RAPPORT
1/7 2017

DIGITALISERINGSSTYRELSEN OG ERHVERVSSTYRELSEN

FOR-ANALYSE AF DANSKERNES INFORMATIONSSIKKERHED

/KL.7
ADFÆRDSDESIGN

Rapporten er udarbejdet af /Kl.7 for Digitaliseringsstyrelsen og Erhvervsstyrelsen

Forfattere: Lasse Frost, Kristian Sørensen og Simon Bentholm

Dato: 1/7 2017

Version

/KL.7 Aps

Nørregade 6

1165 København K

Tlf. 33 48 08 00

www.kl7.dk

Executive Summary

DIGST og ERST ønsker at afdække danskernes it-sikkerhed som borgere og medarbejdere. Formålet med denne for-analyse er at udvælge de væsentligste adfærdsmønstre i relation til digital adfærd og undersøge dem nærmere med henblik på at udarbejde et katalog over anbefalinger af indhold og kanaler til segmentspecifik budskabskommunikation.

/KL.7 løser denne opgave i et projekt bestående af tre faser. Hver ny fase bygger oven på den foregående, således at for-analysen hele tiden bruger opnåede indsigter til at komme nærmere et applicérbart sæt af budskaber. Strukturen for for-analysen er som følger: 1) Research og interview med eksperter i it-sikkerhed og menneskelig adfærd mhp. udvælgelse af de væsentligste adfærdsmønstre, 2) en repræsentativ survey mhp. undersøgelse af specifikke hypoteser om de udvalgte adfærdsmønstre og udarbejdelse af budskaber, 3) kontekstspecifikke brugertest af budskaberne mhp. endelig tilretning, kanalvalg og segmentering.

Den endelige leverance er et budskabskatalog med anbefalinger til overordnet kommunikation om it-sikkerhed, segmentspecifikke råd og handleregler samt optimale kanaler at kommunikere igennem. For-analysen giver DIGST og ERST et solidt evidensbaseret, adfærdsvidenskabeligt fundament for kommende kampagneindsatser til forbedring af danske borgere og medarbejderes it-sikkerhed.

Anbefalingerne Opsummeret

Overordnet

- Gør det fysisk.
    - It-kriminalitet er abstrakt og svært at forholde sig til. Tal det derfor ind i en velkendt metaforisk ramme: Hjemmet. Det øger danskernes **forståelse** af problemets alvor.

- Gør it-kriminelle til tricktyve.
    - Danskerne forestiller sig, at IT-kriminelle er russiske hackertyper. I virkeligheden er de snarere svindlere, der er gode til at udnytte psykologiske tilbøjeligheder. Billedet af en 'tricktyv' giver danskerne mere oplevet **handlekraft** ift. it-kriminalitet.

- Gør offeret til os alle sammen.
    - Danskerne forestiller sig, at det typiske offer for it-kriminalitet er naive ældre kvinder. I virkeligheden bliver alle ramt (og faktisk især mænd og unge mennesker). Billedet af offeret som os alle sammen øger danskernes **motivation** for at handle.

- Undgå ekspertsprog (dvs. 'browser', 'phishing', 'password manager').
    - Skriv det i stedet mere konkret (dvs. 'hjemmeside', trick-mails', 'hjælp til kodeord'). Det øger forståelsen og gør adfærden mere **overskuelig** for danskerne.

- Sæt rådene op i tjeklister for borgere og medarbejdere.
    - Helt konkrete og handlingsanvisende råd med mulighed for afkrydsning gør, at danskerne har en højere oplevet **tryghed** efter handlingerne.

De seks uhensigtsmæssige adfærdsmønstre (i prioriteret rækkefølge)

- Genbrug af passwords: Hjælp med konstruktion og sikker opbevaring af unikke passwords.

- Klik på indhold i usikre e-mails: Giv konkrete handleregler om afsenders adresse og om personlig info.

- Tager ikke backup: Giv konkrete handleregler for, hvordan det sættes op automatisk eller gøres til en ugentlig vane.

- Mangler at opdatere software/styresystem: Lav kobling til it-sikkerhed og giv konkrete handleregler til opsætning af automatisk opdatering.

- Indtaster personlige informationer på usikre hjemmesider: Forklar, hvad 'usikker' vil sige, og hvor man skal orientere sig hen i browservinduet for at afgøre hjemmesiders sikkerhed.

- Mangler at installere antivirus/firewall: Tal om antivirus og firewall som 'udgangspunktet' for it-sikkerhed på computer og telefon – ikke som løsningen.

Kanaler

- Borgere:
    - Videospots og bannere på en flerhed af traditionelle platforme (busreklamer, landsdækkende medier, sociale medier).
    - Eksisterende infrastruktur for offentlig kommunikation (f.eks. ifm. fremsendelse af nyt NemID).
    - App'en 'Mit Digitale Selvforsvar'.
    - Partnermobilisering er et oplagt værktøj til at komme helt bredt ud.
    - Mere uformelt bør det også udnyttes, at mindre IT-kyndige i forvejen konsulterer mere it-kyndige venner/familiemedlemmer for råd og vejledning.

- Medarbejdere:
    - De it-ansvarlige er oplagte til – og udtrykker ønske om – at fungere som katalysator for budskaber. Det gælder også de budskaber, medarbejderne kan tage med hjem i privaten.
    - De it-ansvarlige kan med fordel udstyres med et kit, der hjælper dem med at hjælpe deres kolleger til at agere mere sikkert – både på arbejdet og derhjemme.
    - Derudover bør man kommunikere så tæt på medarbejderne som muligt – dvs. ikke blot opslag på intranet, men også personlige skrivelser/henvendelser til hver enkelt medarbejder.
    - Fokus bør især være på nye medarbejdere, som skal sættes ind i virksomhedens sikkerhedskultur.

Segmentering

- Borgere er forskellige.
    - Ret kommunikationen ind efter følgende segmenter (i prioriteret rækkefølge): Uddannelse, teknologikyndighed, alder og køn.

- Virksomheder er forskellige.
    - Ret kommunikationen ind efter virksomhedens størrelse (større vs. mindre virksomheder).

Indholdsfortegnelse

1.0 Introduktion

Digitaliseringsstyrelsen (DIGST) og Erhvervsstyrelsen (ERST) ønskede i foråret 2017 at få foretaget en for-analyse, som skal lægge fundamentet for resten af digitaliseringsstrategiens indsatsperiode (2017-2020). Formålet med for-analysen var at kortlægge digitale adfærdsmønstre hos borgere samt offentlige og private medarbejdere, som har en risiko for at lede til usikker digital adfærd.

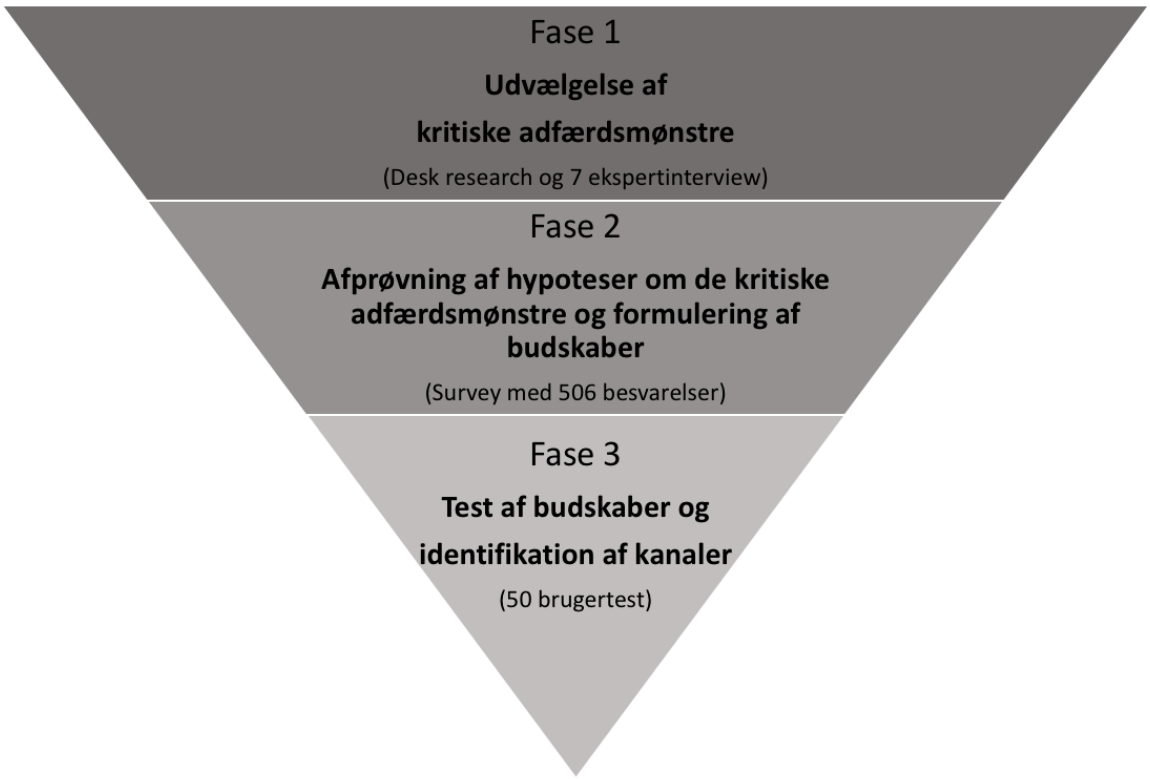
Formålet med foranalysen er at kortlægge adfærdsmønstre, der skal danne baggrund for udvikling af en serie af borger- og medarbejderrettede informationsindsatser i resten af digitaliseringsstrategiens indsatsperiode (fra 2017-2020). Indsatsens mål er at skabe varige adfærdsændringer og styrke kompetencerne blandt borgere samt offentlige og private medarbejdere, så de i højere grad kan færdes sikkert på nettet og i deres arbejdssituationer og derigennem hjælpe til med at beskytte data og systemer.

1.1 Metodedesign

Projektets formål var tredelt: 1) Udvælgelse af kritiske adfærdsmønstre, 2) afprøvning af hypoteser om de kritiske adfærdsmønstre og 3) test af budskaber og identifikation af kanaler.

De tre formål blev knyttet til hver sin fase, og samlet set kan projektets kronologi anskues som en tragtform. Figur 1.1 nedenfor illustrerer projektets kronologi fra Fase 1 til 3.

Figur 1.1



Indledningsvist bredtes processen helt ud for at indfange et dækkende spektrum af de mest prævalente adfærdsmønstre: 18 blev identificeret (se bilag).

Allerede hen mod slutningen af Fase 1 indsnævreres fokus mod seks kritiske adfærdsmønstre, som blev udvalgt i samarbejde med en række eksperter i it-sikkerhed og adfærdsvidenskab.

På baggrund af eksperternes prioritering udvalgte /KL.7, DIGST og ERST seks adfærdsmønstre. Disse adfærdsmønstre blev knyttet til hver sin hypotese, som blev testet kvantitativt i en større survey i Fase 2. Spørgeskemaet var et repræsentativt survey med 506 besvarelser og havde to overordnede formål: (1) At afdække, hvordan borgere og medarbejdere forstår it-kriminalitet og hacking, både som koncepter og som personer i form af kriminelle/ofre, og (2) at teste, hvorvidt hypoteser om de seks kritiske adfærdsmønstre holdt stik.
Centralt for denne tilgang var nærmere afdækning af mentale modeller (dvs. folks konkrete forståelse af abstrakte koncepter og problemstillinger vedr. it-sikkerhed), den oplevede alvorlighed ved de identificerede adfærdsmønstre (dvs. hvad folk *oplever* som relativt mest/mindst alvorligt, ikke hvad der *faktuelt* er tilfældet) samt motivationen for at udføre den ene eller anden handling (dvs. at ændre det ene eller andet usikre adfærdsmønster).

Indsigterne fra hypotesetesten i surveyen blev anvendt til konstruktion af en række budskaber – både om it-sikkerhed generelt og hvert enkelt adfærdsmønster specifikt – som blev testet i 50 kvalitative brugertest á 15 minutters varighed (20 borgere, 22 medarbejdere og 8 it-ansvarlige). Brugertestene havde til formål at afdække informanternes eksisterende viden om 1) it-kriminalitet/cybersikkerhed, 2) forståelse af de overordnede budskaber og individuelle råd, 3) indikationer på optimale kanaler. Resultaterne fra brugertestene blev ført direkte ind i de endelige, segmenterede budskabsformuleringer samt i anbefalinger til valg af kanaler.

2.0 Udvælgelse af Adfærdsmønstre

I de følgende afsnit præsenteres resultatet af projektets Fase 1. Formålet med denne fase var at identificere og udvælge de fem kritiske adfærdsmønstre, som resten af for-analysen skulle fokusere på. Den endelige udvælgelse blev foretaget i samarbejde mellem /KL.7 og styregruppen.

2.1 Uhensigtsmæssige, Digitale Adfærdsmønstre

Fase 1 startede med en grundig desk research, hvor centrale problemstillinger og udfordringer i forbindelse med digital sikkerhed blev identificeret. Disse blev efterfølgende valideret og uddybet af nationale og internationale eksperter på området. Denne tilgang, hvor desk researchen kombineres med ekspertinterviews, er valgt, fordi vi således kombinerer forskningens evidensbaserede metoder med eksperternes praktiske og løsningsorienterede erfaringer på området. På baggrund af dette har vi fået opbygget en solid basisviden om problemets omfang og de tilhørende adfærdsmæssige barrierer.

