultatene til disse to metodene. Til slutt ble videoene brukertestet med IFE og fokusgruppen.

Gjennom videoproduksjonen ble utkaster laget av videoene for tilbakemeldinger. Disse tilbakemeldingene ble tatt i betraktning men ikke alle ble gjennomført eller vurdert for slutt produktet.

Denne oppgaven viser til at videoene er ressursvennlige ettersom de dekker store sikkerhetshull for «mannen på gata», samtidig som at de kun varer i 5 minutter per video.

Gjennom denne bacheloroppgaven har vi fått innsikt i hva «mannen på gata» kan og ikke kan om datasikkerhet ved at vi sendte ut en kvantitativ spørreundersøkelse og gjennomførte semistrukturerte intervjuer med fokusgruppen. Det vi lærte av dette var å lage spørreundersøkelse som tilpasset seg nivået til «mannen på gata» og analyserte dataene som vi fikk fra spørreundersøkelsen.

Vi har lært mye om datasikkerhet, samt undervisning gjennom dette prosjektet og ønsker alle en sikrere verden.

11 Referanser

Bakos, G. (2013). Passordhåndtering. *Ouch!*, (201310). Retrieved from https://www.uninett.no/sites/default/files/webfm/OUCH-201310%20Passordh%C3%A5ndtering.pdf

Dahlum, S. (2019). Kvantitativ analyse. Retrieved from https://snl.no/kvantitativ_analyse

Grønmo, S. (2009). Kvalitativ metode. Retrieved from https://snl.no/kvalitativ_metode

Grønmo, S. (2014). Kvantitativ metode. Retrieved from https://snl.no/kvantitativ_metode

Jacobsen, D. I. (2015). Hvordan gjennomføre undersøkelser? In (pp. 134-136): Cappelen Damm.

Kenneth C. Laudon, J. L. (2018). Management Information Systems – Managing the Digital Firm 15th edition. In (pp. 85-90). Essex, England: Pearson.

Nätt, T. H. (2019). Skadevare. Retrieved from https://snl.no/skadevare

Sjøberg, S. (2020). Didaktikk. Retrieved from https://snl.no/didaktikk

Skei, H. H. (2019). Kriminallitteratur. Retrieved from https://snl.no/kriminallitteratur

Svennevig, J. (2019). Sjanger. Retrieved from https://snl.no/sjanger

Tjeldvoll, A. (2018). Pedagogikk. Retrieved from https://snl.no/pedagogikk

Tom Heine Nätt, C. F. H. (2017). *Datasikkerhet, ikke bli svindlerens neste offer*.

Williams, J. (2014). Hva er Antivirus? *Ouch!*, (201412). Retrieved from https://www.uninett.no/sites/default/files/webfm/OUCH-201412%20Hva%20er%20antivirus.pdf

12 Figurliste

13 Vedleggsliste

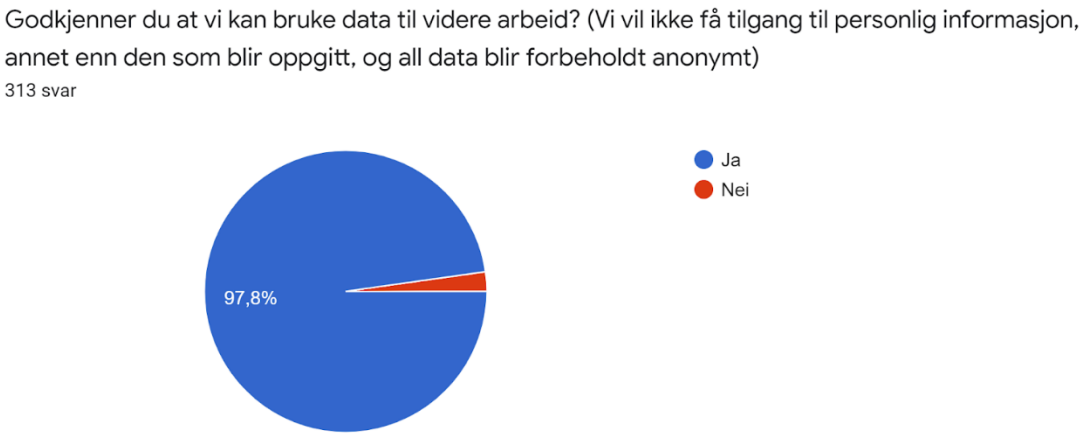
Spørreundersøkelsen: spørsmål og svar

Semistrukturert intervju: spørsmål og svar

Manus

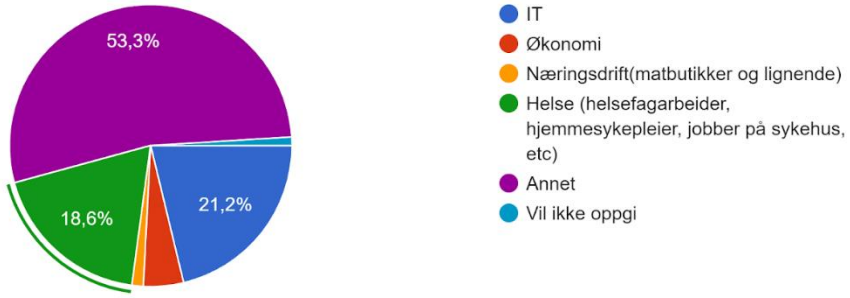
13.1 Vedlegg 1: Spørreundersøkelsen med svar

Godkjennelse



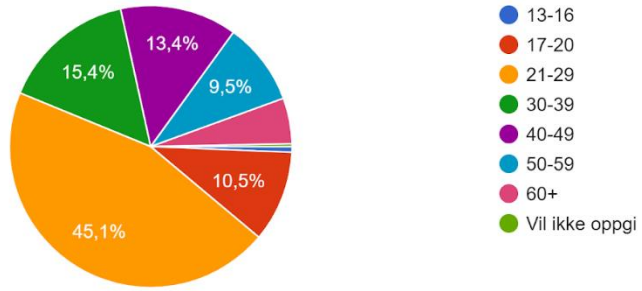
Jobb/Studie

Hva jobber du med/studerer du?
306 svar



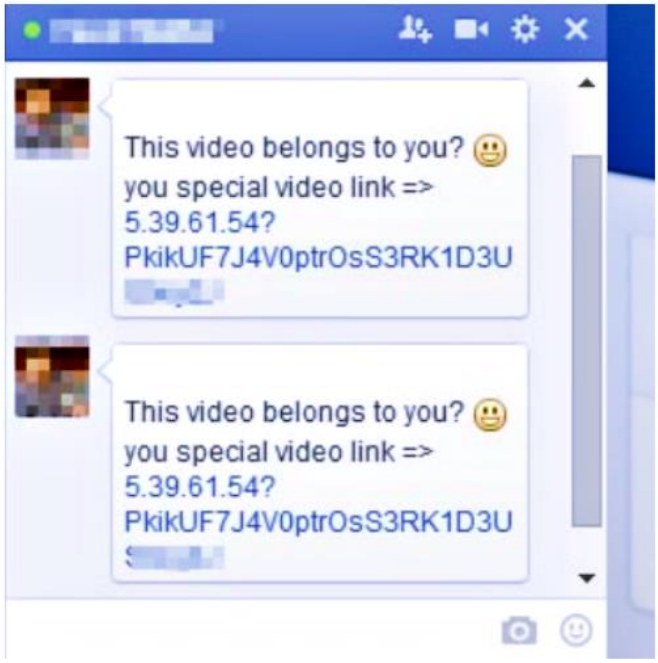
Alder

Alder:
306 svar

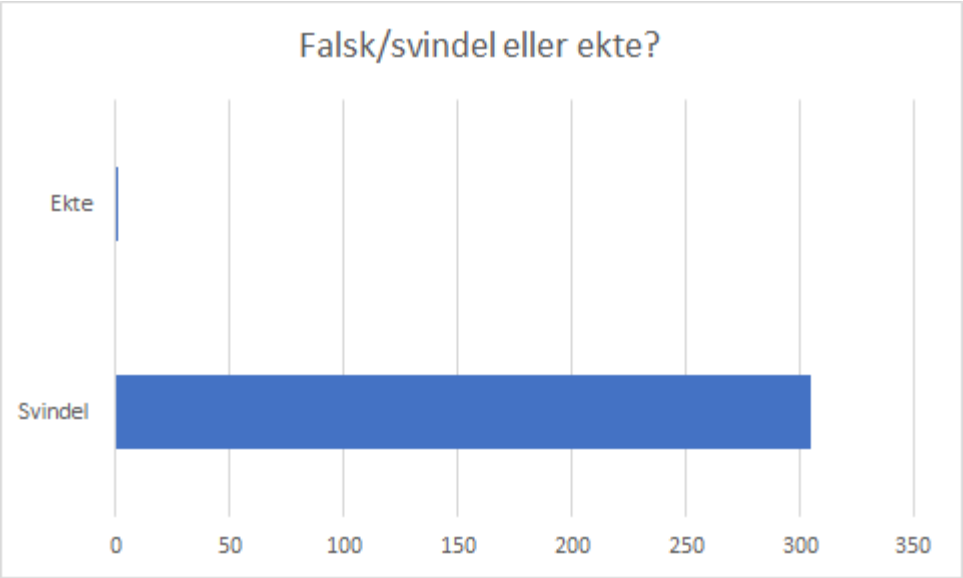


Spørsmål 1:

Falsk/svindel eller ekte? *



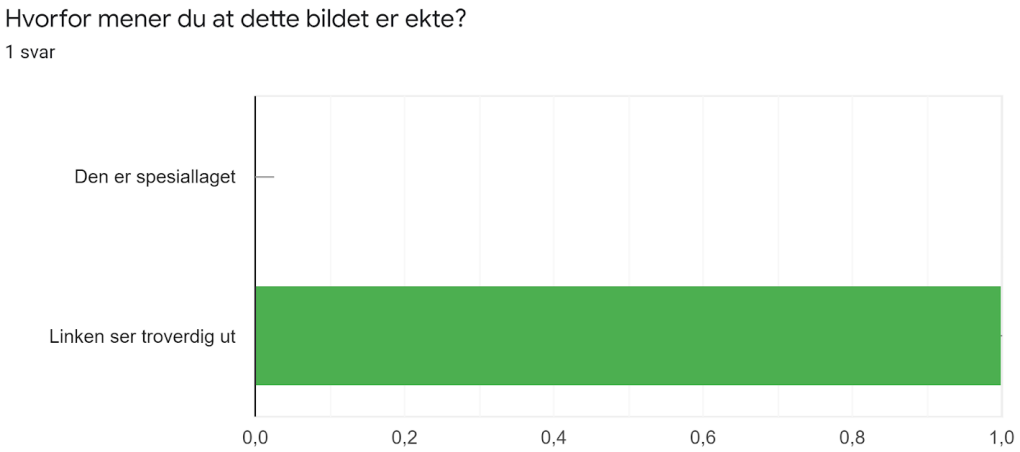
- ◯ Svindel
- ◯ Ekte



Det er totalt 314 som har svar på dette spørsmålet, hvorav 313 svarte at det var svindel og 1 som svarte at meldingen var ekte.

Underspørsmål 1.1:

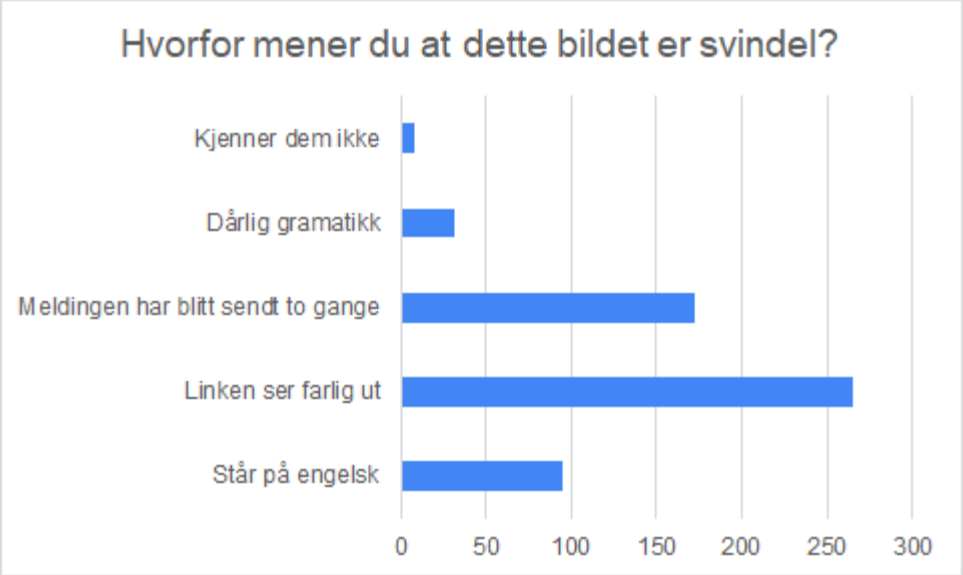
Nedenunder ser du en graf vi har laget til å vise frem meningene om hvorfor de mente meldingen ser ekte ut



Det var en person som svarte at meldingen var ekte og personen mente at linken så troverdig ut.