Tabel 2.1 herunder viser listen over de eksperter, som /KL.7 interviewede med henblik på udvælgelsen af de kritiske adfærdsmønstre. Eksperterne er udvalgt med henblik på at dække både tekniske, samfundsøkonomiske, adfærdsvidenskabelige og formidlingsmæssige aspekter af it-

sikkerhed. Det er en central prioritet for denne for-analyse, at de endelige indsigter og anbefalinger bygger bro mellem alle fire aspekter af it-sikkerhed. Det betyder dog ikke, at alle interviewede eksperter vidste alt om alt. Nogle af eksperterne repræsenterer store dele af det nævnte spektrum (f.eks. Angela Sasse), mens andre har bidraget med mere specifik viden om det adfærdsvidenskabelige (f.eks. Mary Aiken) eller det tekniske og samfundsøkonomiske (f.eks. Kim Aarenstrup).

Tabel 2.1

Navn	Titel	Ekspertise
Jan Kaastrup	Sikkerhedsekspert (CSIS)	De tekniske og formidlingsmæssige aspekter af it-sikkerhed
Kim Aarenstrup	Centerchef (Rigspolitiets Cyber Crime Center)	Primært tekniske og samfundsøkonomiske aspekter af IT-sikkerhed, især med henblik på at bekæmpe it-kriminalitet
Mary Aiken	Retsmedicinsk cyberpsykolog (selvstændig rådgiver)	Menneskelig adfærd i det digitale (mest teoretisk).
Angela Sasse	Professor i Human-Centered Security	Bred praktisk erfaring fra videnskabeligt arbejde med at øge menneskers digitale sikkerhed gennem adfærd.
Christian Jæhger	Sikkerhedsrådgiver (Politiets Efterretningstjeneste)	Rådgivererfaring fra krydsfeltet mellem it-sikkerhed, samfundsøkonomi og menneskelig adfærd.
Anders Kjærulff	Radiovært (Radio 24Syv), teknologikritiker, bestyrelsesmedlem i Rådet for Digital Sikkerhed	It-sikkerhed og digital adfærd bredt set, dog især med etisk fokus.
Rasmus Theede	Skandinavisk Direktør for Cybersikkerhed (CSC) og formand for Rådet for Digital Sikkerhed	De tekniske og formidlingsmæssige aspekter af it-sikkerhed

Digitale handlinger er virkelige handlinger – digital adfærd er virkelig adfærd. Det *ved* vi godt, men vi *oplever* det ikke sådan. Dette har været et af de centrale fund i Fase 1. Vores desk research har gjort det klart, at vi i højere grad opfatter os som anonyme og fritaget for ansvar og overvågning, når vi bruger digitale medier og færdes på nettet (Aiken, 2016). Konsekvensen af dette er, at vi handler mere i overensstemmelse med, hvad vi umiddelbart har lyst til, end vi gør når vi færdes i den fysiske verden. Vi forstår simpelthen ikke konsekvenserne af vores digitale handlinger. Vores adfærd er i mindre grad reguleret af hvad vi vurderer, at andre mennesker synes er acceptabelt. Dette fund gør sig i øvrigt gældende, både når vi er derhjemme og når vi er i en arbejdsmæssig kontekst. Faktisk er vi i nogle tilfælde mere udsatte når vi er på arbejde, da vi har en tendens til at antage at it-afdelingen nok har styr på vores sikkerhed for os. Vi oplever med andre ord at have et

mindre ansvar for vores digitale sikkerhed på arbejdet. Cyberpsykologen Mary Aiken (2016) beskriver dette fænomen som ”the online disinhibition effect”: Online er vi mere modige og direkte, mindre hæmmede og skeptiske end ude i den fysiske verden.

Selvom der umiddelbart kan synes at være stor forskel på adfærd i den digitale og den fysiske verden, så er det mange af de samme adfærdspsykologiske faktorer, som forårsager vores irrationelle og usikre adfærd begge steder. Det ved de it-kriminelle godt, og de udnytter aktivt de kognitive bias der påvirker vores adfærd. Man kan således godt sige, at nutidens it-kriminelle er en form for psykologer (Fallows, 2011). Konsekvensen af dette er, at nøglen til danskernes it-sikkerhed i høj grad ligger i at skabe et indgående kendskab til disse kognitive bias og menneskers adfærd, samt i at designe løsninger på baggrund af denne viden. Christian Jæhger, sikkerhedsrådgiver i PET, formulerer det ganske rammende i vores ekspertinterview med ham: ”Selvom de teknologiske forsvarsværker er perfekte, og murene er tilstrækkeligt høje og robuste, så er der altid nogen, der åbner døren, fordi de skal ud og ryge”. Det er derfor afgørende, at kommunikation til danske borgere og medarbejdere bliver gjort fysisk og konkret, fordi det netop vil tydeliggøre den helt centrale pointe fra researchfasen: At it-sikkerhed i høj grad er et stort problem, fordi mennesker tror, de kan handle mere frit og mindre overvåget på nettet end i den fysiske virkelighed.

I de følgende afsnit præsenteres først de barrierer, som /KL.7 har fundet er til hinder for at folk handler sikkert når de udfører digital adfærd. Der er tale om kognitive bias og andre psykologiske faktorer, som på hver deres måde påvirker vores adfærd. I det efterfølgende afsnit præsenteres alle de identificerede adfærdsmønstre for usikker digital adfærd, og disse kædes sammen med psykologiske barrierer. I bilagsmaterialet fremgår en skematisk liste over samtlige adfærdsmønstre samt psykologiske barrierer for dem med referencer.

2.1.2 Psykologiske barrierer for hensigtsmæssig digital adfærd

Ud fra den adfærdsvidenskabelige litteratur har vi identificeret en række barrierer, der hver især er medvirkende årsager til danskernes usikre digitale adfærdsmønstre. En stor del af disse barrierer er såkaldte kognitive bias, eller systematiske fejl i menneskers tænkning om man vil. De resterende er andre menneskelige vilkår, der på en eller anden måde har indflydelse på vores beslutningstagen og adfærd.

Først og fremmest er der grænser for, hvor meget hjernen kan huske (Miller, 1956). Når vi skal konstruere *og* huske et større antal passwords, som helst er både stærke og unikke, strækker det vores hukommelsesevne til det yderste – og længere endnu (Eysenck 2012). Det giver ikke mening blot at fylde på med kompleksitet og nye tiltag, når danske borgere og medarbejdere skal hjælpes til at handle mere it-sikkert. Især nye tiltag er problematiske, da mennesker som udgangspunkt er forandringsresistente (Kahneman et al., 1991).

Noget af det, vi er bedst til, er at genkende mønstre. Det udnytter it-kriminelle til at ”lulle os i søvn” ved at præsentere os for et mønster, vi kender som sikkert i forvejen Eysenck, 2012). Det kunne

f.eks. være i en e-mail med et særligt layout, afsendt med en velvalgt timing, fra en særligt autoritativ afsender (Milgram, 1963) og/eller med en bestemt måde at skrive på. Generelt er vi meget lidt på vagt på nettet, fordi it-truslerne er svære at forholde sig til, fordi de er abstrakte og ligger ude i fremtiden. ”Det sker alligevel aldrig for mig” eller ”jeg har alligevel ikke noget, der er værd at stjæle” er meget udbredte udsagn, og det skyldes vores psykologiske tendens til at være overoptimistiske mht. fremtidige hændelser – både hvad angår klimaforandringer og cyberangreb (Chapin & Coleman, 2009).

Hvad angår subjektive oplevelser *lige nu* fokuserer dog langt mere på at undgå tab end at opnå gevinster (Kahneman & Tversky, 1992). Det er en yderligere forklaring på, at vi *lige nu* vælger at udskyde besværlige handlinger som at tage backup, fordi de først i fremtiden (og endda kun potentielt) kan redde os fra datatab og ransomware-løsesummer. Vi er desuden evolutionært udviklet til at vurdere potentielle sikkerhedsrisici pba. fysiske *cues*, som den digitale verden netop mangler (Eysenck, 2012). Det gør samtidig også, at vores behov for heuristikker – altså, simple handleregler på komplekse problemer – er ekstra vigtige i en kontekst af it-sikkerhed (Lewis, 2008). Mange af de *cues,* dvs. faresignaler, vi bliver konfronteret med på computeren, er dog falske alarmer. F.eks. fra antivirusprogrammer, der fortæller os, at ’så og så mange trusler er identificeret’. Forskningen viser, at vi er psykologisk hardwired til gradvist at filtrere sådanne ”ulven kommer”-advarsler fra – og på den måde er antivirusprogrammet faktisk med til at gøre os mindre opmærksomme på de rigtige it-trusler (Bouton, 2007).

2.2 Prioritering af Adfærdsmønstre

Sammen med de syv interviewede eksperter prioriterede vi adfærdsmønstrene. Formålet var at udvælge mindst fem kritiske adfærdsmønstre, som de senere budskaber skal adressere. Vi endte med at udvælge seks unikke adfærdsmønstre som fokus for indsatsen fremadrettet. Følgende kriterier lå til grund for udvælgelsen:

- Adfærdens estimerede konsekvenser (store/små) på samfunds- og individniveau
- Den estimerede sværhedsgrad (let/svært) ved at ændre på adfærden med kommunikationsindsats
- At adfærden er generel for hele Danmarks befolkning (både borgere og medarbejdere)
- At adfærden også gælder i fremtiden

Herudover har vi valgt tre yderligere adfærdsmønstre, som enten er en underliggende del af de første fem adfærdsmønstre, eller som ligger som forslag til fremtidige kampagneindsatser.

/KL.7 arbejdede ud fra en række kriterier for prioritering og udvælgelse af de kritiske adfærdsmønstre. Først og fremmest skulle de både udgøre store problemer (dvs. relativt store konsekvenser ved den uhensigtsmæssige adfærd), og de skulle være realistiske at gøre noget ved gennem en indsats, som primært består i massekommunikation af budskaber (dvs. at adfærden skal være relativt nem at ændre). Herudover skal adfærden være generel for befolkningen, både gælde for danske borgere og for ansatte i private og offentlige virksomheder samt være aktuel nu såvel som i fremtiden. Med disse udvælgelseskriterier kommer budskaberne i sidste ende til at gælde de største problemer, som vi sandsynligvis kan gøre noget ved med denne kommunikationsform, og indsatsen vil meningsfuldt kunne udrulles landsdækkende. Herudover er de valgte budskaber fremtidssikrede, idet de alle angår nogle psykologiske grundtræk ved it-kriminalitet, hvorfor de ikke bliver irrelevante blot fordi næste uges angreb er et andet end denne uges.

De identificerede adfærdsmønstres har rod i helt basale psykologiske fænomener, som er fælles for alle mennesker – uanset om de er på arbejde eller i privaten. Hermed skal det ikke forstås, at man skal kommunikere budskaberne på samme måde til borgere og medarbejdere, blot at det er de samme problemstillinger der gør sig gældende for begge grupper. Dertil gælder også, at f.eks. backup ser ud til at være en mindre problemstilling i større virksomheder, da det allerede bliver gjort automatisk af it-afdelingen. Ikke desto mindre oplever flere af disse virksomheder, at deres medarbejdere bruger arbejdscomputer og –telefon privat. Selvom virksomheden har styr på medarbejderens backup af arbejdsrelaterede dokumenter, vil den samme computer/telefon altså stadig kunne anvendes usikkert af medarbejderen. Kort sagt er det digitale og fysiske arbejdsliv flydt sammen med privatlivet, og det er derfor vigtigt at identificere almengyldige adfærdsmønstre, som kan forbedre danskernes it-sikkerhed, uanset hvor de er.

2.2.2 Udvalgte adfærdsmønstre

I det følgende gennemgås de udvalgte adfærdsmønstre, som fremgår af figur 2.1 ovenfor. Den overordnede argumentation for udvælgelsen gennemgås med nedslag i centrale udtalelser fra de interviewede eksperter. Tabel 3.4 i næste kapitel viser en oversigt over alle pointer samt referencer relateret til de udvalgte adfærdsmønstre fra Fase 1-3. For uddybning af referencerne til den inddragne litteratur henvises til tabellen i bilagsmaterialet.

Manglende opdatering af software

Litteratur: Bouton 2007, Eysenck 2012, Digitaliseringsstyrelsen og DKCERT 2017, Proofpoint 2016, Blau et al. 2016, Blau et al. 2016

Der er bred enighed blandt eksperterne om, at dette adfærdsmønster bør have høj prioritet. Iflg. Anders Kjærulff er dette især udbredt blandt yngre mennesker. Det har vi dog ikke fået bekræftet fra andre kilder eller eksisterende rapportmateriale. Uanset om yngre mennesker er hårdest ramt på dette punkt, er det uhyre afgørende for den digitale sikkerhed, at det er på plads.
Det er ofte selve årsagen til opdateringen, at der er et sikkerhedsbrist eller en ny trussel, som serviceudbyderen forsøger at imødegå.
Samtidig er denne adfærd iflg. Angela Sasse blandt de mindre vanskelige at ændre, idet det er en éngangsadfærd. Danskerne skal kun sætte automatisk opdatering til én gang, før problemet er imødegået – det er ikke en kontinuerlig adfærdsændring.
Selvom det er blandt de lettere adfærdsmønstre at ændre, er eksperterne enige om, at adfærdsændringen vil kunne opnås mest effektivt med teknologiske løsninger, som automatiserer opdateringen. En sådan løsning eksisterer heldigvis allerede i form af en app, som Jan Kaastrups firma CSIS har udviklet til automatisk at holde alle apps og programmer opdateret hele tiden.

Manglende backup

Litteratur: Chapin & Coleman 2009, Kahneman & Tversky 1992, Digitaliseringsstyrelsen og DKCERT 2017

Dette er et meget generelt problem, som kun en mindre del af befolkningen er opmærksomme på vigtigheden af. Alle eksperter er enige om, at dette adfærdsmønstre er et af de allermest centrale. Det er samtidig nøglen til løsningen af flere andre problemer. Iflg. Christian Jæhger havde ransomware ikke været et problem, hvis folk tog de backups, de skulle. Rasmus Theede udtaler også, at dette adfærdsmønster er blandt de lavthængende frugter, som med relativt få midler vil kunne forbedre danskernes informationssikkerhed markant.
Det er altså et adfærdsmønster, som har store konsekvenser, men som vi også har gode odds for at ændre på.

Manglende installation af antivirus/firewall

Litteratur: Chapin & Coleman 2009, Kahneman & Tversky 1992, Digitaliseringsstyrelsen og DKCERT 2017.

Der er mere delte meninger om dette adfærdsmønster – både vigtigheden af at adressere det og sandsynligheden for at ændre det.
Anders Kjærulff ser antivirus og firewall som en central del af, hvad han kalder ”en god computerhygiejne”. Hvis alle havde installeret denne software, ville det højne det generelle digitale sikkerhedsniveau betragteligt.
Rasmus Theede er ikke enig. Han mener, at antivirusprogrammer og firewall er gode at have, men ikke nødvendigvis den allervigtigste adfærd at adressere. Dertil siger han, at den firewall, der som standard er installeret på nyere computere, er rigtig effektiv. Angela Sasse udtrykker skepsis overfor blot at anbefale danskerne at installere ”et eller andet” antivirusprogram/firewall, fordi markedet er meget svært at overskue for den enkelte. Hun mener faktisk, at markedets uoverskuelighed er en af de væsentligste årsager til, at relativt mange undlader at investere i antivirus/firewall. Hvis vi derimod – gennem strategisk partnerskab el.lign. – kan anbefale én bestemt software, ser Sasse gode muligheder for adfærdsændring. Desuden mener hun, at en sådan anbefaling er relativt nem at måle effekt på (antal downloads før/efter).
Manglende installation af antivirus/firewall er altså hverken blandt de allervigtigste eller nemmeste adfærdsmønstre at adressere. Når det alligevel er blevet udvalgt, skyldes det de relativt lovende perspektiver i en partnerdrevet anbefaling af en bestemt software.

Genbrug af passwords

Litteratur: Eysenck 2012, Kahneman et al. 1991, Digitaliseringsstyrelsen og DKCERT 2017, Pfleeger & Caputo 2012, Blau et al. 2016.

I bruttolisten havde vi formuleret dette adfærdsmønster som ”Genbrug af svage passwords”. Men stort set samtlige eksperter gjorde os opmærksom på, at det især er *genbrug*, der er problemet. Uanset styrken af det enkelte password, er det markant mere sårbart, hvis det selvsamme password er anvendt før og/eller i flere andre login. Det er forskellen på, om man blot skal hackes én gang, før alle data er kompromitteret. Der er bred enighed om, at genbrug af passwords er meget centralt for danskernes digitale (u)sikkerhed.
DKCERT-undersøgelsen (2016) viste, at ca. to-tredjedele af alle danskere genbruger passwords. Og i lyset af, at flere af de interviewede eksperter (deriblandt Mary Aiken og Angela Sasse) udtaler, at ingen almindelige mennesker kan huske et større antal unikke og stærke passwords i hovedet, ser vi en klar anbefaling for os: Brug en password-manager, og sørg for, at masterpasswordet (som er det eneste, den enkelte selv skal huske) er stærkt og gemt fysisk. Hvis man som i den seneste kampagneindsats anbefaler danskerne at bruge tofaktor-login, behøver passwordet ikke engang at være særligt stærkt.
Som antivirus/firewall er markedet for password-managers uoverskueligt for den enkelte at navigere i. Der er en nødvendighed i at snævre mulighedsrummet lidt ind, måske endda etablere et partnerskab mhp. at anbefale én bestemt passwordmanager (eller udvikle én ifm. et offentligt hackathon el.lign.).

Besøger usikre hjemmesider

Litteratur: Kahneman & Tversky 1992, Lewis 2008, Digitaliseringsstyrelsen og DKCERT 2017, Mosley 2006

Ifølge Christian Jæhger er der altid – selv i det mest sikre it-system – en bruger bagved skærmen, som opfører sig usikkert. At danskerne besøger usikre hjemmesider, er ikke i sig selv et problem. Det bliver det først, når den enkelte indtaster personfølsomme oplysninger på den usikre hjemmeside. Eksperterne er enige om, at danskerne gør netop dette uden at vide, at det kan kompromittere deres sikkerhed.
Det er derfor et af de adfærdsmønstre, som har størst konsekvenser både for den enkelte og for samfundets informationssikkerhed. Det er imidlertid samtidig et adfærdsmønster, som er vanskeligt at ændre, da det vil kræve en meget konkret handleregel for, hvad der gør en hjemmeside "usikker" – og ikke mindst, hvad det konkret betyder. Danskerne mangler *både* en heuristik for at vurdere sikkerheden af en hjemmeside, og de mangler en generel forståelse af, hvad "usikker" indebærer. Dette adfærdsmønster er altså valgt på trods af, at umiddelbart er vanskeligt at ændre på, men netop fordi det udgør et meget centralt problem, indsatser som denne bør søge at ændre.

Åbner indhold i e-mail fra ukendt afsender

Litteratur: Milgram 1963, Eysenck 2012, Digitaliseringsstyrelsen og DKCERT 2017, KMD 2016, Proofpoint 2016, Mosley 2006, Mosley 2006, Pfleeger & Caputo 2012, Blau et al. 2016

Som ovenstående er dette adfærdsmønstre et af de mest centrale, fordi det både for den enkelte og for samfundet involverer enorme omkostninger. Men adfærsmønsteret er samtidig også blandt de vanskeligste at ændre på, fordi angrebene (phishing, ransomware osv.) bliver mere og mere sofistikerede.
Angela Sasse pointerer, at det er umuligt at forestille sig, at borgere såvel som medarbejdere vil kunne klare sig uden at sende links i e-mails. Det er faktisk blevet så integreret del af vores digitale kommunikation, at det vil forstyrre uhensigtsmæssigt meget, hvis danskerne skal tjekke alt indhold i samtlige e-mails, de modtager. Der er altså brug for simple handleregler, hvis denne adfærd skal ændres, og dertil positiv feedback, som fortæller folk, når de handlet i overensstemmelse med anbefalingen.
Oz Alashe mener, at den bedste handleregel ift. at opdage phishing o.lign. ondartede e-mails er at kigge på afsenderens adresse. Barclays direktør blev offer for spearphishing afsendt fra adressen "john.mcfarlane.barclays@gmail". Oz Alashe vurderer, at 80 procent af al phishing kan undgås, hvis bare man tjekker afsenderens adresse og links i e-mailen.
Det er altså med simpel adfærd muligt at forhindre en stor del af konsekvenserne ved dette meget alvorlige problem. Derfor er dette adfærdsmønster udvalgt.

2.2.3 Udvalgt baggrundsadfærd

I det følgende præsenteres to adfærdsmønstre – deler private info offentligt og klikker på usikkert indhold – der er vigtige at rette en indsats imod, men som går på tværs af de ovenstående adfærdsmønstre, og er et underliggende problem for disse. Herudover præsenteres et adfærdsmønster – download af uofficielle apps – der formentligt vil være vigtig at være opmærksom på i fremtiden.

Deler private info offentligt

Litteratur: Kahneman & Tversky 1992, Digitaliseringsstyrelsen og DKCERT 2017, Pfleeger & Caputo 2012

Alle eksperter er enige om, at dette adfærdsmønster udgør et meget stort problem. Kim Aarenstrup mener endda, at det – næstefter klik på uhensigtsmæssige links – er det allermest centrale adfærdsmønster. Når det imidlertid ikke er udvalgt direkte, skyldes det, at det er svært at pege på et bestemt tidspunkt eller en bestemt situation, hvor folk deler deres private info offentligt. Dette sker løbende på tværs af mange kontekster, herunder flere af de ovenfor nævnte.

Danskernes deling af private info offentligt er en af de vigtigste årsager til, at der i det hele taget er så mange følsomme data tilgængeligt på nettet, som de cyberkriminelle kan udnytte i en lang række forskellige angreb. Sammen med eksperterne vurderer vi, at danskernes ukritiske deling af privat info skyldes en manglende *generel* bevidsthed om, hvilke trusler der eksisterer på nettet. Dette adfærdsmønster er med andre ord så bredt funderet og har så mangfoldige konsekvenser, at det snarere end at være et selvstændigt punkt i stedet bør adresseres i den overordnede kommunikation.

Eksperter, der fremhæver adfærdsmønsteret: Angela Sasse, Christian Jæhger, Kim Aarenstrup.

Klikker på usikkert indhold

Litteratur: Milgram 1963, Kahneman & Tversky 1992, Lewis 2008, Proofpoint 2016, Mosley 2006, Blau et al. 2016

Eksperterne peger stort set alle på, at dette adfærdsmønster både er blandt de mest udbredte og uhensigtsmæssige. Uanset om man er på en sikker hjemmeside – f.eks. Facebook – kan man let komme til at klikke på indhold, som leder én uforvarende ind på usikre sider. Det er det, som kaldes at klikke på usikkert indhold Når det heller ikke er udvalgt som et selvstændigt indsatspunkt, er det fordi, at flere af de øvrige adfærdsmønstre ligger tidligere i kausalkæden. Flere af de udvalgte adfærdsmønstre er simpelthen årsagen til, at den enkelte overhovedet når til selve klikket. /KL.7 vurderer derfor, at selvom det er vigtigt at få danskerne til ikke at klikke på usikkert indhold, gør kampagnen klogere i at adressere den adfærd, som leder op til situationen, hvor klikket bliver muligt (besøg på usikre hjemmesider, åbning af usikre mails osv.). Desuden er dette adfærdsmønster så konkret, at det potentielt kan blive forældet inden for en overskuelig

tidsramme. Så da kampagnens budskaber ønskes fremtidssikret, vurderer vi, at de kun indirekte bør fokusere på dette adfærdsmønster.

Eksperter, der fremhæver adfærdsmønsteret: Mary Aiken, Angela Sasse

Download af uofficielle apps

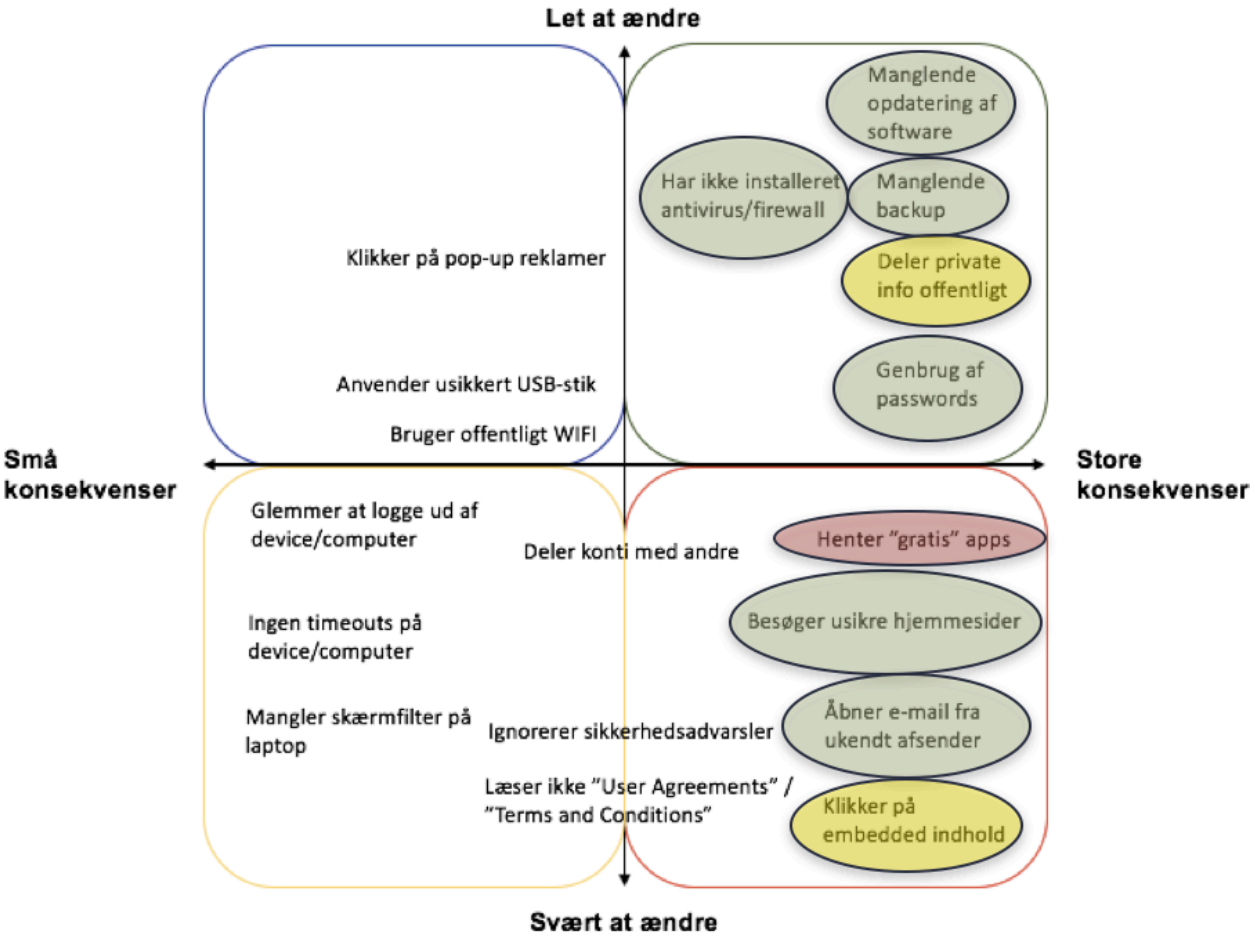
Litteratur: Kahneman & Tversky 1992, Lewis 2008, Eysenck 2012, Milgram 1963, Proofpoint 2016.