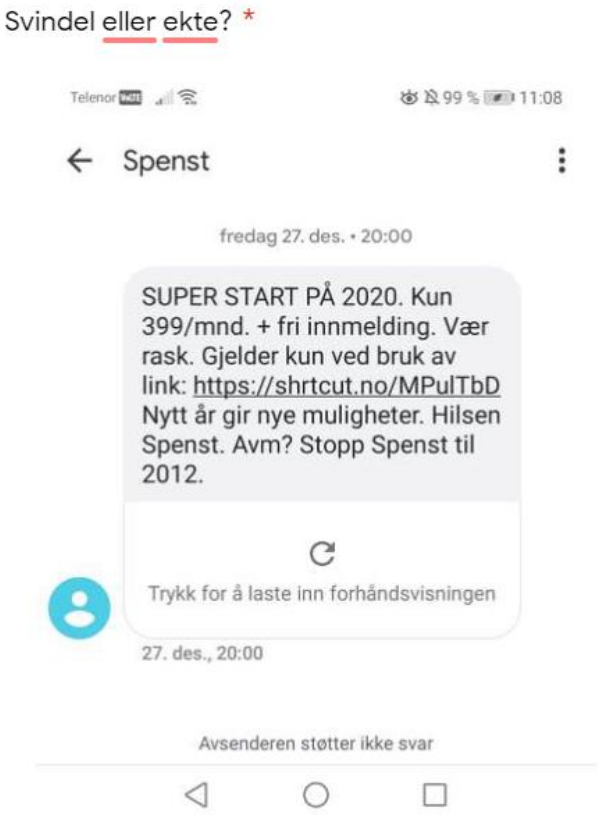
Underspørsmål 1.2:

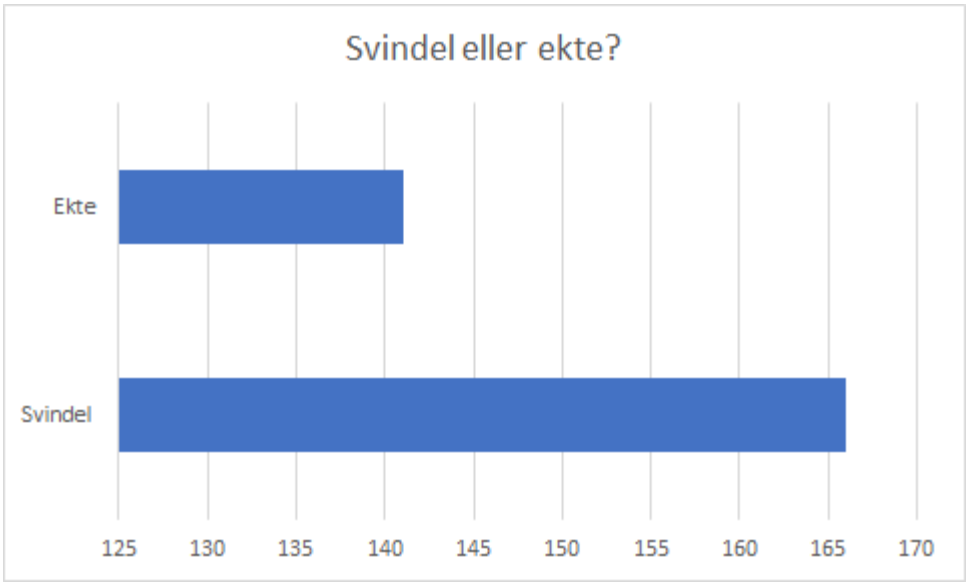
Nedenunder ser du en graf på hvorfor og antall mennesker svarte det på at det var en svindel.



Ovenfor ser du de mest svarte grunnene til at de mente at bildet var svindel. De mente at grammatikken er så dårlig at den ikke var overbevisende nok til at den kan være ekte. De sier en slik link fra en fremmed skaper ikke troverdighet og heller prøver å "lure" dem så de sier at de ikke ville trykket seg videre.

Spørsmål 2:

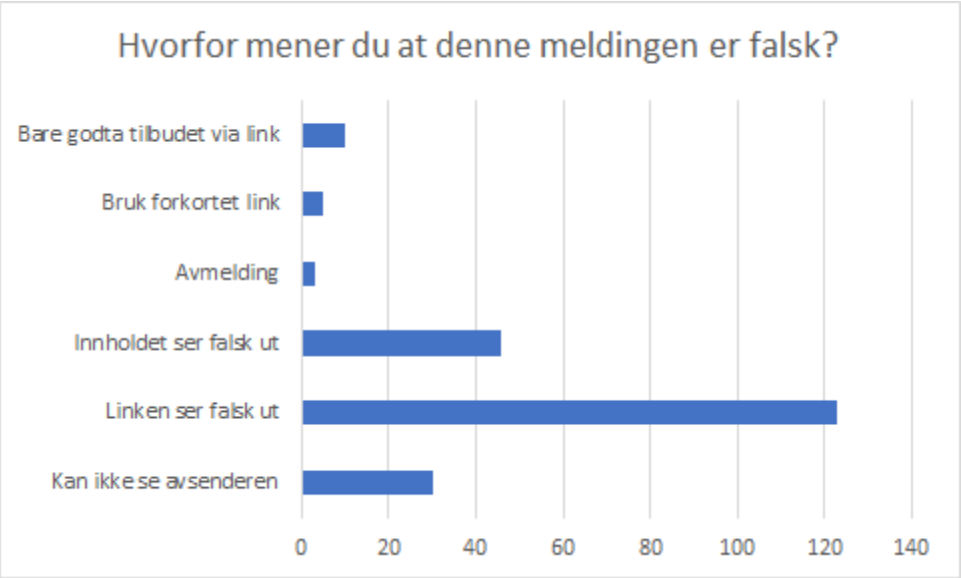

Svindel eller ekte? *
Telenor
99 % 11:08
Spenst
fredag 27. des. • 20:00
SUPER START PÅ 2020. Kun 399/mnd. + fri innmelding. Vær rask. Gjelder kun ved bruk av link: https://shrtcut.no/MPulTbD Nytt år gir nye muligheter. Hilsen Spenst. Avm? Stopp Spenst til 2012.
Trykk for å laste inn forhåndsvisningen
27. des., 20:00
Avsenderen støtter ikke svar
Svindel
Ekte


Svindel eller ekte?
Ekte
Svindel
125
130
135
140
145
150
155
160
165
170

Det er totalt 314 som har svar på dette spørsmålet, hvorav 170 svarte at det var svindel og 144 som svarte at meldingen var ekte

Underspørsmål 2.1:

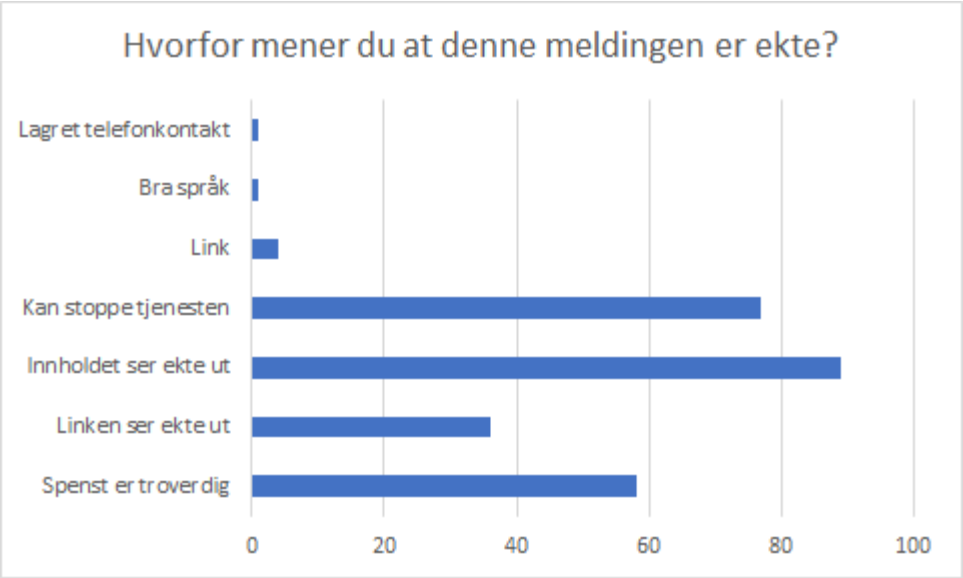
Nedenunder ser du en graf på hvorfor og antall mennesker svarte det på at den var falsk..



Det er totalt 170 personer som har svart at meldingen fra spenst var falsk. Det er noen personer som har valgt flere alternativer. 124 personer svarte at lenken i meldingen ser falskt ut, 45 personer svarte at innholdet ser falskt ut og 32 svarte at de ikke kan se avsenderen. Resten svarte at det er rart at det står avmelding i bunnen av meldingen, at spenst har brukt forkortet link, og at det bare går an å godta tilbudet via linken.

Underspørsmål 2.2:

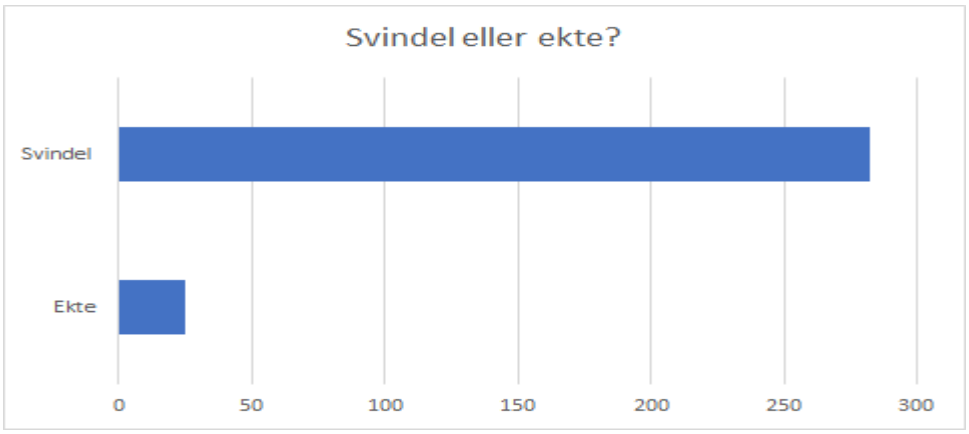
Nedenunder ser du en graf vi har laget til å vise frem meningene om hvorfor de mente meldingen ser ekte ut



Det er totalt 144 personer som har svart at meldingen fra spenst var falsk. Det er noen personer som har valgt flere alternativer. 92 svarte at innholdet i mailen ser ekte ut, 78 personer har svart at det er mulig å stoppe tjenesten, 61 personer svarte at spenst er troverdig og 38 svarte at linken ser ekte ut. Resten svarte at det var brukt bra språk i meldingen, noen kjenner til bruken av forkortet link fra før, og at spenst var lagret som kontakt på telefonen.

Spørsmål 3:

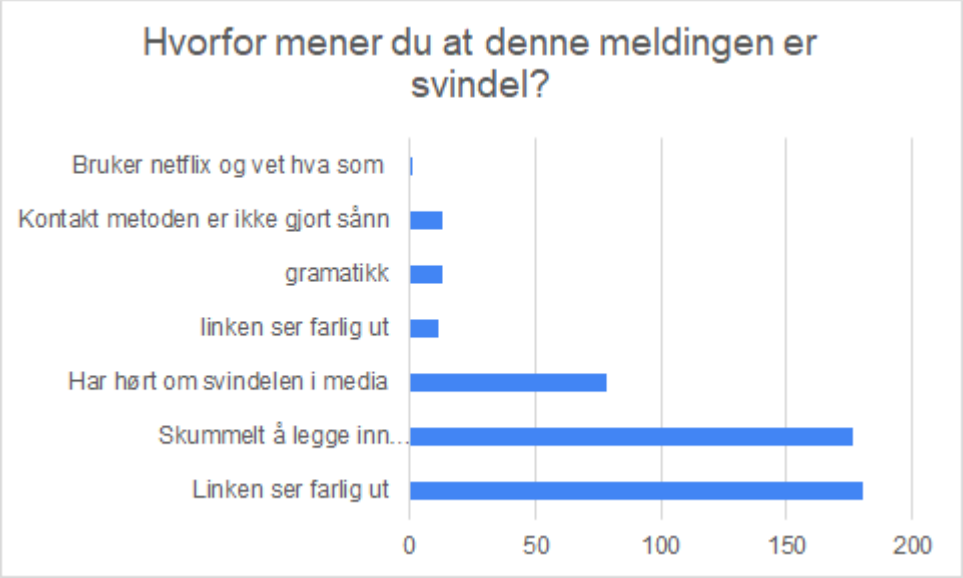
Nedenunder ser du en graf på antall som svarte det var svindel eller ekte.



Det er totalt 314 som har svar på dette spørsmålet, hvorav 289 svarte at det var svindel og 25 som svarte at meldingen var ekte.