Nogle af eksperterne peger på, at dette adfærdsmønster vil komme til at medføre meget store problemer i fremtiden. Det skyldes, at den digitale adfærd centreres i højere og højere grad omkring smartphonen, og at efterspørgslen på apps i takt hermed er stigende. En del af de apps der findes er imidlertid ikke sikre, og man risikerer at kompromittere ens sikkerhed ved at downloade disse. Dette gælder dog langt overvejende for apps til smartphones med Android som styresystem, da Apples sikkerhedskrav til apps er meget høje hvorfor det næsten er umuligt at få skadelige apps lagt på deres 'app store'. Et relateret adfærdsmønster der er særligt kritisk, er gratis download af apps der normalt koster penge. Sideløbende med de officielle app stores er der nemlig opstået platforme, hvor dyre betalingsapps kan hentes gratis. Ofte er koden i disse apps dog blev ændret, således at de ikke blot tjener deres tiltænkte formål, men samtidig stjæler dine private informationer eller på anden måde kompromitterer din digitale sikkerhed.

Eksperter, der fremhæver adfærdsmønsteret: Angela Sasse, Jan Kaastrup.

I figur 2.1 herunder fremgår alle identificerede adfærdsmønstre samt angivelse af, hvilke der blev udvalgt. Umiddelbart under skemaet beskriver vi for hvert adfærdsmønster de centrale argumenter, der har været afgørende i til- eller fravalget af adfærdsmønsteret. Argumenterne i prioriteringen er baseret på de syv ekspertinterviews, som indgår i argumentationen for udvælgelse af de kritiske adfærdsmønstre. Alle ekspertinterview findes i transskriberet form i bilagsmaterialet.

Figur 2.1



*I skemaet skelnes der mellem to tidligere nævnte parametre, henholdsvis hvor store konsekvenser den givne adfærd har og hvor let den er at ændre. Markeret med **grøn** ring er de seks oprindeligt udvalgte adfærdsmønstre. Dertil er to adfærdsmønstre markeret med **gul** ring – det er baggrundsadfærd, som indirekte er med i udvalget. Markeret med **rød** ring er et enkelt adfærdsmønster, som er placeret i en bobler-kategori.*

3.0 Fra Adfærd til Målrettede Budskaber

Dette kapitel er det centrale for afrapporteringen. I det følgende gennemgås rejsen fra adfærdsafdækning til målrettede budskaber. Det gælder altså fra hypotesetest af de seks udvalgte adfærdsmønstre i spørgeskemaet, hvis resultater blev anvendt direkte til udarbejdelse af budskaber, og til brugertest af budskaberne, senere tilretning, segmentering og anbefaling af kanaler. Hvert adfærdsmønster bliver gennemgået individuelt fra research, ekspertinterview, resultater fra spørgeskema og brugertest og til endelige anbefalinger. Alle grafer og visualiseringer fra spørgeskemaet findes i bilagsmaterialet.

Indledningsvist gennemgås overordnede indsigter om danskernes opfattelse af de mest centrale komponenter i it-sikkerhed: It-sikkerhed/-kriminalitet generelt, den it-kriminelle og ofret for it-kriminalitet.

Det er væsentligt at dykke ned i disse komponenter, idet den endelige budskabskommunikation skal øge forståelsen for problemstillingen og motivationen for at handle på den. Og for at kunne øge det, er man først nødt til at forstå, hvordan danskerne forstår universet omkring it-sikkerhed og aktørerne i det. Denne forståelsesramme udgør *tonen* og *formen* i den optimale måde at kommunikere budskaber om it-sikkerhed på.

Efter disse overordnede indsigter dykkes der mere specifikt ned i hvert enkelt af de udvalgte adfærdsmønstre.

På baggrund af indsigterne fra spørgeskemaet i Fase 2 udviklede /KL.7 en række budskaber, som blev testet kvalitativt i 50 brugertest: 20 borgere, 22 medarbejdere og 8 it-ansvarlige. De it-ansvarlige blev inddraget som konsekvens af konklusionen fra spørgeskemaet om, medarbejdere i høj grad ’udliciterer’ it-sikkerheden til arbejdspladsen, dvs. it-afdelingen. Brugertestene varede hver 15 minutter og blev udført som såkaldte ’think aloud’-tests, der i al sin enkelthed handler om at afdække forståelse og handlingsmotivation på baggrund af en semistruktureret interviewform.

Tabel 3.1 herunder viser rekrutteringen af borgere til brugertest, fordelt på disse segmenter, mens tabel 3.2 viser rekrutteringen af medarbejdere og it-ansvarlige fordelt på de centrale segmenteringsvariable branche, offentlig/privat og større/mindre (>35 / <35 ansatte).

Tabel 3.1: Borgere i Brugertest

Køn	Alder	Uddannelse	Teknologikyndighed
Mænd: 10	Yngre (18-39): 7	Ungdomsudd.: 4	Begynder: 6
Kvinder: 10	Midaldrende (40-59): 6	Erhvervsfaglig: 3	Rutineret: 7
	Ældre (60-80): 7	Kort videreg.: 3	Ekspert: 7
		Mellemlang videreg.: 4	
		Lang videreg.: 3	

Tabel 3.2: Medarbejdere og IT-ansvarlige i Brugertest

Branche	Offentlig/privat	Større/Mindre	Antal medarb.	Antal IT-ansv.
Forsikring	Privat	Større	3	1
Finans	Privat	Mindre	3	1
Sundhed	Offentlig	Større	4	0
Boligorg.	Privat	Mindre	0	1
Natur og miljø	Halvoffentlig	Større	1	1
Myndighed	Offentlig	Større	1	0
Digitalt design	Privat	Mindre	5	1
Filantropi	Halvoffentlig	Større	3	1
Sundhed	Privat	Mindre	2	1
Kommunikation	Privat	Mindre	0	1

Spørgeskemaet viste, at der var centrale forskelle i viden og forestillinger om IT-sikkerhed på køn, forskellige aldersgrupper, uddannelsesniveauer og teknologikyndighed. Derfor besluttede /KL.7, at brugertesten også skulle afspejle denne segmentering.

Indledningsvist gives en oversigt over de centrale indsigter, projektet opnåede i Fase 1-3.

Tabel 3.3 herunder viser, hvilke centrale pointer om danskernes oplevelse af it-sikkerhed generelt og deres mere specifikke forestillinger om de it-kriminelle og ofrene, som skal adresseres og på hvilken måde. Der er indsat referencer under Fase 1-kolonnen til de eksperter, hvis udtalelser understøtter de respektive pointer.

Tabel 3.3: Overordnede pointer om it-sikkerhed

	Fase 1	Fase 2	Fase 3
	Research og ekspertinterview	**Survey**	**Brugertest**
	Udvælgelse af kritiske adfærdsmønstre, opstilling af hypoteser	**Afprøvning af hypoteser, udvikling af budskaber**	**Optimering af budskaber med kontekstinput**
It-sikkerhed generelt	The cyber-disinhibition effect – vi føler os fri, anonyme og uovervågede på nettet, selvom vi er det modsatte. *(Mary Aiken, Christian Jæhger, Angela Sasse, Jan Kaastrup, Rasmus Theede)*	Danskerne oplever it-trusler som abstrakte og afkoblet fysiske trusler	Budskabskommunikationen skal kropsliggøres – det øger forståelsen af truslen og den oplevede evne til at handle
Den it-kriminelle	It-kriminelle ved mere om menneskers psykologi og adfærd end om kompliceret kodning, og de arbejder inden for alm. arbejdstid *(Mary Aiken, Christian Jæhger, Angela Sasse, Rasmus Theede)*	Danskerne forestiller sig,at den typiske it-kriminelle er klog og udspekuleret hackertype fra Østen	Italesæt den it-kriminelle som en tricktyv/svindler
Offeret for it-kriminalitet	Alle er potentielle ofre for it-kriminalitet (*Alle eksperter*)	Danskerne forestiller sig, at det typiske offer er en naiv, uforsigtig, ældre kvinde	Italesæt offeret som os alle sammen

Tabel 3.4 herunder viser centrale indsigter om de enkelte udvalgte adfærdsmønstre, og hvad der på baggrund af brugertestene i sidste ende anbefales til overordnet budskabskommunikation.

Tabel 3.4: Indsigter om De Udvalgte Adfærdsmønstre

	Fase 1	Fase 2	Fase 3
	Research og ekspertinterview	**Survey**	**Brugertest**
	Udvælgelse af kritiske adfærdsmønstre, opstilling af hypoteser	**Afprøvning af hypoteser, udvikling af budskaber**	**Optimering af budskaber med kontekstinput**
Manglende backup	Gøres for sjældent og af for få	Danskerne synes ikke, det særligt vigtigt, og især medarbejdere gør det meget sjældent.	Danskerne skal have at vide, nøjagtigt hvordan man tager backup, og hvordan det bliver gjort til en ugentlig vane.
Manglende installation af Antivirus/Firewall	Mange har det ikke installeret	Danskerne synes, det er meget vigtigt. Men har kun meget overordnet forestilling om, hvad Antivirus/Firewall er.	Danskerne skal have at vide, hvilke programmer de skal kigge efter, og at der skal mere end Antivirus/Firewall til at holde dem sikre.
Manglende opdatering af Styresystem og Software	Mange gør det ikke, hvilket er hovedårsagen til mange større cyberangreb	Danskerne mener ikke, det er særligt vigtigt at gøre, og de kobler det kun delvist med it-sikkerhed	Danskerne skal have hjælp til at sætte automatisk opdatering til, og de skal have at vide, at det er koblet til it-sikkerhed.
Genbrug af Passwords	Det er umuligt at huske, konstruere og fornye unikke og stærke passwords	Danskerne genbruger i stor stil, og de oplever det ikke som et problem	Danskerne skal have støtte til sikker konstruktion og opbevaring af passwords. Teknologiske løsninger (f.eks. password manager) fungerer ikke for alle.
Indtaster Personlige Oplysninger på Usikre Hjemmesider	Næsten ingen ved, hvordan en usikker hjemmeside ser ud, og hvad 'usikker' indebærer af risiko	Visuelle cues i browservinduet forbedrer danskernes risikovurdering	Danskerne skal have konkrete råd til, hvad de skal kigge efter i deres browservindue.
Åbner Indhold i E-mail fra Ukendt Afsender	Skyldes uopmærksomhed hos brugeren og psykologisk kompetence hos it-kriminelle	Danskerne oplever det som en meget alvorlig trussel, men mangler konkrete handleregler	Konkrete, relevante handleregler gør danskerne bedre i stand til at imødegå truslen.

Disse indsigter giver et solidt udgangspunkt for at formulere overordnede anbefalinger til en budskabskommunikation, som både øger danskernes forståelse for problemstilling, deres motivation for at handle og deres oplevede evne til faktisk at udføre handlingerne. Det er imidlertid klart, at ikke alle borgere og alle medarbejdere har samme udgangspunkt for forståelse, motivation og handling. De følgende afsnit gennemgår de segmenterede anbefalinger for it-sikkerhed generelt og de enkelte adfærdsmønstre specifikt.

3.1 It-sikkerhed Generelt

3.1.1 Research

Adfærd, kriminalitet og sikkerhed er rent psykologisk svært for mennesker at forstå. Vores hjerner og kognitive evner har gennem tusindvis af år udviklet sig i et miljø, som bestod af andre mennesker og genstande, som vi *rent fysisk* har kunne observere og interagere med. En digital verden er – i hvert fald indtil videre – defineret ved fraværet af fysiske observationer og interaktioner, og det er med til at gøre det svært for mennesker at forstå de potentielle farer ved at have en usikker, digital adfærd (Aiken 2016).

Når vi forsøger at forstå eller blot at tænke over noget, som vi ikke kan interagere med direkte har hjernen udviklet evnen til at benytte en såkaldt **mental model** (Morgan 2002). Ud fra erfaringer, forestillinger og overbevisninger laver hjernen en model – altså en forsimplet version – af et abstrakt fænomen.

> *The image of the world around us, which we carry in our head, is just a model. Nobody in his head imagines all the world, government or country. He has only selected concepts, and relationships between them, and uses those to represent the real system (Forrester 1971).*

I relation til IT-sikkerhed vil mennesker bruge deres *egen* viden om computere, kriminelle, informationssikkerhed, osv. til at forstå at kommunikation, der handler om, hvordan man undgår it-kriminalitet, hvad det er, hvor stort problemet er, osv.

3.1.2 Survey – Danskernes Forestillinger om It-Kriminalitet

Mentale modeller kan have stor indflydelse på menneskers fortolkninger af kommunikation og generel adfærd. Derfor valgte vi at undersøge en række af danskernes mentale modeller, som relaterer sig til it-kriminalitet og –sikkerhed.

For at afkode danskernes mentale model for en cyberkriminel bad vi dem om at gøre følgende:

Forestil dig en typisk cyberkriminel. Beskriv denne person med de første 3-5 ord, der falder dig ind.

Danskerne tror, at en cyberkriminel er:

1. Ung
2. Mand
3. Intelligent
4. Udspekuleret
5. Nørd/hacker/ekspert i computere
6. Fra Asien/Rusland

Denne mentale model kan have en stor indflydelse på danskernes adfærd. Nytter det overhovedet noget at sikre min computer, hvis de cyberkriminelle er så dygtige hackere? Bryder de ikke bare døren ind alligevel? Når bekymringer som disse ser ud til at være så centrale for danskernes opfattelse af it-kriminelle, leder det til apati og mangel på handlekraft. Det gør, at danskerne vil være mere tilbøjelige til at anskue it-kriminalitet som et problem, de ikke selv kan gøre noget ved. Det er derfor væsentligt, at den endelige budskabskommunikation italesætter de it-kriminelle som nogen, hvis arbejde man rent faktisk godt kan forhindre, selvom man ikke er en haj til kodning.

Al it-kriminalitet har også et offer. Derfor lavede vi samme øvelse for at afkode danskernes mentale model for et typisk offer ved at bede respondenterne om at beskrive det typiske offer med 3-5 ord. Her fandt vi ligeledes et gennemgående mønster i besvarelserne.

Danskerne tror, at et typisk offer for cyberkriminalitet er:

1. Naiv/godtroende
2. Uskyldig/uheldig/uforsigtig
3. Ældre kvinde
4. Teknisk uvidende/dum

Adfærdsvidenskaben viser, at mennesker tror, at negative hændelser i højere grad sker for andre end os selv (Chapin & Coleman, 2009). Hvis det typiske offer for de kriminelles handlinger er en ældre, naiv kvinde, som ikke forstår sig på teknologi, og hvis man ikke selv passer på denne beskrivelse, så opleves risikoen for, at man selv bliver et offer forsvindende lille. Samtidig viste surveyen også, at danskerne direkte adspurgt overvejende vurderer, at det ikke er folks egen skyld, hvis de bliver ofte for cyberkriminalitet.

Danskerne vurderer selv, at deres digitale adfærd generelt er forholdsvis sikker. De vurderer, at den en er mere sikker på arbejdet end i hjemmet, men der er dog også en større tendens til, at de har svært ved at vurdere deres digitale adfærd på arbejdspladsen. Der er altså både flere positive svar og flere 'ved ikke'-svar. Dette skyldes formentlig en ansvarsfralæggelse og en oplevelse af, at "nogle andre har ansvaret for min it-sikkerhed".

Danskerne er et tillidsfuldt folkefærd. Af de interviewede eksperter nævnte bl.a. Christian Jæhger, at det er noget af årsagen til, at danskerne ikke har de store skrupler ved at dele egne personfølsomme info digitalt. Surveyen viser dog, at danskernes tillid til andre mennesker på nettet er lavere end til folk i det offentlige rum. Samtidig med, at den enkelte dansker føler sig mere sikker, fri og uovervåget i den digitale verden end i den fysiske (Aiken 2016), har han/hun altså en oplevelse af andre mennesker på nettet som potentielt mere farlige. Det kan skyldes, at andre mennesker på nettet er sværere at sætte ansigt på og mere ukendte, hvilket i sig selv er utryghedsskabende. Dernæst kan det ses som en bekræftelse af, at it-kriminalitet foregår i en verden, som den enkelte ikke rigtig oplever at have greb om. Andre mennesker på nettet opleves som mere ukendte og farlige, men på nettet oplever man også sig selv som mere anonym og fri for fare. Disse to faktorer viser til sammen, at det er nødvendigt kommunikativt at bringe den digitale verden ind i den fysiske for *på samme tid* at øge danskernes forståelse, motivation og evne til at handle.

Sammenhængen gælder imidlertid kun for de højest uddannede og de mest it-kyndige. De, der maksimalt har gennemført folkeskolen, har lavere tillid til folk i offentligheden end på nettet. Der er altså en social ulighed, som materialiserer sig i væsentlige forskelle i danskernes risikoopfattelse i hhv. den fysiske og den digitale verden. Dette bekræfter en generel pointe fra risikopsykologien om, at oplevet risiko er det samme som oplevet kontrol over egen livssituation. Bredt set har de mere velstillede/-uddannede mere kontrol over egen livssituation, hvilket materialiserer sig i højere oplevet tryghed, mens det forholder sig omvendt for de mindre velstillede-/uddannede (Ropeik 2010).

Desuden er det interessant at betragte danskernes opfattelse af, hvilke tiltag, der er mest effektive til at nedbringe it-kriminalitet, og hvilke trusler, der er værst. Tabel 3.5 og 3.6 umiddelbart nedenfor viser disse informationer. Her fremgår det tydeligt, at danskernes opfattelse af it-sikkerhed ikke stemmer helt overens med fakta. Ifølge eksperterne er genbrug af passwords, jævnlig backup og undladelse af deling af privat info offentligt de tre mest afgørende tiltag for at undgå at blive offer for it-kriminalitet, mens antivirus/firewall blev beskrevet som et af de mere perifære af de udvalgte adfærdsmønstre. Danskernes rangering er imidlertid fuldstændig modsat. Det samme gælder for danskernes rangering af truslers hyppighed, hvor blokering af dataadgang placeres allernederst – på trods af, at truslen fra ransomware af eksperterne blev vurderet som en af de mest udbredte og alvorlige.

Tabel 3.5: Danskernes rangering af tiltags effektivitet ift. at nedbringe risikoen for it-kriminalitet

Nr.	Tiltag
1	**Installere antivirus-program og firewall**
2	**Undlade at åbne indhold i usikre e-mails**
3	**Holder software opdateret**
4	**Undlader at besøge usikre hjemmesider**
5	**Genbruger ikke passwords**
6	**Undlader at dele privat info offentligt**
7	**Tager backup jævnligt**

Tabel 3.6: Danskernes rangering af it-sikkerhedstruslers alvorlighed

Nr.	Trusler
1	**Nogen sender dig en e-mail med usikker indhold, som du åbner**
2	**Nogen eller noget får dig til at klikke på et link til en usikker hjemmeside**
3	**Nogen inficerer din computer med virus el. lign. malware**
4	**Nogen får ulovlig adgang til dine personlige oplysninger**
5	**Nogen får ulovlig adgang til dine password**
6	**Nogen inficerer din smartphone med virus el. lign. malware**
7	**Nogen blokerer adgangen til dine data på din computer**

3.1.3 Brugertests

Det er afgørende, at den endelige kommunikation imødegår de mentale modeller for it-kriminalitet, it-kriminelle og ofrene, så danskerne i højere grad oplever en handlekraftighed i forhold til problemstillingen. Derfor indgik nye bud på disse mentale modeller i de kvalitative brugertest af budskaber i Fase 3. Resultaterne af denne del af brugertestene er opsummeret i nedenstående skema.

Tabel 3.7: Oversigt over metaforer og deres kommunikative fordele/ulemper

Den Overordnede Fortælling			
Metafor	*Sikker computer*	*Hygiejne*	*Sikkert hjem*
Eksempel på formulering	”Firewall og antivirus er **muren ind til dine informationer**.”	”En computer er kun sikker, hvis du **holder den ren**.”	”En usikker computer **inviterer kriminelle ind i stuen.**”
Fordele	Det er nemt at forstå, at ens computer kan have ”huller” eller usikre indgange, hvor de kriminelle kan bryde ind.	Erfaringsmæssigt er det nemt at forstå, at dårlig hygiejne kan lede til sygdom (læs: virus).	Tanken om at invitere kriminelle ind i ens eget hjem er yderst ubehagelig og hjemmet er også der, hvor alle vores mest følsomme informationer og relationer er at finde.
Ulemper	Det er nemt at fraskrive sig ansvaret for, at ens computer er sikker, især på arbejdspladsen. Desuden fjernes al fokus på egen adfærd.	Selv de mest hygiejniske mennesker har en risiko for at blive syge, og metaforen indeholder ingen konnotationer om bevidste, kriminelle handlinger.	-
Et Typisk Offer			
Metafor	*Naiv senior*	*Den uheldige borger*	*Kollektivet*
Eksempel på formulering	”Typisk går it-kriminelle efter de borgere, som er **de mindst it-kyndige**.”	”It-kriminalitet bliver et større og større problem – hver 3. dansker **er kommet til** at invitere it-kriminelle ind i stuen.”	”**It-kriminalitet rammer os alle**. Men hvis du følger anbefalingerne og holder din computer og smartphone sikker, er du med til at gøre livet surt for de IT-kriminelle.”
Fordele	-	-	Hvis alle kan blive ofre for IT-kriminalitet betyder det også, at vi sammen kan være med til at gøre livet surt for de kriminelle.
Ulemper	Hvis det typiske offer for it-kriminalitet ikke ligner mig selv, så er der nok ikke en særlig stor risiko for, at jeg bliver ramt.	Hvis offeret bare er uheldig gør det ingen forskel i sidste ende, om man sikrer sin computer – og adfærd – eller ej.	-
Den it-Kriminelle			
Metafor	*Manipulator*	*Hacker*	*Trick-tyv*
Eksempel på formulering	”Jeg har alligevel ikke noget, der er værd at stjæle” og venter med at opdatere programmer eller at tage backup. Men **det er de it-kriminelle udmærket klar over**.”	”En af de mest risikable ting, man kan gøre, er at genbruge sit password på flere hjemmesider og login. Så skal den kriminelle nemlig kun **afkode dit password én gang** for at få adgang til mange af dine informationer.”	”Mange it-kriminelle sender **trick-mails** ud med links og vedhæftninger, som installerer farlige programmer.”
Fordele	Beskrivelsen af de kriminelle som nogen, der kan manipulere os til at gøre noget, vi ikke har lyst til, er ny for mange og skaber grundlag for handling.	Dette er den typiske måde at skrive it-kriminelle på, så borgerne kender den.	Alle har erfaringer – direkte eller indirekte – med at være udsat for tricktyveri. Det er ubehageligt men samtidig noget, hvor vi selv kan gøre noget for at undgå det.
Ulemper	En del brugere havde svært ved at tro på denne beskrivelse. Det fjerner også deres følelse af agens.	Hvis it-kriminelle er eksperter i den teknologi, det drejer sig om, så føler almindelige mennesker ikke, at de har en chance for at gøre noget for ikke at blive hacket.	-

Det fremgår tydeligt af ovenstående, at der er flest kommunikative fordele at hente i at italesætte it-sikkerhed som et sikkert hjem, det typiske offer som os alle sammen (kollektivet) og den it-kriminelle som en slags trick-tyv eller svindler. På baggrund af disse resultater anbefales det, at fremtidig kommunikation om it-sikkerhed benytter sig af de overordnede, konceptuelle rammer beskrevet i kolonnen til højre. Ud fra disse grundlæggende koncepter og metaforer opnås den bedste effekt i forhold til at udnytte danskernes forståelser – og misforståelser – for, hvad it-kriminalitet og –sikkerhed er.

3.1.4 Opsummering: Gør det digitale fysisk

Det digitale er abstrakt og svært at forholde sig til. Den it-kriminelle anses for at være en kodestærk person langt væk, som udfører et arbejde, danskerne ikke oplever, at de kan gøre noget ved. Det typiske offer bærer ikke selv skylden – men det er heller ikke 'mig'. I den fysiske verden er det – modsat i den digitale – nemt at forstå kriminalitet som noget, man selv kan gøre noget for at forebygge. Det er derfor nødvendigt at bringe it-kriminalitet ind i den fysiske verden ved simpelthen at gøre det digitale fysisk. Det vil sikre budskabskommunikationens effektivitet til at øge motivation for at handle og oplevet handlekraftighed ift. problemstillingen.

Nedenfor er de generelle indsigter og anbefalinger om danskernes generelle forståelse skematiseret og de tre faser opsummeret.

Grundlæggende metafor for indsatsen

Anbefaling: Brug hjemmet som grundlæggende metafor.

Som alle andre mennesker er danskerne enormt sensitive over for trusler, som rammer deres mest intime sfære: Deres eget hjem. Ved at skabe kobling mellem fysiske indbrud i hjemmet og it-kriminalitet skabes en mere fysisk og kropslig forståelse for fænomenet; den abstrakte trussel bliver gjort *mærkbar*. Det kan være svært at forstå, hvordan en hacker kan kigge med, når man surfer på nettet, men hvis selvsamme situation bliver formuleret som en frem, der står og kigger ind ad stuevinduet, bliver den rent intuitivt meget nem at forstå. Det øger samtidig motivationen for at handle på problemstillingen, netop fordi den bliver sat ind i en familiær ramme.

Gør det digitale fysisk

Anbefaling: Kropsliggør rådene metaforisk.

Hjemmet som metafor har en direkte indflydelse på, hvordan indsatsens råd til sikker, digital adfærd bør formuleres. Hvert af de udvalgte adfærdsmønstre – og rådene til at undgå dem – kan med fordel tænkes ind i den metaforiske ramme. Dette kaldes med et teoretisk udtryk "embodied cognition", dvs "kropsliggjort kognition", eller slet og ret kropsliggørelse. Det er en række konkrete måder, vi anbefaler at bruge metaforen 'hjemmet' aktivt for at understøtte forståelsen af vigtigheden ved hvert enkelt adfærdsmønster og gøre det mere overskueligt at handle. Ud over at det giver en mere sammenhængende kommunikation at tage udgangspunkt i den samme metaforiske verden, så har kropsliggørelsen også en adfærdsmæssig funktion: Når en problemstilling bliver gjort fysisk og håndgribeligt, så opleves det nemmere at handle på den, end hvis den var abstrakt. Når man så at sige kan 'se handlingen for sig', er det også mere overskueligt at foretage den. At italesætte passwords som fysiske nøgler gør det både mere forståeligt, hvorfor det er vigtigt at passe på dem, og handlingen bliver mere konkret.

Hvem er offeret for it-kriminalitet?

Anbefaling: Offeret for it-kriminalitet skal italesættes som os alle sammen. Kommunikationen skal opfordre til, at 'vi taler om it-sikkerhed med hinanden'.

Forståelse af, hvem det typiske offer for it-kriminalitet er, har en stor indflydelse på danskernes adfærd. Ved at formulere offeret som *os alle* skabes en forståelse af, at det ikke alene er ældre, naive kvinder, der rammes (jvnf. den mentale model for et typisk offer). Samtidigt gør denne formulering det muligt at formulere den samlede indsats for større it-sikkerhed som en "os-mod-dem" kamp (os = almindelige borgere, dem = de it-kriminelle); vi skal hjælpe hinanden og stå sammen for at komme problemet til livs.

Det betyder samtidig, at it-kriminalitet – som Angela Sasse også nævner direkte i ekspertinterviewet (se bilag) – i højere grad skal blive noget, 'vi taler om med hinanden'. Det kræver, at danskerne i højere grad identificerer sig med det typiske offer, og at det opleves mere som et fælles problem for alle danskere end et isoleret problem for en lille subgruppe af naive ældre kvinder.