Underspørsmål 3.1:

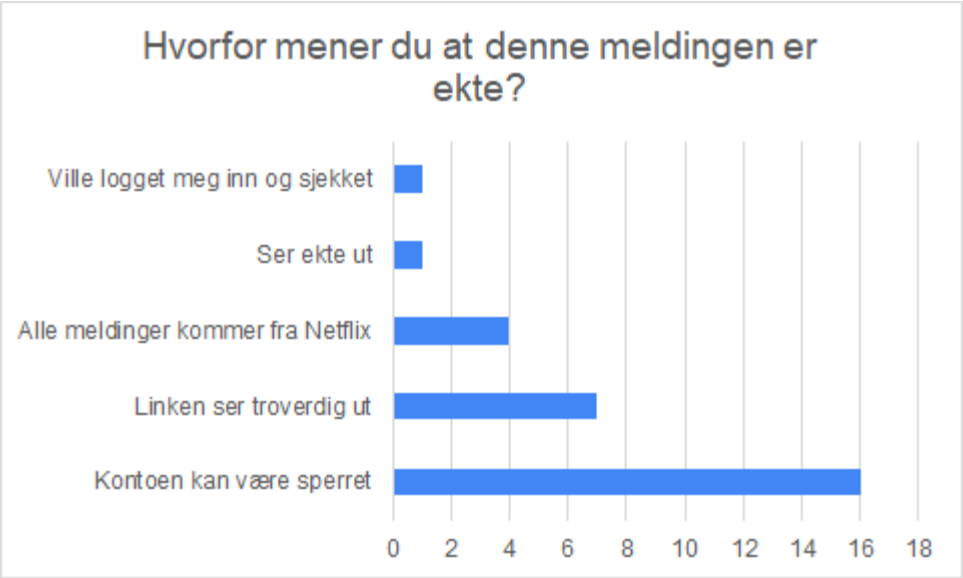
Nedenunder ser du en graf på hvorfor og antall mennesker svarte det på at det var en svindel.



Det er totalt 289 personer som har svart at meldingen fra Netflix var falsk. Det er noen personer som har valgt flere alternativer. 186 personer svarte at linken ser farlig ut, 182 har svart at det er skummelt å legge inn betalingsinformasjon, og 81 har hørt om svindelen i media. Resten har svart at linken ser farlig ut, kontaktmetoden er ikke gjort på en slik måte, og at noen bruker Netflix og vet hvordan det ser ut.

Underspørsmål 3.2:

Nedenunder ser du en graf vi har laget til å vise frem meningene om hvorfor de mente meldingen ser ekte ut.

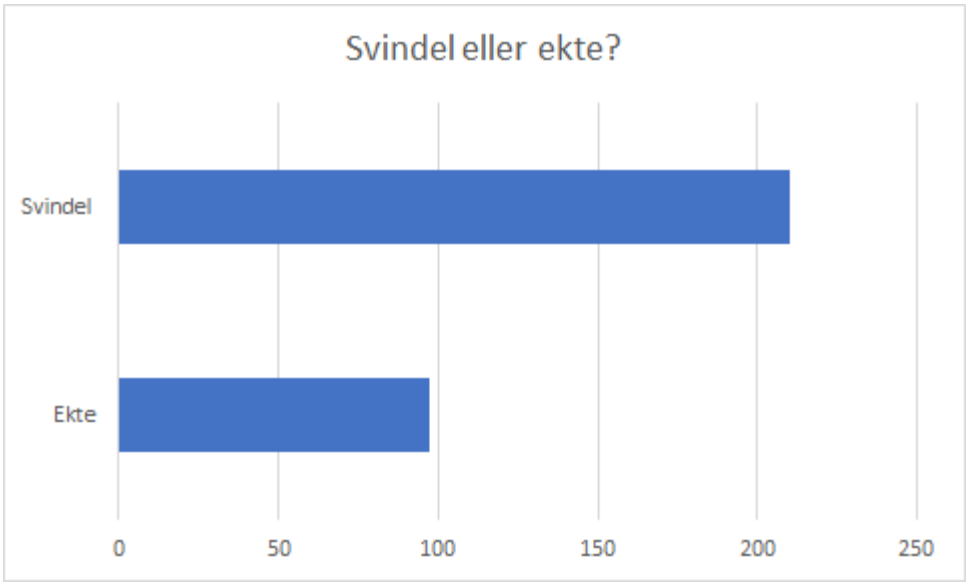


Det er totalt 24 personer som har svart at meldingen fra Netflix var ekte. Det er noen personer som har valgt flere alternativer. 16 personer svarte at kontoen kan være sperret, 7 personer svarte linken ser troverdig ut, og 4 personer svarte at alle meldinger kommer fra Netflix. Resten har svart at meldingen ser ekte ut, og noen ville logget inn på kontoen og sjekket.

Spørsmål 4:

Svindel eller ekte? *

- Svindel
- Ekte



Det er totalt 314 som har svar på dette spørsmålet, hvorav 215 svarte at det var svindel og 99 som svarte at konkurransen var ekte.

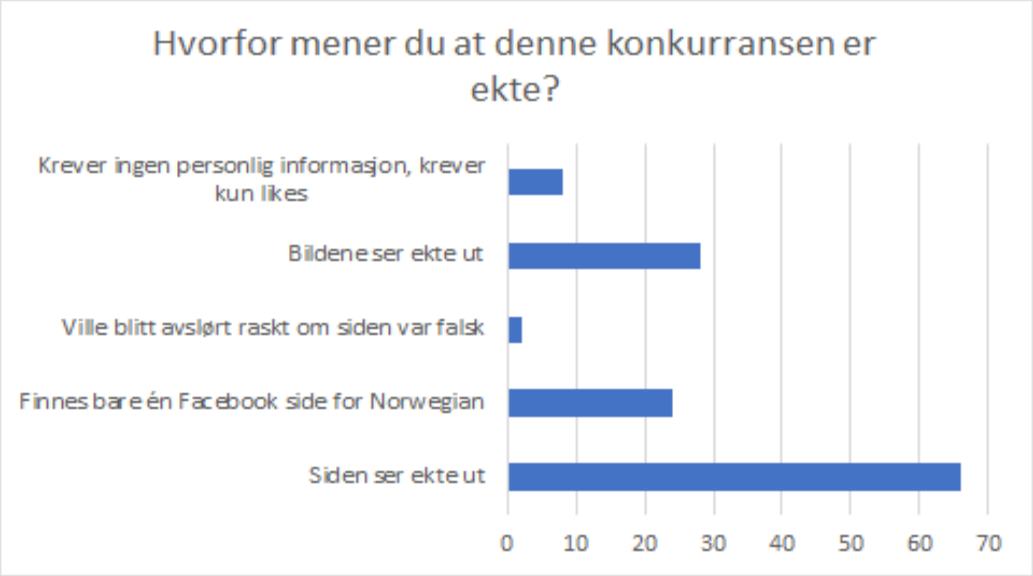
Underspørsmål 4.1:

Nedenunder ser du en graf på hvorfor og antall mennesker svarte det på at det var en svindel.

Det er totalt 215 personer som har svart at konkurransen var ekte. Det er noen personer som har valgt flere alternativer. 133 personer svarte at det er skrivefeil i beskrivelsen, 129 svarte at Norwegian heter bare Norwegian på Facebook, og 117 svarte at det står fansite i kolonnen til venstre. Resten svarte at det er altfor lite bilder/innhold på Facebook side, konkurransen bryter regler/virker "for god til å være sann, og den oppgir feil informasjon

Underspørsmål 4.2:

Nedenunder ser du en graf vi har laget til å vise frem meningene om hvorfor de mente meldingen ser ekte ut.

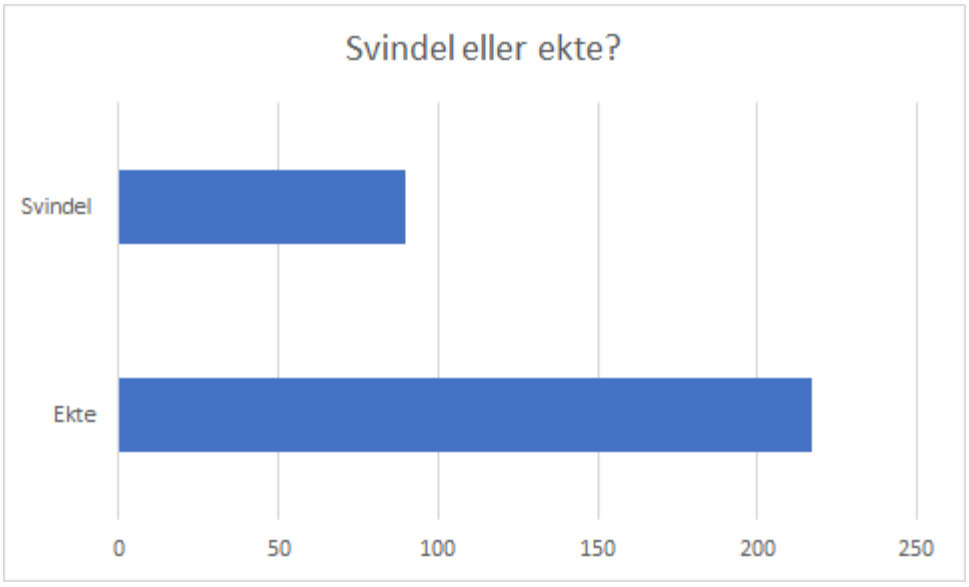


Det er totalt 99 personer som har svart at konkurransen var ekte. Det er noen personer som har valgt flere alternativer. 67 personer svarte at siden ser ekte ut, 29 har svart at bildene ser ekte ut, og 25 har svart at det bare finnes en Norwegian side på Facebook. Resten svarte at konkurransen ikke krever personlig informasjon, men kun likes, og noen svarte at siden ville blitt raskt avslørt om den var falsk.

Spørsmål 5:

Svindel eller ekte? *

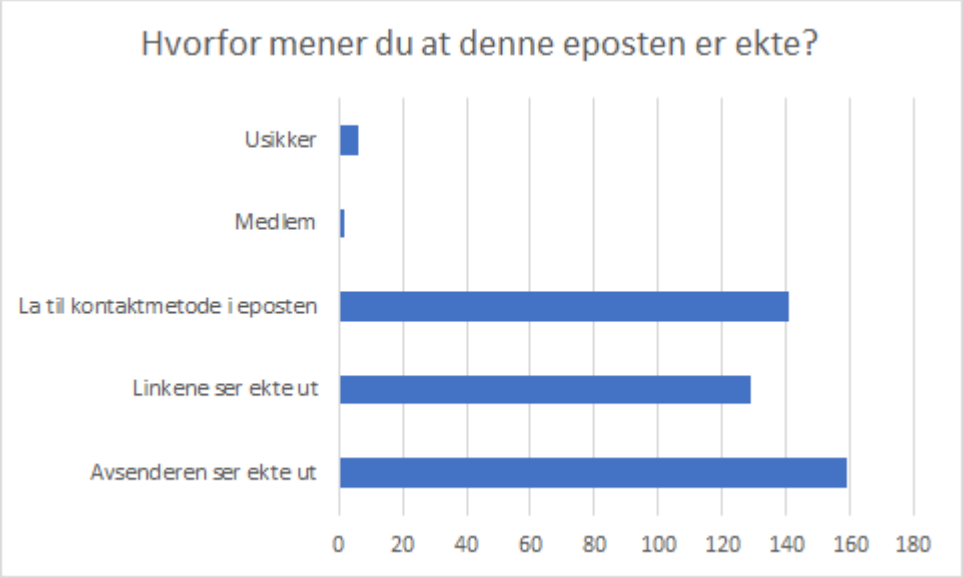
- ○ Svindel
- ○ Ekte



Det er totalt 314 som har svar på dette spørsmålet, hvorav 91 svarte at det var svindel og 223 som svarte at eposten var ekte.

Underspørsmål 5.1:

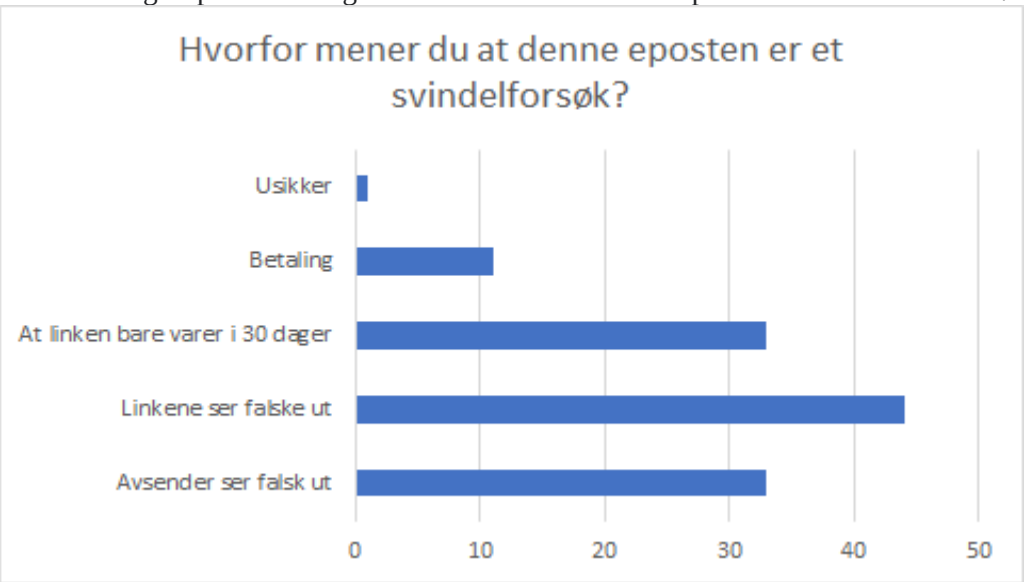
Nedenunder ser du en graf vi har laget til å vise frem meningene om hvorfor de mente meldingen ser ekte ut.



Det er totalt 223 personer som har svart at eposten var ekte. Det er noen personer som har valgt flere alternativer. 165 personer svarte at avsenderen ser ekte ut, 145 personer svarte at de la til kontaktmetoden i eposten, og 135 personer svarte at linkene i eposten ser ekte ut. Resten svarte at noen var medlem der, og noen var usikker på om den var ekte eller svindel.