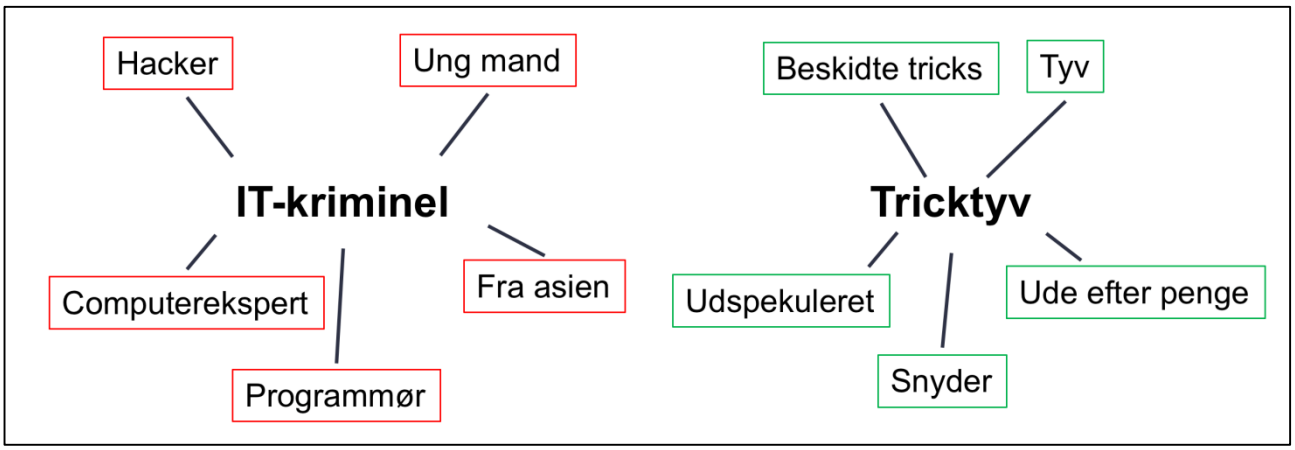
Italesættelsen af offeret som os alle sammen er derfor vigtig af to årsager: 1) Fordi den indgyder det påtrængende i at gøre noget ('det kan også ske for dig'), og 2) fordi den opildner til en fælles samtale, som er afgørende for, at it-sikkerhed bliver noget, vi kan tale åbent og frit om med hinanden og dermed sammen stå bedre rustet mod fremtidige trusler.

Italesættelse af den it-kriminelle

Anbefaling: Den it-kriminelle skal italesættes og visualiseres som en tricktyv/svindler.

Hvis en it-kriminel italesættes som en ekspert i programmering og kodning skaber det en uhensigtsmæssig forståelse af problemstillingen; hvis de er så gode til det med computere, så har jeg som borger ikke en ærlig chance for at sikre mig. Derfor anbefales det at italesætte den it-kriminelle som en tricktyv. Langt de fleste danskere har erfaringer med tricktyve eller svindlere – direkte eller indirekte. Det medfører en større mental aktivitet, når problemet omtales, og giver samtidigt en forståelse af, at man selv kan gøre noget for ikke at blive snydt; tricktyven gør, hvad han kan, for at snyde sig til mine penge, men han er ikke klog nok til at snyde mig!

Vi anbefaler derfor at bruge ord og koncepter, som har med tricktyve eller svindlere at gøre, når de it-kriminelle omtales:



Efter disse generelle anbefalinger til budskabskommunikationens overordnede tone, gennemgås i det følgende anbefalingerne til de udvalgte kritiske adfærdsmønstre. Hvert adfærdsmønster gennemgås enkeltvis fra research til segmenterede budskabsanbefalinger.

3.2 Manglende Backup

3.2.1 Research

Den manglende backup er et stort problem, som kun en mindre del af befolkningen er opmærksomme på vigtigheden af. Mange af eksperterne er enige om, at dette adfærdsmønster er et af de allermest centrale. Det er samtidig nøglen til løsningen af flere andre problemer. Ifølge Christian Jæhger havde ransomware eksempelvis ikke været et problem, hvis folk tog de backups, de skulle. Rasmus Theede udtaler også, at dette adfærdsmønster er blandt de lavthængende frugter, som med relativt få midler vil kunne forbedre danskernes informationssikkerhed markant. Det er altså et adfærdsmønster, som har store konsekvenser, men som vi også har gode odds for at ændre på.

Eksperter, der fremhæver adfærdsmønsteret: Angela Sasse, Christian Jæhger, Rasmus Theede.

For at undersøge hypotesen om, at danskerne ikke rigtig er klar over, hvorfor det er vigtigt at tage backup, inkluderede vi en validering af denne hypotese i spørgeskemaet.

3.2.2 Survey

Til at starte med spurgte vi ind, hvor vigtigt danskerne synes, det er, at tage backup.

Hvor vigtigt vurderer du, det er at tage backup af indholdet på din computer jævnligt? (Angiv dit svar på en skala fra 1-7, hvor 1 er, at det slet ikke er vigtigt, og 7 er at det er meget vigtigt).

Danskerne vurderer, at det overvejene er meget vigtigt at tage backup jævnligt:

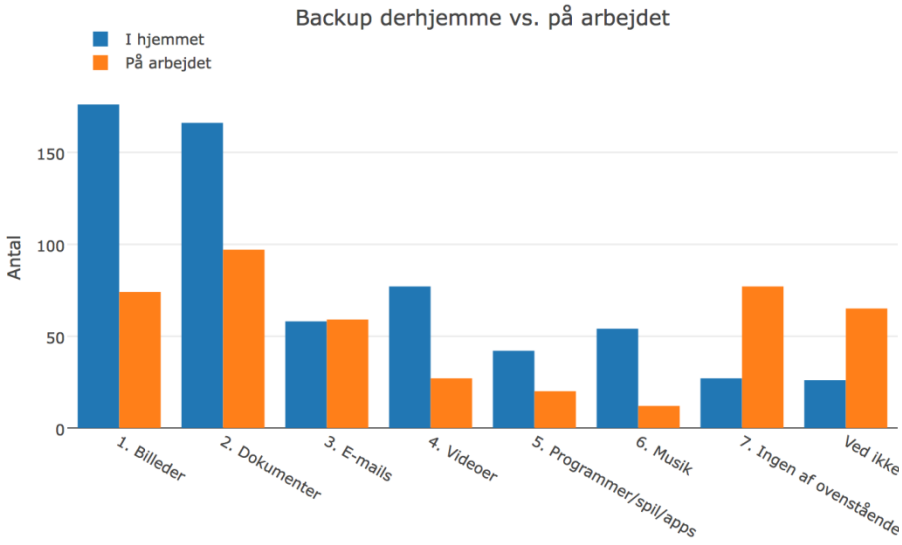
Vi bad også danskerne i undersøgelsen om at rangere forskellige tiltag efter, hvor effektive de tror, de er, for at sikre sig mod it-kriminalitet. Her danner der sig et mere nuanceret billede af danskernes forståelse af backup.

Danskerne rangerer i surveyen ”tage backup jævnligt” som værende det absolut *mindst* effektive tiltag for at sikre sig mod it-kriminalitet. Desuden rangerer danskerne ransomware (her formuleret som ”at blokere adgangen til data”) som værende den trussel, der sker mindst hyppigt. Det er interessant, fordi eksperterne rangerede backup blandt de allermest vigtige tiltag. Her er der altså en diskrepans mellem danskernes opfattelse af vigtigheden af at tage backup, og hvor vigtigt det rent faktisk er. Det er afgørende, at fremtidige kampagneindsatser tager dette til efterretning og forsøger at hjælpe danskerne med at forstå, hvor vigtigt det er at tage backup.

På baggrund af besvarelserne i surveyet tegner sig derfor et billede af, at danskerne godt ved, at det er vigtigt at tage backup af sine data – de ved bare ikke, *hvorfor* det er vigtigt.

Som tidligere nævnt finder vi desuden igen en forskel i adfærden derhjemme i forhold til på arbejdet. Billeder og dokumenter er den type filer, som respondenterne – i hvert fald adspurgt – finder vigtigst at backe up. På arbejdet er der en større tendens til, at respondenterne ikke ved, hvad proceduren for backup er.

Figur 3.1: ”Hvilke slags filer tager du backup af?”



Denne observation tolkes som en tendens til en ansvarsfraskrivelse for IT-sikkerhed, når man er på arbejdet.

3.2.3 Brugertests

Brugertestene adfækkede danske borgere, medarbejdere og it-ansvarliges forståelse af, hvad backup er, og hvorfor det er vigtigt. Her var de overordnede indsigter, som fremgår af tabel 3.8 nedenfor, 1) at en del af borgerne ikke ved, hvad det vil sige at tage backup og 2) at mange ikke oplever at have data på deres computer, som er værd at stjæle.
Hos virksomhederne styres backup typisk centralt, men især de mindre virksomheder tilkendegiver, at det ikke gøres ofte nok.

Tabel 3.8

Fase	Borgere	It-Ansvarlige	Medarbejdere
1. Research	Gøres for sjældent og af for få	Gøres for sjældent og af for få (årsag til ransomware)	Gøres for sjældent og af for få (årsag til ransomware)
2. Survey	Vi gør det ikke, og vi synes ikke, det er særlig vigtigt	-	Vi gør det ikke, og vi forholder os ikke til, om det bliver gjort
3. Brugertests (tag backup mindst én gang om ugen)	**Ældre begyndere:** Ved ikke, hvad ”backup” er. **Unge begyndere:** Jeg har alligevel ikke noget af værdi. **Rutinerede og eksperter (alle aldersgrupper):** Det skal gøres automatisk, ellers får jeg det aldrig gjort	**Større vh.:** Backup styres centralt, således at det bliver gjort automatisk med relativt høj frekvens (dvs. minimum ugentligt) **Mindre vh.:** Backup styres centralt, men bliver gjort mere ad hoc og med lavere frekvens (ca. hvert halve år)	**Alle:** It-afdelingen har ikke styr på vores private data på arbejdscomputeren og –telefon.

3.2.4 Opsummering: Forklar, hvorfor det er vigtigt at tage backup

Anbefaling: Forklar borgerne, hvorfor det er vigtigt at tage backup, og hvordan det bliver gjort automatisk. Hjælp de it-ansvarlige med at gøre medarbejderne bedre i stand til at tage personlige backup af private data på arbejdscomputer og –telefon.

3.3 Manglende Installation af Antivirus/Firewall

3.3.1 Research

Der er blandt eksperterne delte meninger om dette adfærdsmønster – både vigtigheden af at adressere det og sandsynligheden for at ændre det. Anders Kjærulff ser antivirus og firewall som en helt central del af, hvad han kalder ”*en god computerhygiejne*”. Hvis alle havde installeret denne software, ville det højne det generelle digitale sikkerhedsniveau betragteligt.

Angela Sasse udtrykker dog skepsis overfor blot at anbefale danskerne at installere ’et eller andet’ antivirusprogram, fordi markedet er meget svært at overskue for den enkelte. Hun mener faktisk, at markedets uoverskuelighed er en af de væsentligste årsager til, at relativt mange undlader at investere i antivirus/firewall. Hvis vi derimod – gennem strategisk partnerskab el.lign. – kan anbefale og/eller udvikle én bestemt software, ser Sasse gode muligheder for adfærdsændring. Desuden mener hun, at en sådan anbefaling er relativt nem at måle effekt på (antal downloads før/efter indsatsen påbegyndes).

Manglende installation af antivirus/firewall er altså hverken blandt de allervigtigste eller nemmeste adfærdsmønstre at adressere. Når det alligevel er blevet udvalgt, skyldes det de relativt lovende perspektiver i en partnerdrevet anbefaling af en bestemt software.

Eksperter, der fremhæver adfærdsmønsteret: Anders Kjærulf, Angela Sasse,

3.3.2 Survey

Iflg. surveyen opfatter danskerne antivirus og firewall som værende det mest effektive tiltag, man kan gøre, for at sikre sig mod it-kriminalitet, og de angav infektion af virus/malware som noget af mest hyppigt forekommende (kun overgået af e-mails med usikkert indhold og links til usikre hjemmesider). En væsentlig pointe er her, at vira og malware ikke anses som værende lige så stor en trussel, når det kommer til antivirus og firewall på ens smartphone. Selvom antivirus/firewall anses som vigtigt af danskerne, gælder det primært på computeren. På smartphonen er der en noget mindre bevidsthed om, at det er vigtigt at have installeret.

3.3.3 Brugertests

I brugertestene blev hypotesen om, at der er for mange valgmuligheder, når det kommer til at vælge et antivirus-program valideret. Mange respondenter udtalte ordret, at de forstår vigtigheden af at have sådan et program installeret. Samtidigt udtalte de også, at de har svært ved at navigere i markedet. Der er simpelthen for mange valgmuligheder! Adfærdsteoretisk kaldes dette fænomen *choice overload*; når hjernen bliver præsenteret for alt for mange valgmuligheder kan en typisk respons være, at den simpelthen undlader overhovedet at tage et valg.

Fase	Borgere	It-Ansvarlige	Medarbejdere
1. Research	Mange har det ikke installeret	-	Mange har det ikke installeret
2. Survey	Vi tror, det er det mest effektive	-	Vi tror, det er det mest effektive
3. Brugertests (installér antivirus – også på din smartphone)	**Alle:** Det er meget vigtigt at gøre. Men hvilken én skal vi bruge?	**Alle:** Det styrer vi centralt	**Alle:** Det har it-afdelingen styr på

3.3.4 Opsummering: Antivirus/firewall er kun første skridt

Anbefaling: Antivirus og firewall benytter et sprog, som danskerne kan forstå. Men det skal tydeliggøres, at man ikke får en sikker computer alene ved at have et antivirus-program installeret.

Antivirus/firewall er den første reference, danskerne kommer i tanke om, når man taler om it-sikkerhed. Danskerne er alene i tvivl om, hvilket antivirus-program, de skal investere i. Det gælder især mht. smartphone. Men da en offentlig kampagneindsats ikke kan anbefale et specifikt produkt, og da den fabriksinstallerede antivirus-/firewall-software på nyere Windows- og Mac-computere samt iPhones er på højde med markedets bedste (Casey 2016), bør det vigtigste budskab være et andet: At installering af sådan et program er et godt første skridt at tage på vej til større it-sikkerhed – men at det ikke er nok.

Det giver ikke mening at fortælle danskerne, at antivirus/firewall er vigtigt at have installeret på sin computer. Det ved de allerede. Og det er ikke heller ikke muligt at hjælpe danskerne med deres eneste tvivl, nemlig hvilket produkt de skal investere i. Slutteligt er det heller ikke nødvendigt for den signifikante del af befolkningen, som har en nyere Windows-/Mac-computere og/eller en iPhone.

/KL.7 anbefaler derfor, at antivirus/firewall bruges som løftestang til at kommunikere de øvrige råd, som danskerne er mindre bevidste om vigtigheden af. **Vær klar i mælet om, at antivirus ikke er nok**, fordi it-kriminelle er tricktyve, som udnytter din usikre digitale adfærd i højere grad end huller i din antivirussoftware. Et andet bud kunne være at **slå dette råd sammen med opdatering af styresystemer og software** – det vigtigste for at holde antivirussoftwaren sikker, er, at den bliver opdateret så ofte som muligt.

Specifikt ift. smartphones er der behov for, at man gør Android-brugere opmærksomme på, at det er vigtigt at sikre deres telefon med solid antivirussoftware. Da det ikke er muligt at give en konkret anbefaling af en bestemt udbyder, vil det være nok med forøget bevidsthed om, at det er vigtigt at sikre sin telefon. Dette råd kunne med fordel slås sammen med en adressering af det fravalgte adfærdsmønster ”Download af uofficielle apps”, idet denne problemstilling også knytter sig specifikt til Android-brugere.

3.4 Manglende Opdatering af Styresystem og Software

3.4.1 Research

Der er bred enighed blandt eksperterne om, at dette adfærdsmønster bør have høj prioritet. Iflg. Anders Kjærulff er dette især udbredt blandt yngre mennesker. Det har vi dog ikke fået bekræftet fra andre kilder eller eksisterende rapportmateriale. Uanset om yngre mennesker er hårdest ramt på dette punkt, er det uhyre afgørende for den digitale sikkerhed, at det er på plads. Dette skyldes at softwareopdateringer ofte er direkte foranlediget af en sikkerhedsbrist eller en ny trussel, som serviceudbyderen forsøger at imødegå aktivt.

Rasmus Theede peger på at "…*langt størstedelen af alle uhensigtsmæssige digitale hændelser sker som følge af dårlig it-hygiejne.*", herunder at danskerne ikke holder deres programmer opdaterede. Samtidig er denne adfærd iflg. Angela Sasse blandt de mindre vanskelige at ændre, idet det er en éngangsadfærd, hvis man blot slår automatiske opdateringer til.

Selvom det potentielt er blandt de lettere adfærdsmønstre at ændre, er eksperterne enige om, at adfærdsændringen vil kunne opnås mest effektivt med teknologiske løsninger, som automatiserer opdateringen. En sådan løsning eksisterer heldigvis allerede i form af en app, som Jan Kaastrups firma CSIS har udviklet til automatisk at holde alle apps og programmer opdateret hele tiden.

Eksperter, der fremhæver adfærdsmønsteret: Anders Kjærulf, Angela Sasse, Rasmus Theede.

3.4.2 Survey

Ifølge resultaterne fra spørgeskemaet forstår danskerne, at det er vigtigt at holde software og styresystem opdateret. Det opleves dog som mere vigtigt, når der i spørgsmålsformuleringen bliver etableret en kausalitet mellem it-sikkerhed og opdatering af software og styresystem. Det tolkes som et tegn på, at danskerne i mindre grad er klar over, at opdateringer ikke blot er nye programfunktioner, men at de også ofte indeholder opgradering af it-sikkerheden ift. aktuelle trusler og/eller nyligt opdagede svagheder i programmeringen.

3.4.3 Brugertests

Gennem vores brugertests fandt vi, at koblingen mellem opdaterede programmer og it-sikkerhed ikke er særlig stærk i respondenternes bevidsthed. Nogle af respondenterne udtalte, at opdatering primært er et irritationsmoment, fordi programmer nogle gange rent visuelt ændrer udseende efter en opdatering. Opdatering bliver dermed af nogle set som værende primært et funktionsmæssigt spørgsmål og ikke noget, der er direkte relateret til it-sikkerhed.

Samtidigt er det ikke nok at råde danskerne til at slå automatisk opdatering til, da en del af respondenterne savnede konkrete råd om, hvordan man gør.

Fase	Borgere	It-Ansvarlige	Medarbejdere
1. Research	Alt for mange forsømmer det	Alt for mange forsømmer det (årsag til WannaCry-angreb)	Alt for mange forsømmer det (årsag til WannaCry-angreb)
2. Survey	Vi mener ikke, det er særligt vigtigt, og kobler det ikke entydigt med datasikkerhed	-	Vi mener ikke, det er vores ansvar
3. Brugertests (sæt automatisk opdatering til)	**Eksperter (alle aldersgrupper):** Vi skal have vejledning til, hvordan vi slår det til automatisk. **Begyndere og rutinerede:** Det er besværligt, og vi søger hjælp hos mere it-kyndige til det.	**Større:** Det styrer vi centralt **Mindre:** Vi styrer det centralt, men ikke automatisk	**Alle:** Det har it-afdelingen styr på

3.4.4 Opsummering: Gamle programmer er usikre programmer

Anbefaling: Gør sammenhængen mellem opdatering af software og styresystemer og it-sikkerhed mere tydelig og vis, hvordan man rent teknisk slår automatisk opdatering til.

På nyere Windows-computere (dvs. med operativsystemet Windows 10) er automatisk opdatering standardindstillet. Det er det dog ikke på Apple-produkter. På iPhone og iPad er det nemt at slå til: 1) Tryk på Indstilling, 2) [Dit navn], 3) Slå automatisk opdatering til for hver af dine apps og operativsystem. På Mac-computere er det tilsvarende enkelt: 1) Tryk på ”Systemindstillinger”. 2) Vælg”App Store”, 3) Markér alle fem tjekbokse i vinduet.

3.5 Genbrug af Passwords

3.5.1 Research

I den indledende desk research blev dette adfærdsmønster formuleret som ’Genbrug af svage passwords’. Men et flertal af eksperterne gjorde os opmærksom på, at det især er *genbrug*, der er problemet. Uanset styrken af det enkelte password, er det markant mere sårbart, hvis det selvsamme password genbruges. I praksis er det vigtigt ikke at genbruge sine passwords, fordi man derved kun behøver at få stjålet sine login-informationer én gang, før alle ens konti og data potentielt er kompromitterede. Der er således bred enighed om, at dette adfærdsmønster er helt centralt at rette en indsats imod.

DKCERT-undersøgelsen (2017) viste, at ca. to-tredjedele af alle danskere genbruger passwords. Hertil påpeger Mary Aiken såvel som Angela Sasse, at ingen almindelige mennesker rent faktisk kan huske et større antal unikke og stærke passwords i hovedet. Angela Sasse og Rasmus Theede foreslår samstemmigt to mulige teknologiske løsninger på denne problemstilling: Password manager, som genererer, lagrer og opdaterer unikke og stærke passwords, og to-faktor autentifikation, som (på de udvalgte tjenester, hvor det rent faktisk kan slås til, bl.a. Google og

Facebook) eliminerer behovet for at konstruere og huske stærke, unikke passwords ved at rutinemæssigt at afkræve identifikation gennem en personlig enhed.

Eksperter, der fremhæver adfærdsmønsteret: Angela Sasse, Jan Kaastrup, Mary Aiken, Rasmus Theede.

3.5.2 Survey

At undlade at genbruge passwords bliver rangeret forholdsvist lavt i spørgeskemaet.
Danskerne er tilsyneladende ikke klar over, hvor potentielt farligt det er at genbruge et password på tværs af logins.
Spørgeskemaet viser også, at danskerne vurdere deres primære passwords er forholdsvis stærke, men igen er der en markant forskel mellem den digitale adfærd derhjemme vs. på arbejdet: En del af informanterne ved simpelthen ikke, om det password, de bruger på arbejdet, er sikkert eller usikkert – men gennemsnitligt vurderes det som mere sikkert end det, der bruges derhjemme. Derudover er der en udbredt tendens til genbrug af passwords, som – forventeligt – stiger, des flere passwords, man har.

3.5.3 Brugertests

Brugertestene viste, at rådet om at bruge en password manager ikke er det mest hensigtsmæssige. En del brugere tolkede ordet i sig selv som værende en person på arbejdspladsen, som holder styr på ens passwords. Yderligere var der en del skepsis omkring at lade et program konstruere sine passwords og holde styr på dem. En stor del af respondenterne udtalte, at de ville være bange for at bruge sådan et program, da det vel i princippet også kan hackes af de it-kriminelle.

Fase	Borgere	It-Ansvarlige	Medarbejdere
1. Research	Umuligt at huske og konstruere	Umuligt at få medarbejdere til at huske og konstruere	Umuligt at huske og konstruere, ”ikke mit ansvar”
2. Survey	Vi genbruger, men oplever det ikke som et problem	-	Vi genbruger, men oplever det ikke som et problem
3. Brugertests (brug en password manager)	**18-39 år:** Har relativt mange passwords, og ved ikke, hvilket der er vigtigst at holde unikt. **60+ år:** Har relativt få passwords, og har mest brug for en sikker måde at konstruere og opbevare dem på. **Begyndere:** Det er godt nok smart! Hvad er det? **Rutinerede:** Det er smart, men er det sikkert? **Eksperter:** Hvilken én skal jeg bruge?	**Større vh.:** Vi kan ikke bruge en password manager. **Mindre vh.:** Vi kan godt bruge en password manager – men det kræver en anbefaling fra ERST.	**Større vh.:** Vi har brug for hjælp med at huske passwords og konstruere nye **Mindre vh.:** Det lyder usikkert med kun ét password – men det kræver en anbefaling fra it-ansvarlig.

3.5.4 Opsummering: Fra ”enten-eller” til trinvist mere sikre password

Generel anbefaling: Eftersom rådet om at bruge en password manager ikke umiddelbart fungerer efter hensigten anbefaler vi i stedet at dele råd om password-adfærd op i mindre dele.

1. Brug ikke det samme password på flere platforme, f.eks. privat og på arbejde.
2. Få gode råd til at lave et sikkert password her.
3. Brug en password manager. Se vores forslag til gode programmer her.

Rådene om password-adfærd ændres dermed fra at være: enten har du et sikkert password (til ALLE dine logins) eller også har du ikke, til at være en trinvis anbefaling mod mere og mere sikker adfærd efter ens tekniske kompetencer.

Ligesom med antivirus er markedet for password-managers dog uoverskueligt for langt de fleste at navigere i. Det er en nødvendighed at snævre mulighedsrummet lidt ind, måske endda etablere et partnerskab med henblik på at anbefale én bestemt passwordmanager, eller udvikle en i forbindelse med et offentligt hackathon elller lignende.

Unge har relativt flere passwords end ældre, og derfor ligger der en klar anbefaling i at gøre det mere tydeligt for dem, hvilket password der er det vigtigste at holde unikt. Her kunne rådet om to faktor-autentifikation bringes i anvendelse, idet det er relativt enkelt at sætte op på facebook og Google, som sandsynligvis er de væsentligste indgange til mange unges digitale liv.

De ældre har derimod mere brug for sikre måder at konstruere og opbevare passwords sikkert på. Brugertestene viste dertil, at de ældre var mest trygge ved fysisk opbevaring af deres passwords. Her kunne en digital password-generator hjælpe med konstruktionen, mens opbevaringen kunne klares med manuel nedskrivning i en helt almindelig notesbog.

3.6 Indtaster personlige oplysninger på usikre hjemmesider

3.6.1 Research

Ifølge Christian Jæhger er der altid – selv i det mest sikre it-system – en bruger bagved skærmen, som opfører sig usikkert. At danskerne besøger på usikre hjemmesider, er ikke i sig selv et problem. Det bliver det først, når den enkelte indtaster personfølsomme oplysninger på den usikre hjemmeside. Eksperterne er enige om, at danskerne gør netop dette uden at vide, at det kan kompromittere deres sikkerhed.

Det er derfor et af de adfærdsmønstre, som har størst konsekvenser både for den enkelte og for samfundets informationssikkerhed. Det er imidlertid samtidig et adfærdsmønster, som er vanskeligt at ændre, da det vil kræve en meget konkret handleregel for, hvad der gør en hjemmeside ”usikker” – og ikke mindst, hvad det konkret betyder. Danskerne mangler *både* en heuristik for at vurdere sikkerheden af en hjemmeside, og de mangler en generel forståelse af, hvad ”usikker” indebærer. Dette adfærdsmønster er altså valgt på trods af, at det umiddelbart er vanskeligt at ændre på, men netop fordi det udgør et meget centralt problem, bør indsatser som denne søge at ændre det.

Eksperter, der fremhæver adfærdsmønsteret: Anders Kjærulf, Angela Sasse, Kim Aarenstrup, Rasmus Theede.

3.6.2 Survey

Resultaterne fra spørgeskemaet viser tydeligt, at usikre hjemmesider bliver set som en forholdsvis ofte forekommende trussel inden for it-kriminalitet:

Vi undersøgte også danskernes forståelse af de mest populære browseres visualiseringer af sikre og usikre hjemmesider. Vi gav dem hver især ét af fire browservinduer, som alle viste den samme hjemmeside (en generisk handelshjemmeside med en iPhone). Som det fremgår af grafen herunder, er det helt tydelige visuelle cues, der gør en forskel for danskernes oplevede tryghed ved at indtaste personlige oplysninger på en hjemmeside.

3.6.3 Brugertests

Rådet om at bruge en browser, som angiver sikre og usikre hjemmesider vha. visuelle cues, viste sig at være for generisk til at påvirke målgrupperne. ”Begynderne” kender ikke til ordet browser, de rutinerede kan ikke selv afkode, hvilke browsere, der er tale om, og eksperterne bruger ofte forskellige browsere i forskellige sammenhænge.