Underspørsmål 5.2:

Nedenunder ser du en graf på hvorfor og antall mennesker svarte det på at det var et svindelforsøk.

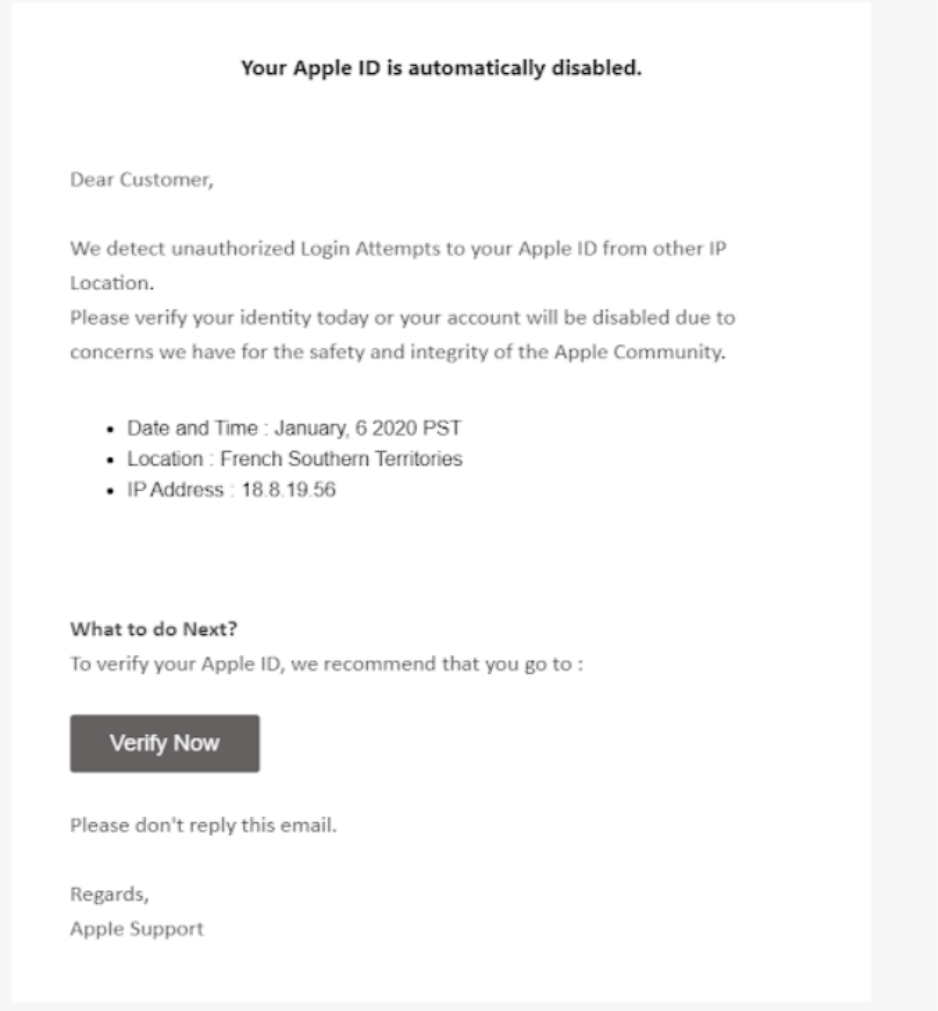


Det er totalt 91 personer som har svart at eposten var svindel. Det er noen personer som har valgt flere alternativer. 42 personer svarte at linkene ser falske ut, 33 personer svarte at avsenderen ser falsk ut, og 32 personer svarte at linken bare varer i 30 dager. Resten svarte de ber om betalingsinformasjon i eposten, og noen er usikker på om eposten er ekte eller svindel.

Spørsmål 6:

Svindel eller ekte? *

1 poeng



Your Apple ID is automatically disabled.

Dear Customer,

We detect unauthorized Login Attempts to your Apple ID from other IP Location.
Please verify your identity today or your account will be disabled due to concerns we have for the safety and integrity of the Apple Community.

- Date and Time : January, 6 2020 PST
- Location : French Southern Territories
- IP Address : 18.8.19.56

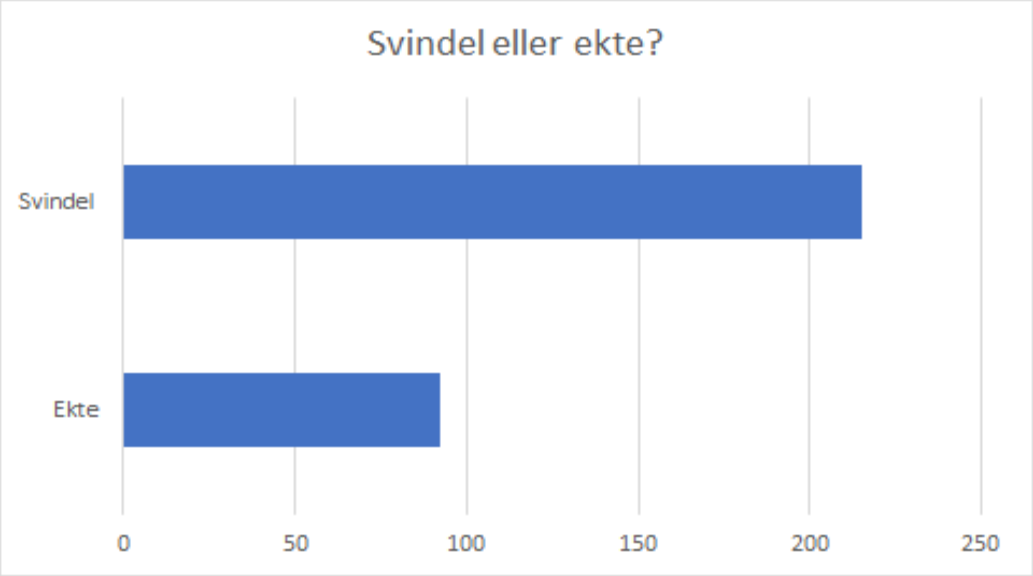
What to do Next?
To verify your Apple ID, we recommend that you go to :

Verify Now

Please don't reply this email.

Regards,
Apple Support

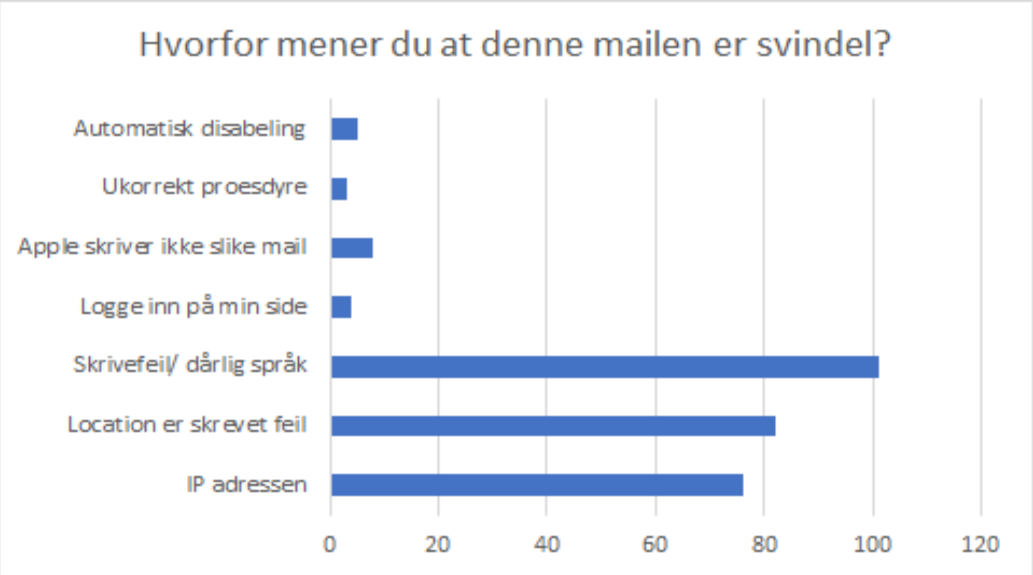
- ○ Svindel
- ○ Ekte



Det er totalt 314 som har svar på dette spørsmålet, hvorav 221 svarte at det var svindel og 93 som svarte at eposten var ekte.

Underspørsmål 6.1:

Nedenunder ser du en graf på hvorfor og antall mennesker svarte det på at det var en svindel.

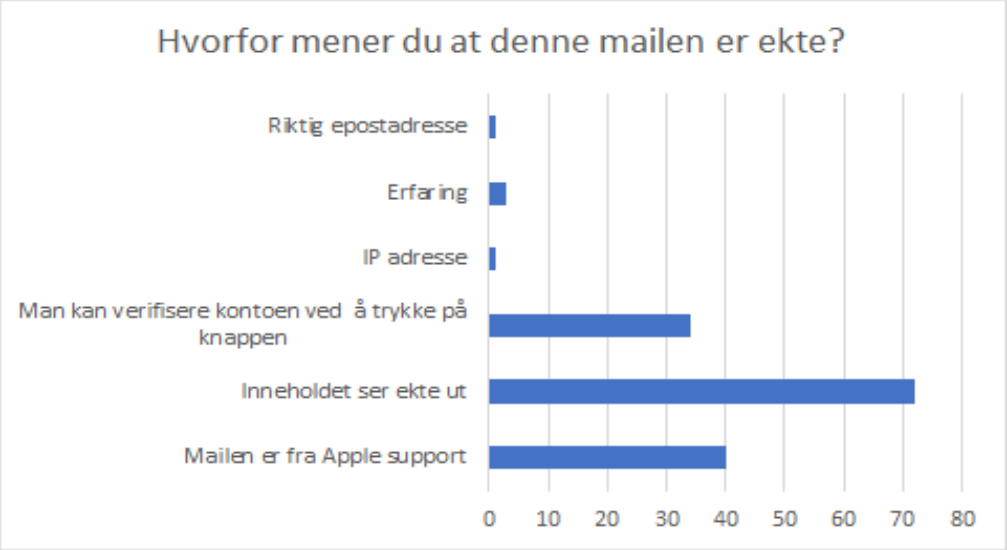


Det er totalt 221 personer som har svart at eposten var svindel. Det er noen personer som har valgt flere alternativer. 103 personer svarte at det var skrivefeil i eposten, 84 personer svarte at "location" var skrevet rart, og 80 personer

syntes det var noe rart med IP adressen. Resten svare at Apple ikke skriver slike eposter, ukorrekt prosedyre å utføre, automatisk disabling og noen ville logget inn på min side på Apple.

Underspørsmål 6.2:

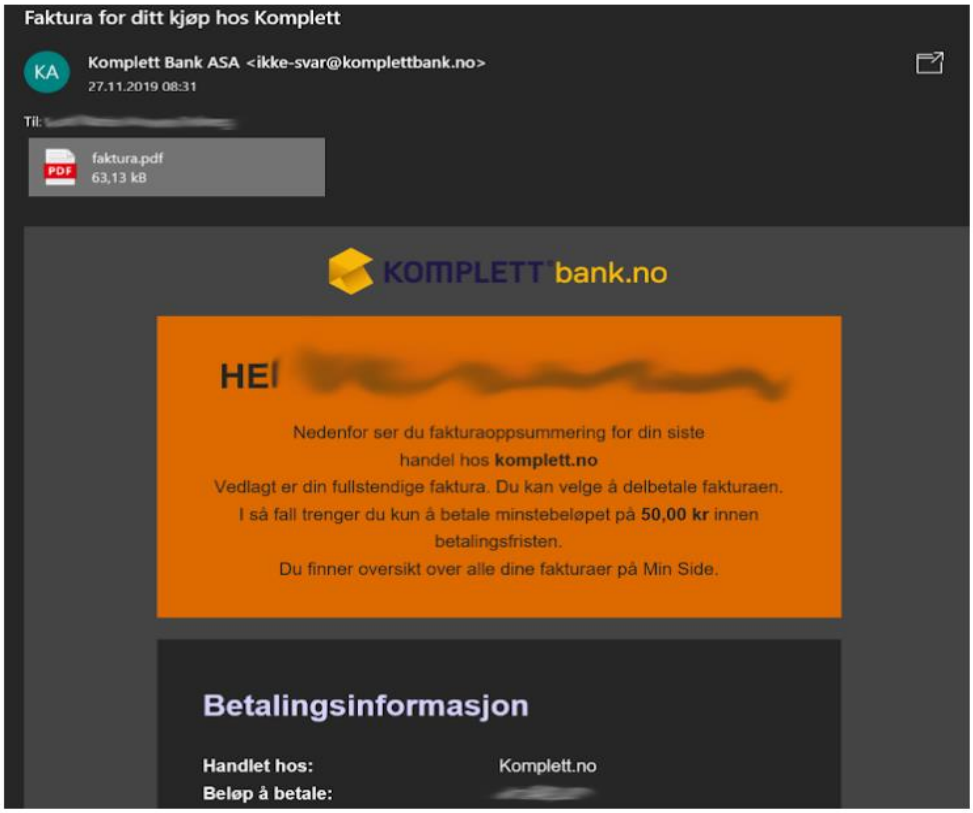
Nedenunder ser du en graf vi har laget til å vise frem meningene om hvorfor de mente meldingen ser ekte ut.



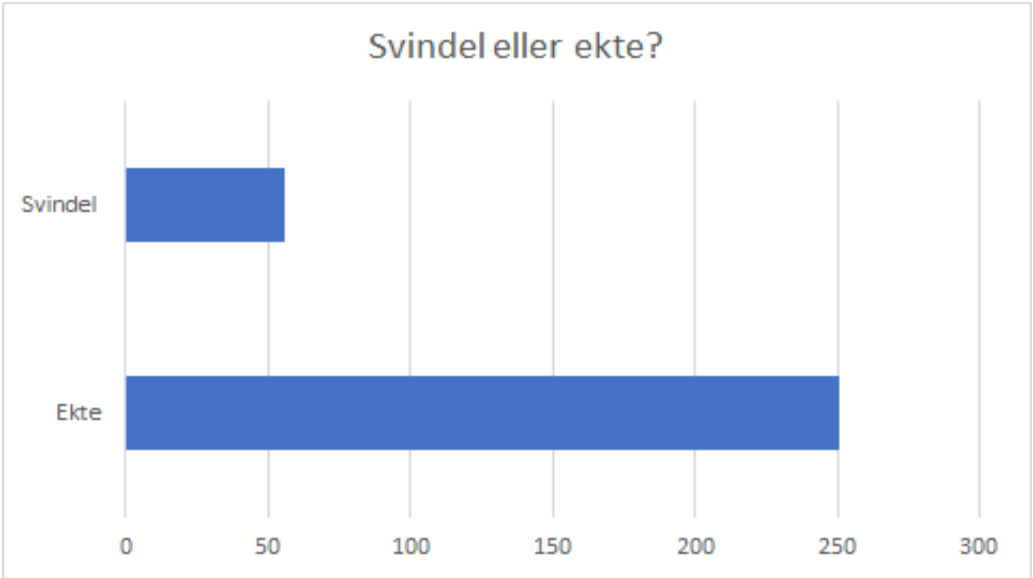
Det er totalt 93 personer som har svart at eposten var ekte. Det er noen personer som har valgt flere alternativer. 73 personer svarte at innholdet i eposten ser ekte ut, 41 personer svarte at eposten er fra Apple support, og 34 personer svarte at man kan verifisere kontoen ved å trykke på knappen. Resten svarte de har fått en lignende epost fra Apple før, at det er riktig epostadresse og at IP adressen er riktig.

Spørsmål 7:

Svindel eller ekte? * 1 poeng



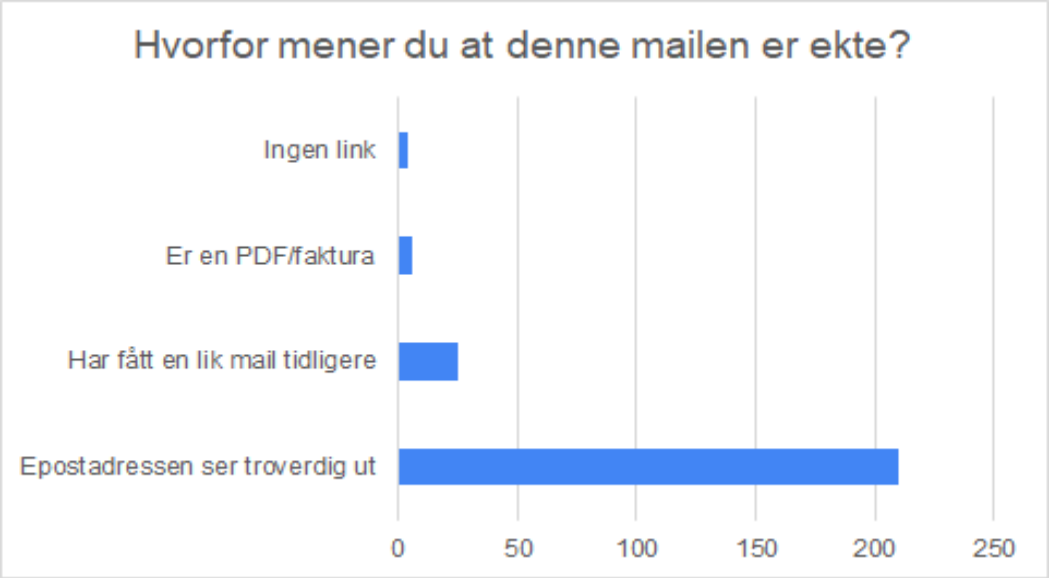
- ○ Svindel
- ○ Ekte



Det er totalt 314 som har svar på dette spørsmålet, hvorav 60 svarte at det var svindel og 254 som svarte at eposten var ekte.

Underspørsmål 7.1:

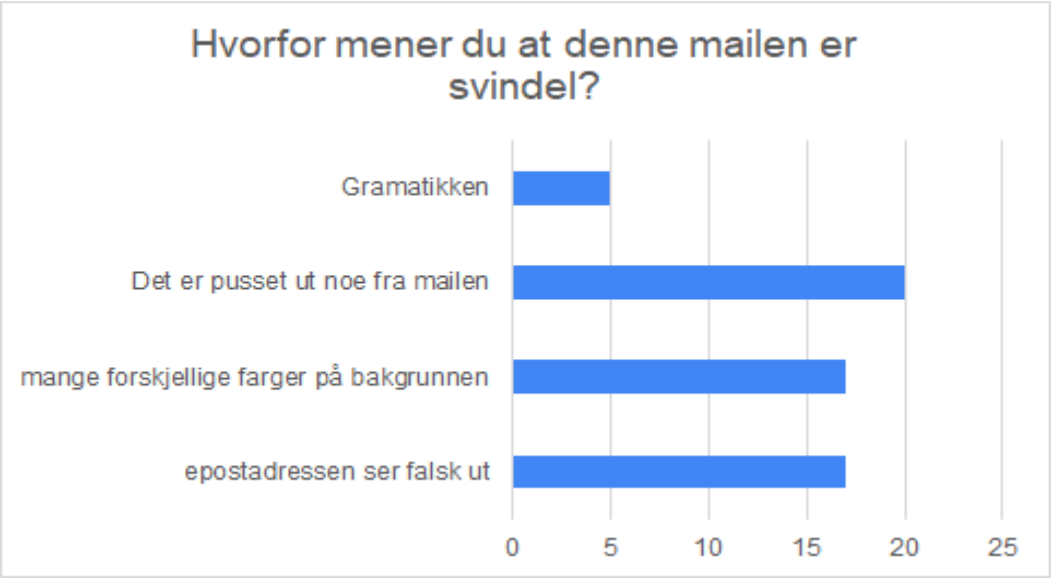
Nedenunder ser du en graf vi har laget til å vise frem meningene om hvorfor de mente meldingen ser ekte ut



Det er totalt 254 personer som har svart at eposten var ekte. Det er noen personer som har valgt flere alternativer. 213 svarte at epostadressen ser troverdig ut, og 63 svarte at de har fått en lik epost tidligere. Resten har svart at det ikke finnes noen linker i eposten, og at det er vedlagt en PDF/faktura.

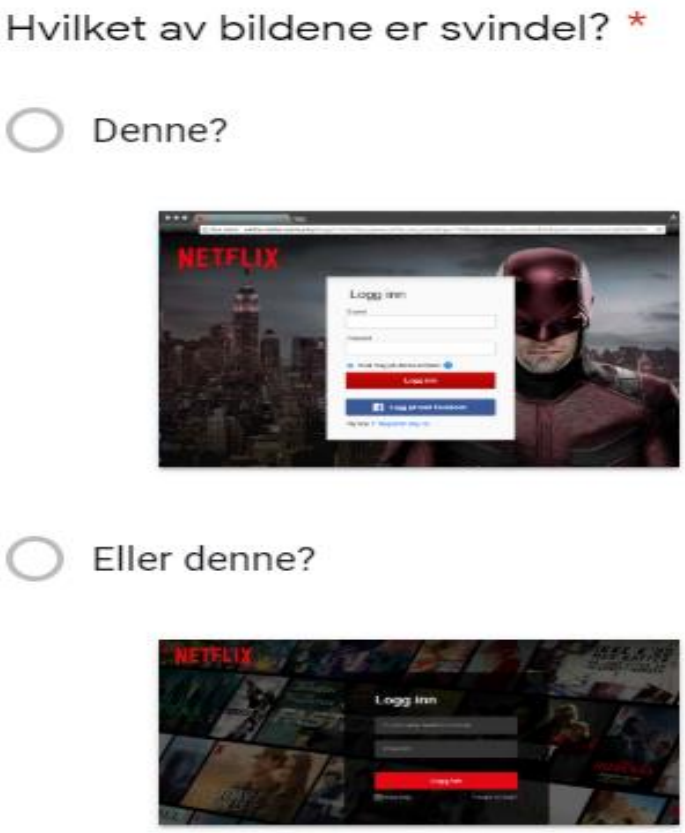
Underspørsmål 7.2:

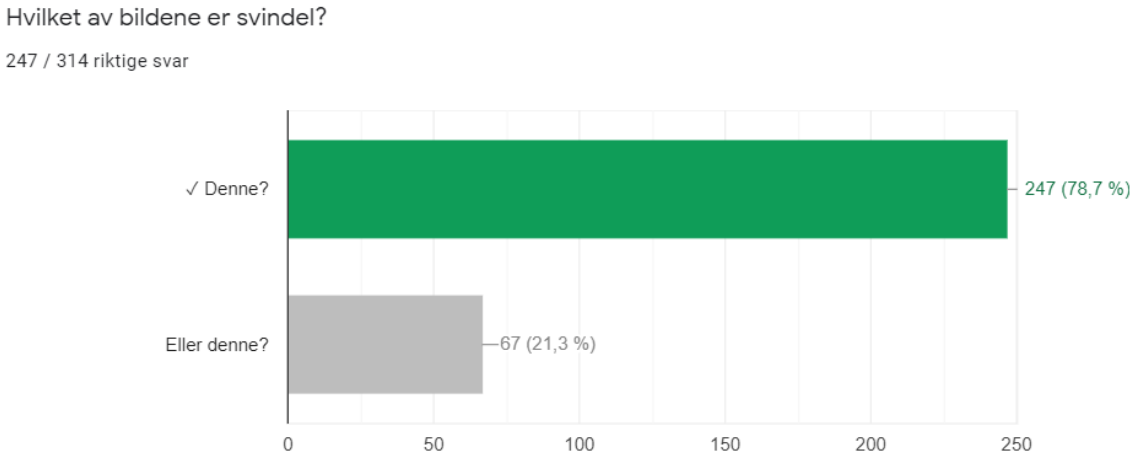
Nedenunder ser du en graf på hvorfor og antall mennesker svarte det på at det var en svindel.



Det er totalt 60 personer som har svart at eposten var svindel. Det er noen personer som har valgt flere alternativer. 20 personer svarte at epostadressen ser falsk ut, 20 personer svarte at det er pusset noe ut fra mailen, og 17 personer svarte at det var mange forskjellige farger på bakgrunnen. Resten svarte at gramatikken i eposten var dårlig

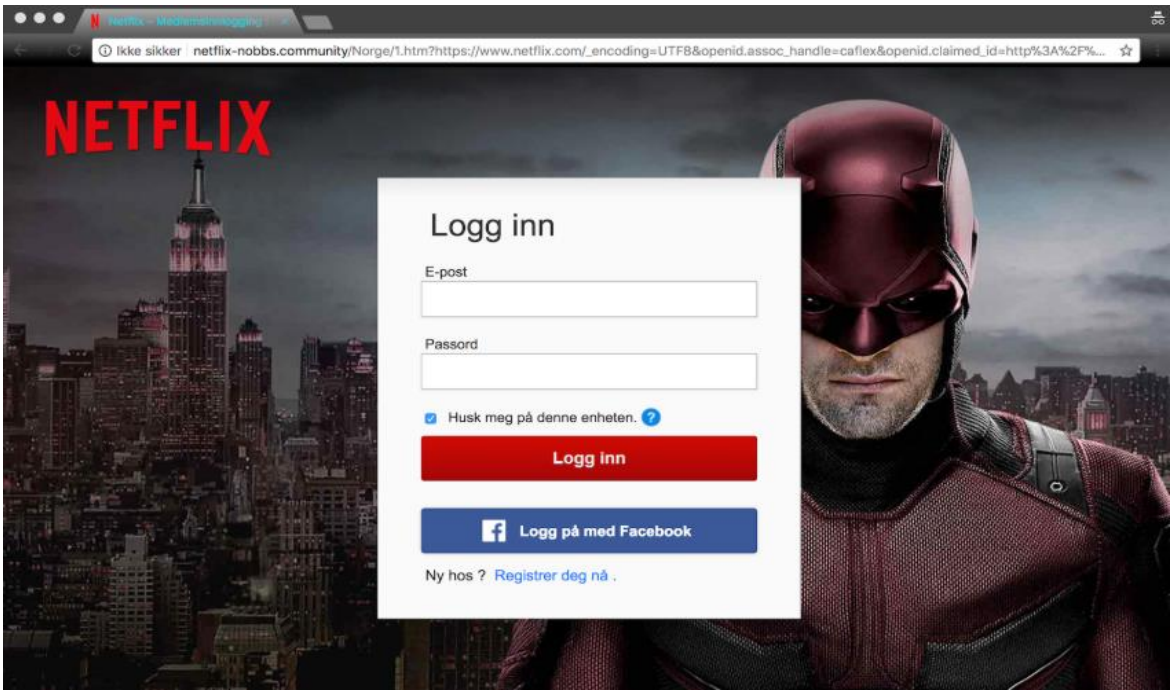
Spørsmål 8:





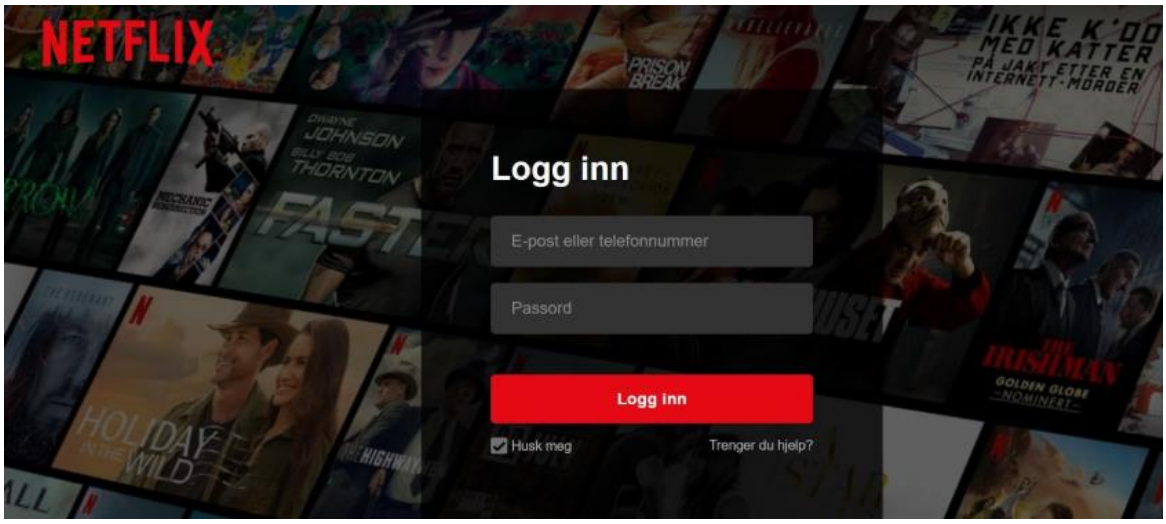
Her er det 247 personer som har svart det første alternativet som er riktig svar, og 67 som har svart det andre alternativet som er feil svar. Totalt er det 314 svar på spørsmålet.

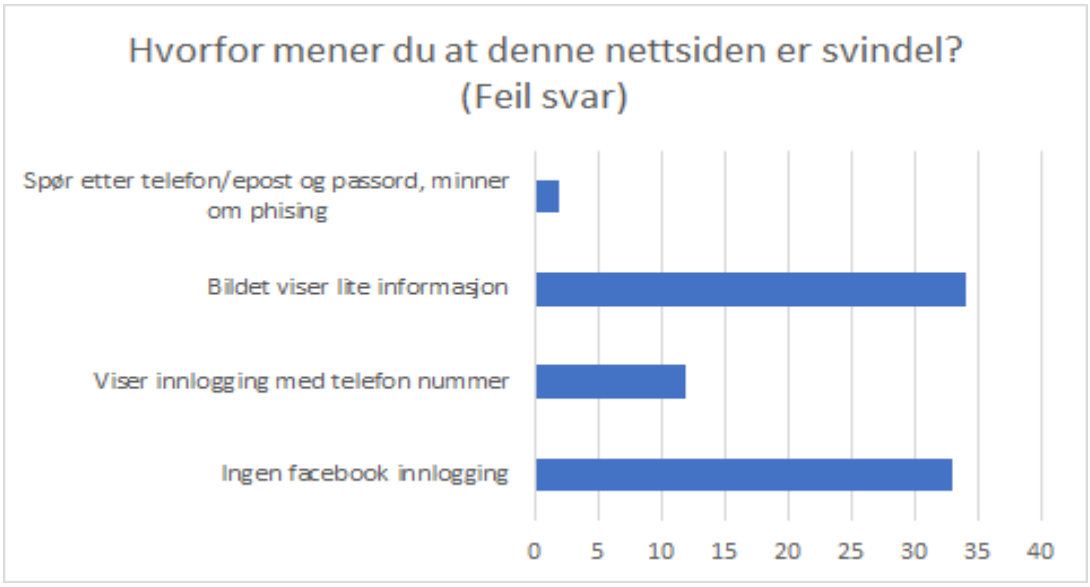
Underspørsmål 8.1(Riktig)



Det er totalt 247 personer som har svart at denne nettsiden er svindel. 180 har svart at nettadressen ser lang og rar ut, 163 har svart at man ikke kan logge inn på netflix med facebook, og 128 har svart at “ny hos?” ikke ser riktig ut. videre har 29 svart at det var en gammel serie. Det har også vært en del som har svart annet, og vi har oppsummert det her. Cirka 17 personer svarte at det ikke var sikker tilkobling på siden, og cirka 11 svarte at bakgrunnsbilde ikke stemte overens med netflix.

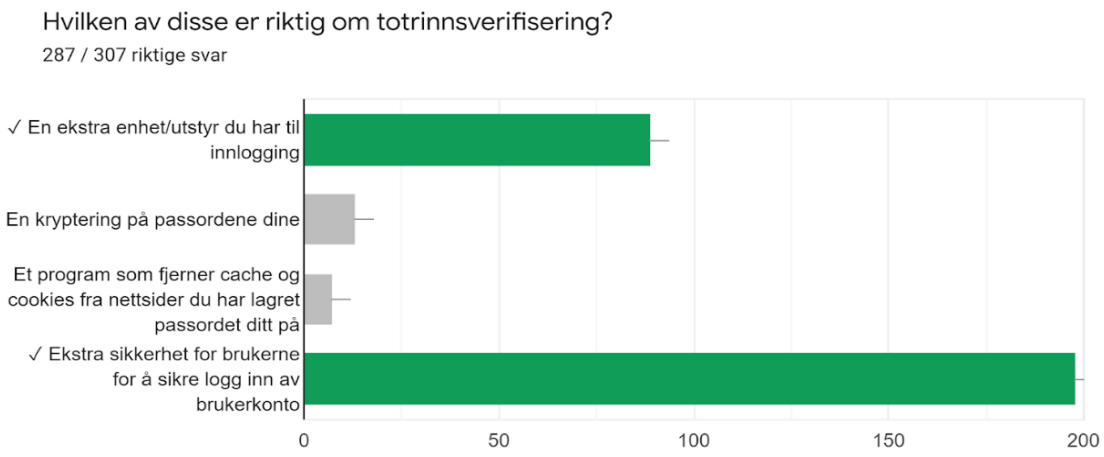
Underspørsmål 8.2(Feil)





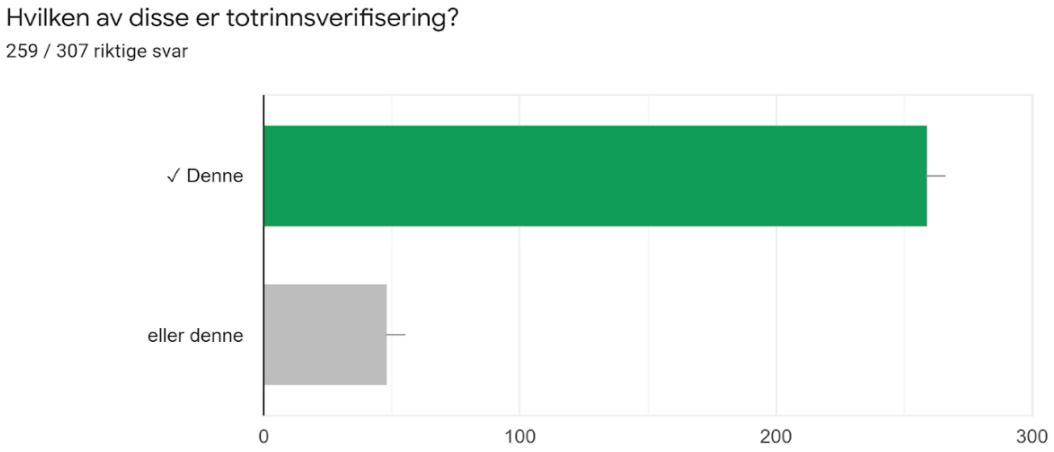
Totalt 67 personer har svart at denne nettsiden er svindel (feil svar), hvorav 34 har svart at bilde gir for lite informasjon, 33 har svart at det mangler facebook innlogging, 12 har svart at det viser innlogging med telefon nummer, og 2 har svart at de spør etter telefon/epost og passord, og at dette minner de om phising.

Spørsmål 9:



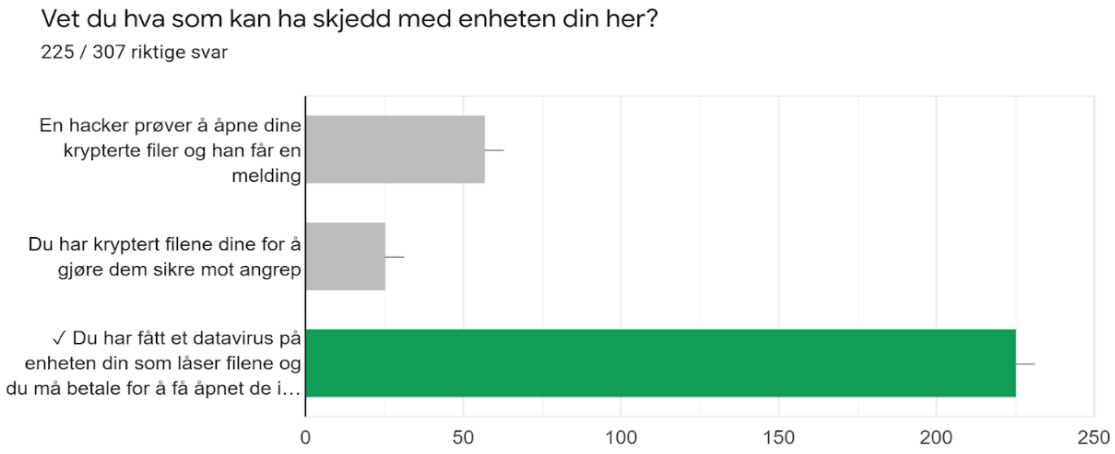
Her ser vi at flesteparten har svart riktig. Men noen har fortsatt svart feil. Her svarte 93,5 % riktig.

Spørsmål 10:

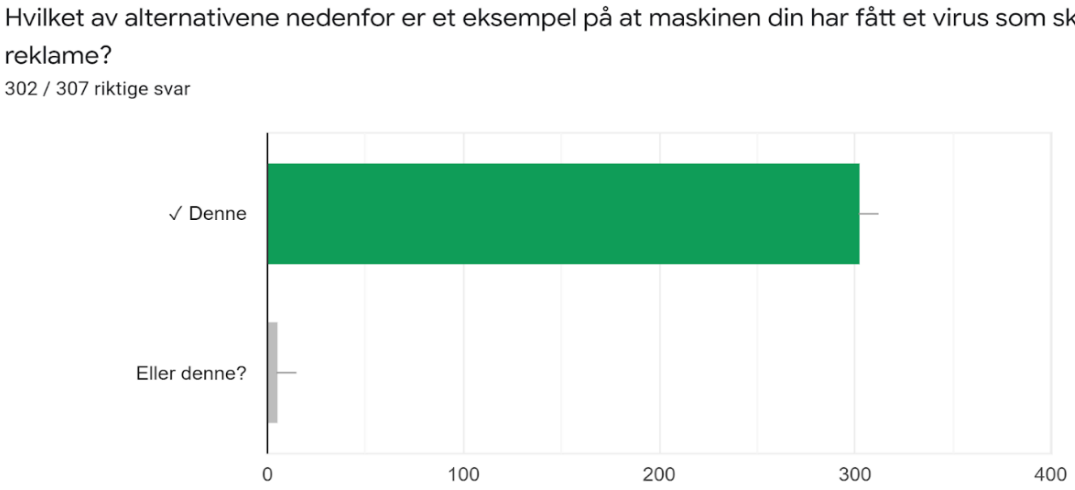


Fra vårt forrige spørsmål om toveis verifisering fikk vi et svart prosent på over 93 prosent svarte riktig men da vi lagde et bilde spørsmål som skulle egentlig vært mye enklere svarte faktisk folk mer feil med 15,8% feil svar. Dette sier oss at de vet nok mindre enn det de tror.

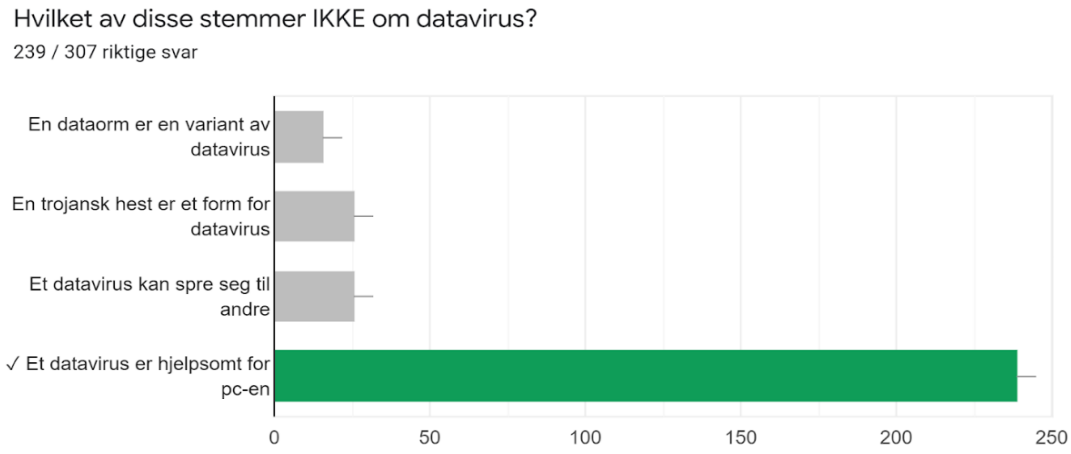
Spørsmål 11:



Spørsmål 12:



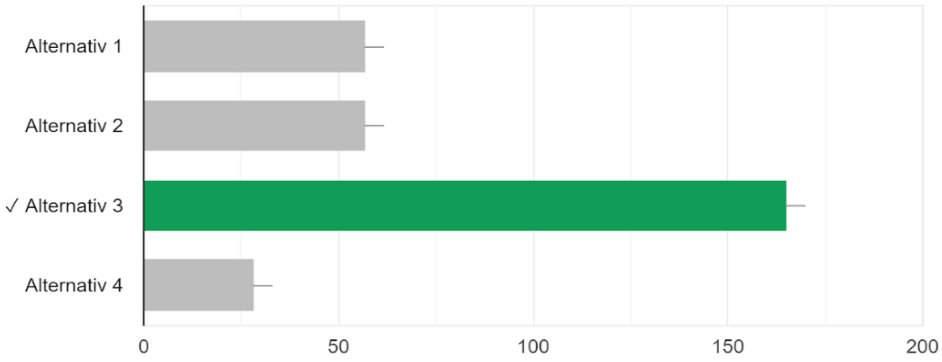
Spørsmål 13:


Hvilket av disse stemmer IKKE om datavirus?
239 / 307 riktige svar
En dataorm er en variant av datavirus
En trojansk hest er et form for datavirus
Et datavirus kan spre seg til andre
✓ Et datavirus er hjelpsomt for pc-en
0
50
100
150
200
250

Spørsmål 14:

Kan du se hvilket av disse som er en form for pålitelig antivirus? Antivirus er noe som prøver å forhindre og fjerne skadevare på din enhet.

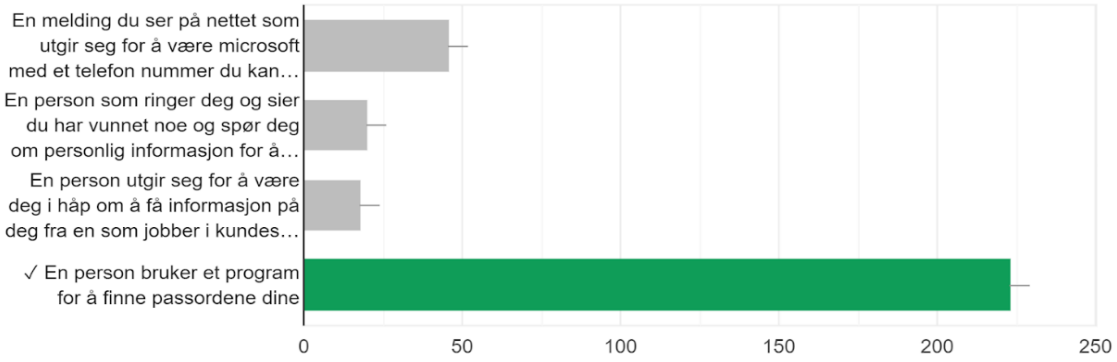
165 / 307 riktige svar



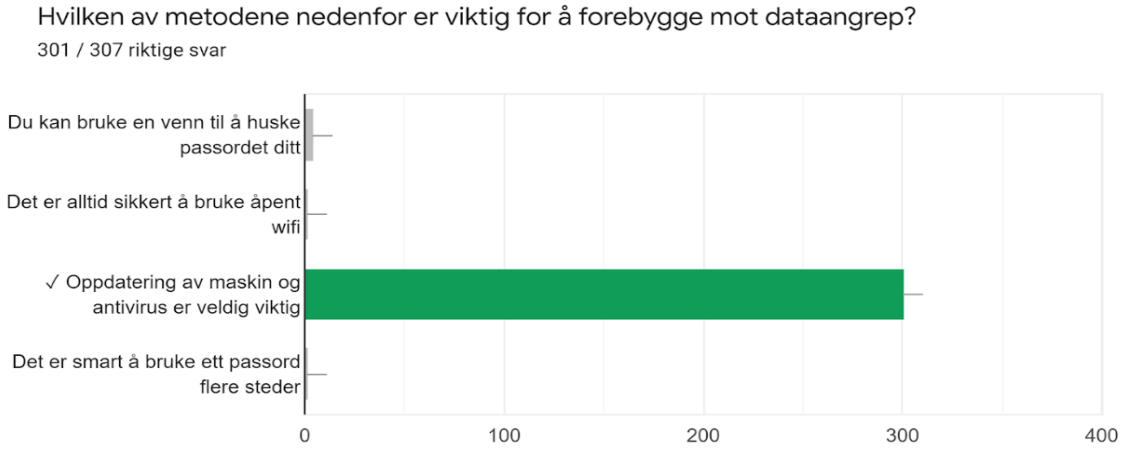
Spørsmål 15:

Hvilken av de metodene nevnt nedenfor er IKKE en form for at mennesker prøver å bruke psykologi til å hente ut informasjon?

223 / 307 riktige svar



Spørsmål 16:


Hvilken av metodene nedenfor er viktig for å forebygge mot dataangrep?
301 / 307 riktige svar
Du kan bruke en venn til å huske passordet ditt
Det er alltid sikkert å bruke åpent wifi
✓ Oppdatering av maskin og antivirus er veldig viktig
Det er smart å bruke ett passord flere steder
0
100
200
300
400

13.2 Vedlegg 2: Semistrukturert intervju

Spørsmål

1) Aldersgruppen 30-39 er best på datasikkerhet, er du enig i denne påstanden? hvorfor / hvorfor ikke?
2) Hvilken arbeidssektor tror du er best på datasikkerhet? Hvorfor tenker du det?
3) Vet du om noen dataprogrammer/mekanismer/metoder som man kan benytte seg av for å ha bedre datasikkerhet?
4) Hva er dine tekniske ferdigheter?
5) Hvordan beskytter du deg mot dataangrep? Hvordan kan du?
6) Hvor skeptisk føler du at du er på internett?
7) Kjenner du til noen former for hacking?
8) Kjenner du til noen former for totrinnsverifisering? Hvilke?
9) Bruker du noen slags totrinnsverifisering?
10) Kjenner du til noen antivirus programmer? Hvilke?
11) Bruker du antivirus programmer?
12) Holder du maskin/maskinvare oppdatert?
13) Kjenner flere enn deg passordet/passordene dine?
14) Bruker du samme passord flere steder?
15) Har du noen gang lagt merke til at noen har prøvd å hacke deg?
16) Hvilke kvaliteter/egenskaper har en hacker?

17) Har du arbeidet annerledes etter Corona krisen?
18) Vil du si at du bruker mer internett privat eller i arbeid? Hvordan bruker du internett?
19) Bruker du noen programmer mer etter krisen?
20) Føler du at det at det er noen begrensninger i arbeid?

Svar på spørsmålene

Respondent 1

1) Ja, fordi denne aldersgruppen er mest oppdatert. Livserfaring og modenhet betyr en del.
2) Helse, viktig å verne pasientinformasjonen. Konfidensielle opplysninger.
3) Antivirusprogram. Har hørt om Mcafee.

4) Dårlige tekniske ferdigheter. Lært om noe da hun gikk på skolen. Klarer å svare på e post og skrive i word. Gå i banken. Bruker bankid på telefon aldri på pcen. Bruker bare pc til å skrive lengre tekster ellers så går det primært på telefon. feks leser mail, Surfer på nettet, leser nyheter. Er ho hjemme så googler ho på pcen.
5) Bruker enkle passord. Har vanskelig passord på jobb. Kan legge filer i en cloud istedenfor å lagre dem på pcen.
6) Stoler ikke på alt. Veldig skeptisk til mail, sms og messenger. Kjenner ho ikke personen den kommer fra så åpner ho ikke mailen. Er en mail spoofet til en person ho kjenner så klarer ho alltid å se feil i språket. Grammatikken feks. Dobbel sjekker på ekte nettsider om meldinger. Står vanligvis på nett om det er svindel.
7) Har hørt om trojaner. Lurer deg til å åpne filer men viser seg å være virus.
8) Ja, du har to koder. Har det i banken. Ja har det også når ho skal logge seg på telefonen sin. Telenor har en kode og telefonen har en kode.
9) Ja, har sagt det alt. Banken
10) Ja, har sagt det alt. Mcafee
11) Ja, mcafee
12) Ja, oppdatere telefon med engang aldri pcen.
13) Ja til pcen. Og telefon.
14) Ja, et passord til 5 forskjellige steder. mail, facebook/google, messenger,
15) Ja på meldinger som sms, epost og messenger meldinger. Du har vunnet noe fra kiwi, bitcoin noe, veldig mye om penger.
16) Nysgjerring, prøver å knekke en kode. Flink på en måte. Flink på datasikkerhet, kan sikkert få seg en bra jobb ærlig.
17) Nei, kanskje jobbet litt mer.
18) Mer i privat. Leser nyheter googler viere hvis ting er interessant. Skriver/svarer på eposter. Chatter på messenger/ringer familie og venner. Dating sider.
19) Leser mer nyheter.
20) Må bare vaske seg oftere på jobben. Vasker husket og ting oftere. Kan gjøre akkurat det samme som før bare må tenker seg gjennom over hygiene.

Respondent 2

21) Nei, 40-50. Mer erfaring. Livserfaring.
22) IT og økonomi. IT. Jobber med IT. Burde kunne mest

23) To trinns verifisering. Teipe over web kamera. Dobbel sjekk eposter du mottar. Haveibeenpwned nettsiden. Langt/sterkt passord med tegn og tall/store/små bokser/spesial tegn.
24) Gjennomsnittlig god. Antivirus.
25) Antivirus programmer. To trinnsverifisering.
26) Lite skeptisk. Tror ikke noen skal hacke henne. Har ingenting som gjør henne sårbar.
27) Trojaner. Spider-web. Social engineering(folk som ringer deg). Epost phishing.
28) Du har noe i hånda. Epost verifisering. Banken, kodebrikke eller bankid på telefon.
29) Svart på alt.
30) AVG
31) Husker ikke, tror avg
32) Oppdatere telefon når ho får besked om det. Oppdatere ikke med engang på pc(kommer an på situasjonen.
33) Nei
34) Ja, noen steder. Lager varianter av et passord flere steder. Ja bruker også samme passord på kritiske steder.
35) Ja, trykk på linker i meldinger på epost, telefon.
36) Analytisk og metodisk. Må kunne se hele bildet. Må vite hva du driver med/gjør ting riktig.
37) Nei,
38) I privat. Spiller på telefon. Leser nyheter. Hører på podcasts. Musikk på spotify. Leser/svarer på eposter. Messenger (men ikke så ofte).
39) Spiller mer.
40) Ble satt i karantene. Kan ikke jobbe.

Respondent 3

1) Ja, generasjon som har fått mer data kunnskaper. Født inn i data tiden.
2) IT. Har bakgrunnen for det gjennom utdanning feks
3) Ingen aning

4) Meget dårlig. Ingen.
5) Har ikke peiling
6) Komfortabel, tilitt til skaperen. Stoler på mye.
7) Nei
8) Nei
9) nei, men vet hva det er etter forklaring
10) Har antivirus men vet ikke hva
11) Ja, går automatisk
12) Ja, men vet ikke hva
13) ja. konen hans. Enkler å huske. Jobber tettere sammen
14) Ja, nesten samme på alle steder. Enkelt å huske.
15) Ja,fått eposter om spam og sånt. Svarer ikke
16) Kriminell. Datanerd. Ute etter vinning.
17) Nei
18) Bruker det like mye
19) Nei
20) Nei

Respondent 4

1) Ja, pga kombinasjonen bredden av livserfaring (kunnskap, erfaringer), modenhet, relativt up-to-date mht data
2) Sektorer: Forsvaret, bank, energi, skatteetaten, offshore. Fordi disse jobber med faktiske trusler, "angrep" og sikkerhetsoperasjoner daglig og har mer bevisst forhold til risikovurderinger. Helse har vist til mange saker der de ikke har tatt sikkerhet på alvor.
3) Ja. Den menneskelige faktor er stor. Dessuten: "inherent capabilities" og IT-oppsett. Så er det bruk av verktøy som fysisk og IT-adgang/tilgangskontroll, passord, brannmur, VPN, anti-virus...
4) Mange: noen er nevnt over.
5) Bruker brannmur, lukkede nett, VPN, anti-virus, passord, holder meg unna nettsider som klassifiseres som "farlige".
6) Nok.
7) Ikke-autorisert inntrengning, datatyveri, forfalsking/manipulering av data, ødeleggelse av informasjon (destruction), stansing av informasjonsflyt (denial).
8) Ja, feks innlogging/passord og "fingeravtrykk" som ved innlogging i bank
9) Se svar pkt 8
10) Ja. McAfee, Norton, F-secure

11) Ja
12) Ja.
13) Nei
14) Ja.
15) Ja, det sier iallefall McAfee...
16) Dårlig moral og sikkert litt flink med data
17) Tja, mindre fysisk kontakt med andre
18) Mest privat
19) Nei
20) Ja, den fysiske komponenten

.

Respondenten 5

1) Ja, det er første generasjon som vokste opp med data.
2) Økonomi, handler om penger. Er nazi i bank. Regnskap. Sensitiv informasjon
3) Windows defender, Norton, Sophos. Unngå shady nettsider. Ha et bra passord. Forskjellige passord. Bytt passord ofte.
4) Helt normalt. Kan alt, kan google seg til løsninger selv men stor problemer ringer han it vakta. Klarer ikke programere.
5) Sophos. Antivirus. Bra passord. Varsom på mails.
6) Lite skeptisk fordi han har gode nok it kunnskaper til å se hva som er en trussel.
7) Ransomware. Fake microsoft som ringer, epost som sier han har vunnet penger
8) At du har et brukernavn, passord og bankid.
9) Bruker det med betaling, dvs bankid. og andre sider hvor han bruker bankid til innlogging som altinn.
10) Sophos, Nox, Windows defender, Mcafee
11) Sophos (jobb antivirus) Nox på telefon som han har fått fra samsung
12) Ja, på alle enheter. Har ikke privat pc
13) Nei, it avdelingen kan finne jobb passordet hans da.
14) Ja, enklere å huske. Bruker også forskjellige passord.
15) Ja, han har fått mail på jobb eposten sin. En av kollegaen hans svarte og fikk ransomware.
16) Flink med data. Slu, kriminelle, Har det sikkert gøy
17) Det blir mindre face to face møter. Bruker teams og skype istedenfor.
18) Helt likt. Bruker internet hele dagen rundt
19) Bruker skype/teams istedenfor face to face møter.
20) Ja, viktig med møter over bordet men han må ikke

Respondent 6

1) Fordi de har vært med på hele «datareisen»
2) De som jobber innenfor IT, fordi de må jo være best?
3) Vpn,brannmur
4) Middels
5) Annet en det som er med på PC og i ruter .. bruker vpn i jobb
6) Ikke skeptisk
7) «Datapakkeangrep» for å krasje servere?
8) BankID på mobil + pin , bankid + pin ,faceid + pin
9) Alle de over
10) Norton
11) Nei
12) Ja
13) Ja
14) Ja
15) Ja en kompis gjorde det for moro skyld..
16) Over middels int i PC , glad i grandis og cola?
17) Ja
18) 50/50
19) Nei
20) Nei

Respondent 7

1) Ja, tror det. Tror de er mer erfarne enn den gjennomsnittlige populasjonen, de har mer erfaring.
2) IT, Tror det er siden de har innsikt i hvordan de tekniske tingene faktisk fungerer, ikke bare direkte skam mail, men også hva man ikke bør gjøre. De har vanskeligere for å bli lurt av direkte skam, siden det er mer snakket om i det community.
3) Så lenge du har et operativsystem som er mye brukt, så skal ikke det være et problem. Nettleseren kan være viktig, mye brukt nettleser som støtter funksjoner som forteller når ting ikke er kryptert. Spamfilteret kan være nyttig. Flerfaktorautentisering bør brukes der det lar seg gjøre. Holde seg oppdatert på hvilke tjenester du bruker, og hvordan de håndterer dataen din siden man ikke vet mye om hva de gjør med den.
4) Tilstrekkelig, kan en del om websikkerhet for eksempel, og så har jeg kjennskap til hva som er legit og ikke, kan identifisere skam. Kan jo filtrere ut spam for eksempel.
5) Holder operativsystemet mitt oppdatert, og bruker bare de tjenestene jeg vet er krypterte og sikre, og er selektiv med informasjonen min og, prøver å holde den til få plattformer. Bruker ikke offentlig nett. (hvorfor ikke?) fordi det er enkelt å intercepte det. Bruker flerfaktorverifisering på alle tjenester, og passer på at all data er kryptert.
6) Vil si jeg er ganske skeptisk, tenker over om det er farlig hver gang jeg ser en link i en mail for eksempel. Passer på å ikke gi informasjon om meg til tjenester jeg ikke stoler på.
7) Bortsett fra phising, er det blitt begrenset hva en hacker kan gjøre direkte. Keylogger, trojanere, worms, alt mye sånt. Det jeg ville vært varsom mot nå er offentlige nett og phising og at de applikasjonene som behandler informasjonen ikke er svake på sikkerhet. Cross-site-scripting
8) Avg, Norton, macafee. Windows defender er neste
9) Windows defender
10) Ja, holder OS og software oppdatert.
11) Nei. Password manager, bruker hovedsak keeper og google sin manager
12) Ja, men på viktige ting så har jeg eget passord. (Hva er viktige ting?) Bank passord, utdanning institusjon, store tjenester, Instagram, Facebook.
13) Har du noen gang lagt merke til at noen har prøvd å hacke deg?
14) I forhold til store breaches men ikke noe annet enn det. Jeg vet at noen av passordene mine har blitt leaked.
15) Teknisk anlagt, Kommer an på hvilken hat de er. Men hovedsak tekniske evner som gjør deg til en god hacker, men du kan også ha scam som store deler av det og da trengs ikke store tekniske kunnskaper. Vidt spekter. Nigerian prince til social engineering.
16) Brukt mye mer videochat konferanser. Bortsett fra det er det ikke stor forskjell. (Føler du at du må være mer tilgjengelig digitalt en før) Annet enn jobb sammenheng, nei.

17) Jeg vil si at det er lite merkbart, det blir mer mengde. Vil si at jeg bruker mer tid. For eksempel, de tre timene jeg brukte til trening før, blir nå brukt til jobbing via nettet.
18) Ikke med unntak av videokonferanser. Streamer dere skjermen mer? Ja. (Hvilke programmer?) zoom, google hangouts.
19) Nei. Bruker zoom nå, men brukte det ikke før. Erstatning for alt det meste vi trenger.
20) (Studentassistent) Konsultere studenter over videochat, som vi gjorde i klasserom før. Alt blir digitalisert med klasserom og sånn.
    Merker ikke at det er mange begrensinger for mitt arbeid/sektor, får gjort alle de samme møtene og, ja, undervisninga blir litt annerledes kanskje, men ikke så stor effekt på det. Tror jeg kunne gjort dette i lengre tid.

13.3 Vedlegg 3: Manus for den første filmen

Filmmanus

INT. ROMMET TIL SINDRE - DAY 1

Person 1 Går inn på mailen sin og finner en mail fra netflix, går inn på mailen og trykker på linken, og prøver å logge inn. Person 1 blir deretter sendt over til den originale netflix siden.

PERSON 1 Hei, Tom sier han på en nervøs måte

PERSON 2 Hei Sindre

PERSON 1 hvordan går det i disse tider?

PERSON 2 Nei, går bare bra med meg, hvordan går det med deg?

PERSON 1 Tja, jeg fikk jo en sånn mail fra netflix da. Har du også fått denne mailen?

PERSON 2 Nei, jeg har ikke fått en sånn mail. Når fikk du den?

PERSON 1 Fikk den i dag tidlig, rundt 6

PERSON 2 Jeg har også Netflix abonnomang, men jeg har ikke fått en slik mail

PERSON 1 Jeg trykket jo på linken i mailen, også kom jeg rett inn på en side som jeg logget inn på.
PERSON 2 hva skjedde når du prøvde å logge in?
PERSON 1 Siden ble bare oppdatert

Forklaringsmanus

INT. WEBCAMERA TIL MARTIN - DAY 1

Martin: hva skjedde egentlig nå? Det som skjedde her var at sindre ble utsatt for phishing forsøk. phising er at noen prøver å fiske ut sensitiv informasjon, som foreksempel: betalninginformasjon, kontoinformasjon og personopplysninger nå skal vi se på noen ting som sindre kunne gjort annerledes for å beskytte seg fra phishing forsøket. ser på e-posten Første man burde se på er avsender, som man ser her så kan man se e-post adressen som her er netflix noen tall også gmail.com som da ikke er mailen til netflix. Etter det så burde man se på gramatikken på mailen, er det noen skrivefeil i mailen ? for eksempel her er det skrevet "konto informasjon" istedenfor "kontoinformasjon" og istedenfor "å" skulle det stått "og". I tillegg til at e-posten var skrevet kort, og ville ha deg inn på en annen side raskt. Så burde man se på linken som er sendt, for å se om den sender deg til netflix.com, men som man kan se her, så sender denne linken deg til netflux.com Etter dette kan du se om du har fått noen mailer fra netflix tidligere? er mailen lik som de mailene du tidligere har mottatt?

Går inn på netflux.com Første man burde gjøre når man går inn på en link fra en e-post, det er å sjekke nettadressen. er det riktig nettadresse? i dette tilfelle skulle det vært

netflix.com, men som vi ser her så har vi kommet til netflux.com. Neste så kan man trykke på forskjelle linker på nettsiden, da noen av disse kanskje ikke fungerer, hvis linkene ikke fungerer så er sansynligheten for at dette er en phishing side stor. MERK: Noen linker kan fortsatt fungere, selvom dette ikke er en ekte nettside, som vi ser her. trykker på terms of use linken Om du enda er i tvil at nettsiden er ekte, så kan du skrive inn et fake brukernavn og passord, for å teste loggin funksjonen. Dette er grunnet at phishing sider ofte vil sende deg til den ekte nettsiden dersom du prøver å logge inn, uavhengig om du bruker ekte eller falsk loggin. skriver inn fake brukerinformasjon som vi ser her, etter jeg logget inn, så ser det bare ut som nettsiden oppdaterte seg, men som man kan se har jeg nå blitt sendt til netflix.com, og hackerne har bare fått falsk informasjon når jeg forsøkte å logge inn. Oppsummering: Dette er de viktigste tingene å tenke på: sjekk alltid avsender se etter gramatikkfeil sjekke mail fra samme firma/avsender sjekke nettadresse sjekke linker på nettside skrive inn falsk brukerinformasjon

13.4 Vedlegg 4: Manus for den andre filmen

Filmmanus

EXT. ET STED I HALDEN - DAY
Sindre og Martin går langsetter en gate, Sindre ser en minnepenn på bakken og plukker den opp.

Sindre: Oi se her a, en minnepenn
Martin: AAAA
Sindre: jeg har så lyst å se hva som er på'n
Martin: nææææ, Jeg tror ikke det er helt trygt
Sindre: kanke være så farlig vel
Martin: nei, men man vet aldri
Sindre: prøver!

Sindre går ut av bilde, mens martin står igjen på samme sted. Sindre går hjem, setter minnepennen i pc en sin. åpner et dokument som er på minnepennen.

Sindre: Jeg er kulere enn deg, du bare vet det ikke enda. Det var ikke så veldig kult egentlig. får bare gå og lese nyheter da.

går over til forklaringsdel

Forklaringsmanus

INT. WEBCAMERA TIL MARTIN - DAY

martin ser på kamera Hva var det som skjedde her? Jo, Sindre fant en minnepenn på bakken, og valgte å ta med seg denne hjem for å finne ut hvem som eier den. Det vi også ser, er at sindre åpner et dokument, som det egentlig ikke er noe spennende på. I dette dokumentet ligger det noe som kalles en orm, dette er et virus som deles av seg selv, ved at du åpner et dokument, eller mottar en mail du åpner, eller kobler en minnepenn i pc en din som i dette eksempelet. En orm kan gjøre flere forskjellige ting, foreksempel: låse dokumenter på pc en din, lage en keylogger, kan gi hacker tilgang til pc en din og kamera ditt. (Keylogger: en keylogger er når alle tastetrykk du gjør på tastaturet ditt, blir tatt opp og sendt til et dokument som hackeren har.)

Når en orm låser dokumenter på pc en din, så vil disse dokumentene bli holdt som gissel av hackeren, og de vil da ønske å motta penger, ofte i bitcoin mot at du får åpnet dokumenter igjen. Dette kalles Ransomeware. når en hacker for tilgang til pc en din, og kamera ditt, så vil hackeren kunne gå igjennom pc en din, uten å bli oppdaget, for å gjøre dette må pc en din være på, hackeren kan også få tilgang på webkamera i pc en din, dette er også vanskelig å legge merke

til, men om webkamera er i bruk, så er det ofte et lys ved siden av webkamera som lyser.

Det er noen ting å huske på for å sikre seg. Det er viktig å holde pcen oppdatert, vil dette si at du sjekker windows oppdateringer gjevnlig, og oppdaterer hvis mulig. Det er også lurt og holde anti virus programvare oppdatert. Det er flere varianter, hvor blant annet winsows har sitt eget innebygde windows defender antivirus. Videre er det lurt å være skeptisk til opplukking av minnepenner, minnepenner du finner på bakken, enten ute, eller på ditt kontor, er ikke alltid sikkert, gjerne bring minnepennen til et IT personel så de kan heller åpne den på en trygg måte. Du bør være forsiktig med åpning av dokumenter på minnepenn som du ikke vet hvor har vært, da det kan være skadevare på disse Til slutt burde du også være skeptisk til åpning av dokumenter du mottar på mail, om du ikke kjenner til avsender, kjenner du til avsender, men mailen ser rar ut så vil det anbefales å ta kontakt med avsender på et annet sosialt medie eventuelt telefon, for å høre om dette er noe som dem har sendt.