Fase	Borgere	It-Ansvarlige	Medarbejdere
1. Research	Ved ikke, hvad en usikker hjemmeside er, og hvad det betyder for risiko	-	Ved ikke, hvad en usikker hjemmeside er, og hvad det betyder for risiko
2. Survey	Visuelle cues forbedrer risikovurdering	-	Visuelle cues forbedrer risikovurdering
3. Brugertests (brug en browser med visuelle cues)	**Begyndere (alle aldre):** Hvad er en browser? **Rutinerede (alle aldre):** Hvilken browser er det? **Eksperter (alle aldre):** Jeg bruger flere forskellige, så rådet giver ikke mening for mig.	**Større vh.:** Vi bruger flere forskellige browsere, men vi kan bruge info om visuelle cues til at uddanne medarbejderne. **Mindre vh.:** Hvilken browser er det? Vi kan bruge info om visuelle cues til at uddanne medarbejderne.	**Større vh.:** Vi bestemmer ikke selv browser. Hvad skal vi kigge efter i browservinduet? **Mindre vh.:** Hvilken browser er det, og hvad skal vi kigge efter i browservinduet?

3.6.4 Opsummering: Visuel feedback gør det lettere at afkode usikre hjemmesider

Anbefaling: Browsere med visuelle cues er effektive, men indsatsen bør gå skridtet videre og fortælle, *hvilken* browser man skal bruge, og *hvor* man skal kigge efter de visuelle cues.

Visuelle cues er eksempelvis en grøn farve med teksten ”Sikker”, som står i adressefeltet i browservinduet, når den aktuelle hjemmeside er sikker. Tilsvarende kan usikre hjemmesider angives med rød farve og teksten ”Usikker”. På den måde gør man det nemmere for den enkelte at orientere sig hurtigt og uden at bruge al for mange kognitive kræfter, hvilket man f.eks. ville gøre, hvis man altid skulle kigge efter ”httpS” for at være sikker. Farver, symboler og tydelig tekst fremmer forståelsen. Google Chrome har dette som standard, men øvrige browsere kan få det gennem såkaldte add-ons, dvs. overvejende gratis tilføjelsesprogrammer.

3.7 Åbner Indhold i E-mail fra Ukendt Afsender

3.7.1 Research

Som ovenstående er dette adfærdsmønstre et af de mest centrale, fordi det både for den enkelte og for samfundet involverer enorme omkostninger. Men adfærdsmønsteret er samtidig også blandt de vanskeligste at ændre på, fordi angrebene (phishing, ransomware osv.) bliver mere og mere sofistikerede.

Angela Sasse pointerer, at det er umuligt at forestille sig, at borgere såvel som medarbejdere vil kunne klare sig uden at sende links i e-mails. Det er faktisk blevet så integreret del af vores digitale kommunikation, at det vil forstyrre uhensigtsmæssigt meget, hvis danskerne skal foretage grundige tjek af alt indhold i samtlige e-mails, de modtager. Der er altså brug for simple handleregler og dertil positiv feedback, som fortæller folk, når de har handlet i overensstemmelse med anbefalingen.

Oz Alashe mener, at den bedste handleregel i forhold til at opdage phishing og lignende ondartede e-mails er at kigge på afsenderens adresse. Barclays direktør blev eksempelvis offer for spearphishing afsendt fra adressen ”john.mcfarlane.barclays@gmail”, hvilket illustrerer, at hvem som helst kan falde for disse angreb. Oz Alashe vurderer dog, at 80 procent af al phishing kan undgås, hvis bare man tjekker afsenderens adresse og links i e-mailen.

Det er altså med simpel adfærd muligt at forhindre en stor del af konsekvenserne ved dette meget alvorlige problem. Derfor er dette adfærdsmønster udvalgt.

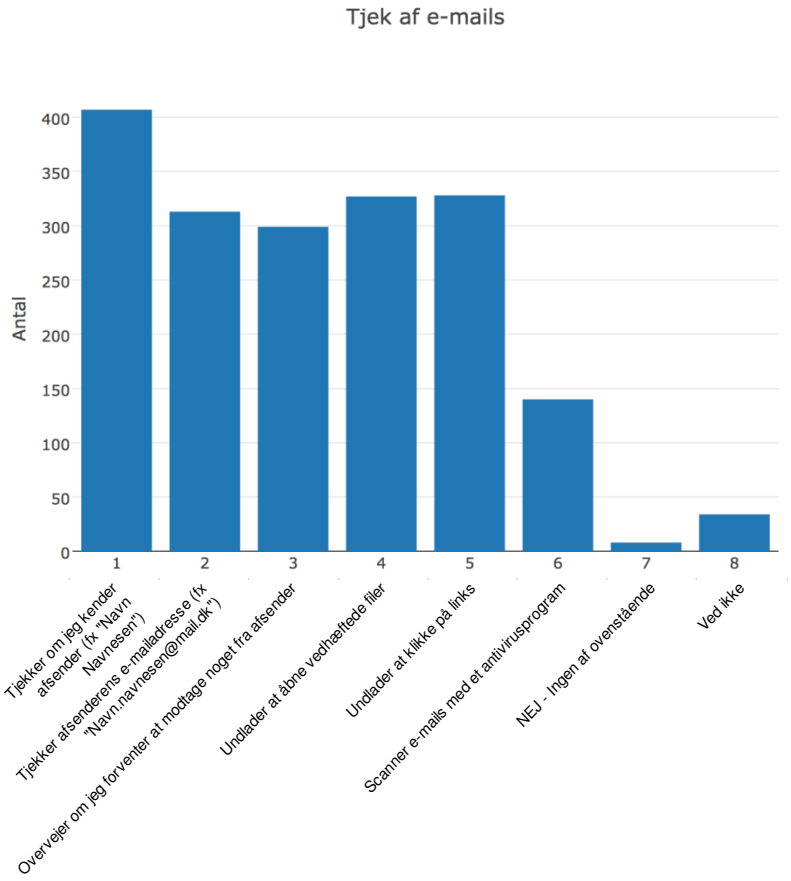
Eksperter, der fremhæver adfærdsmønsteret: Anders Kjærulf, Angela Sasse, Christian Jæhger, Jan Kaastrup.

3.7.2 Survey

Spørgeskemaet viste, at respondenterne i den grad er klar over, at phishing-mails udgør en stor fare for den digitale sikkerhed:

Respondenterne svarede yderligere, at de tager en række forholdsregler for at undgå at blive offer for phishing:

Figur 3.2: ”Hvad gør du for at sikre dig, når du modtager en e-mail?”



Der er dog en uhensigtsmæssig forskel mellem de angivne forholdsregler, da tjek af afsenderens navn, som ikke er en god forholdsregel, rangerer højere end tjek af afsenderens e-mailadresse.

Dermed viser disse resultater, at respondenterne ikke er enstemmigt klar over, hvad der er det meste effektive at gøre for at undgå phishing.

3.7.3 Brugertests

Brugertestene validerede yderligere pointen, da flere respondenter udtalte, at de godt ved, at de skal kigge efter en e-mailadresse, som ser "forkert" ud. Men de ved ikke, *hvordan* en "forkert" e-mailadresse ser ud.

Fase	Borgere	IT-Ansvarlige	Medarbejdere
1. Research	Uopmærksomhed, psykologisk kompetente hackere	-	Uopmærksomhed, psykologisk kompetente hackere
2. Survey	Vi oplever det som meget vigtigt, men mangler konkret handleregel	-	Vi oplever det som meget vigtigt, men mangler konkret handleregel
3. Brugertests (råd til at undgå phishing)	**Begyndere og rutinerede (alle aldre):** @-rådet er godt. **Eksperter (alle aldre):** Der skal lidt mere kompleksitet til. **De yngste:** Brug facebook-messenger som eksempel i stedet for SMS.	**Mindre vh.:** Rådet om at udskrive den seneste alvorlige phishing-mail er godt. **Større vh.:** Vi bruger allerede intranet til oplysning om seneste trusler. Mere fokus på ransomware og CEO-fraud.	**Mindre vh.:** @-rådet er godt, men skal eksemplificeres. NemID og personlige oplysninger er for privat til arbejdspladsen. **Større vh.:** Vi har godt styr på adresser, links og personlige oplysninger, men vi er mindre kritiske over for interne mails.

Dermed blev pointen om, at jo mere konkret et råd er, jo nemmere er det at følge.

3.7.4 Opsummering: Kig efter det, der står efter @'et

Anbefaling: Bryd tjek af e-mails ned i mindre trin og start med det meste effektive råd.

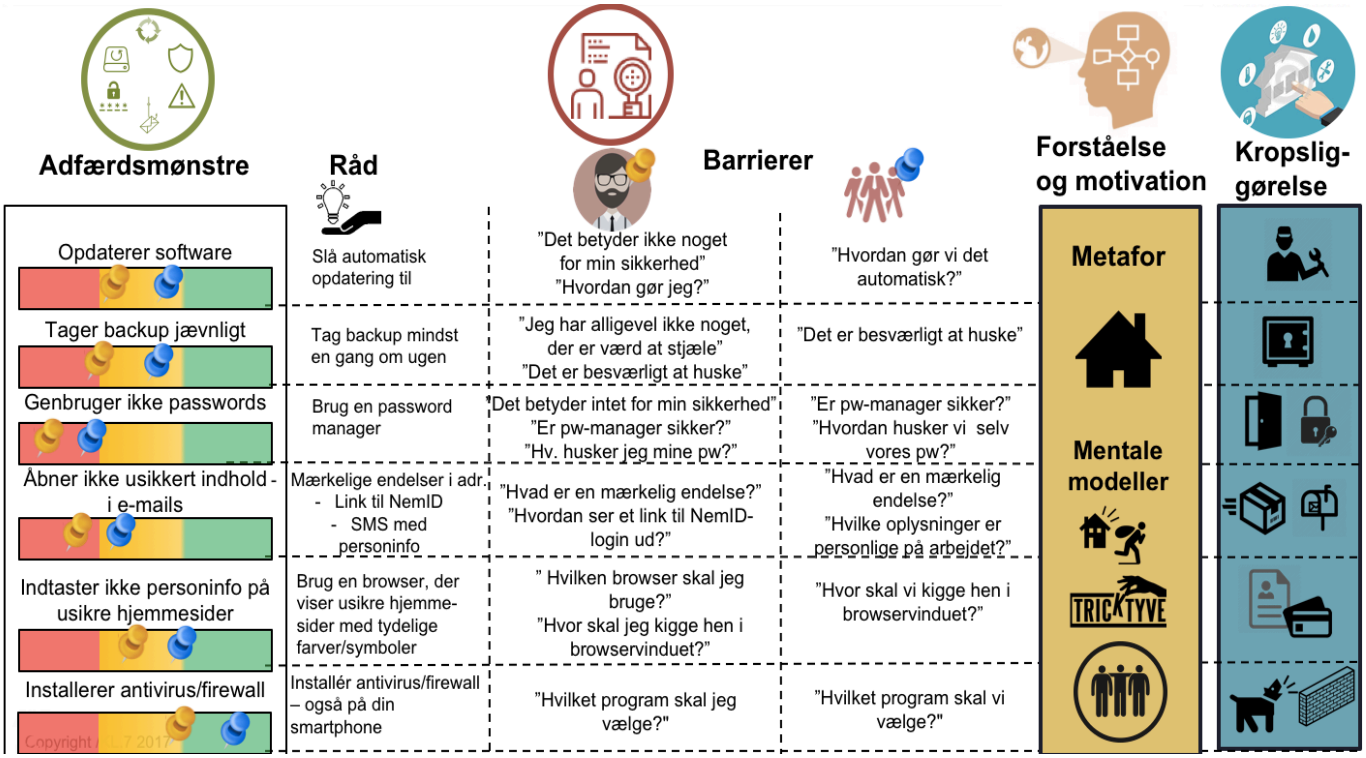
1. Undersøg det, der står efter @'et. Har du set det før?
2. Kender du afsenderen? Forventer du at modtage en e-mail fra afsender på dette tidspunkt og på denne dag?

Til it-ansvarlige: Offentliggør phishing-mails løbende på f.eks. virksomhedens intranet, så medarbejderne kan se, hvad de skal være opmærksomme på.

4.0 Overordnede Anbefalinger til Kampagnen

I dette kapitel gennemgås de overordnede kampagneanbefalinger, og hvordan de er rodfæstet i indsigter fra projekets tidligere faser. Figur 4.1 nedenfor viser en oversigt over adfærdsmønstre, råd, barrierer samt vores anbefalinger til forståelse og motivation samt kropsliggørelse.

Figur 4.1



Under **Adfærdsmønstre** ses hvert enkelt adfærdsmønster med en angivelse af, hvor tæt borgerne (den gule nål) og medarbejderne (den blå nål) er på at udføre den. Angivelsen er baseret på brugertestene i Fase 3. Det røde felt er "langt fra at have adfærden", det gule felt er "hverken langt fra eller tæt på", og det grønne felt er "tæt på". Det fremgår derfor tydeligt, hvilke adfærdsmønstre, som borgerne/medarbejderne er langt fra at udføre, og hvilke de er tættere på. Værst står det til med "Genbruger ikke passwords", mens både borgere og medarbejdere er så godt som i mål med "Installerer antivirus/firewall". På nær sidstnævnte er alle udvalgte adfærdsmønstre placeret af eksperterne under "Store konsekvenser" (se figur 2.1). Der er derfor antageligvis ca. lige store gevinster at høste på samfundsniveau ved at nå i mål med de seks adfærdsmønstre. Det betyder, at den væsentligste faktor i prioriteringen af dem bør være, hvor langt der er til korrekt udførelse af adfærden.

Under **Råd** er de konkrete handlingsanvisninger, borgerne og medarbejderne fik i materialet til brugertesten.

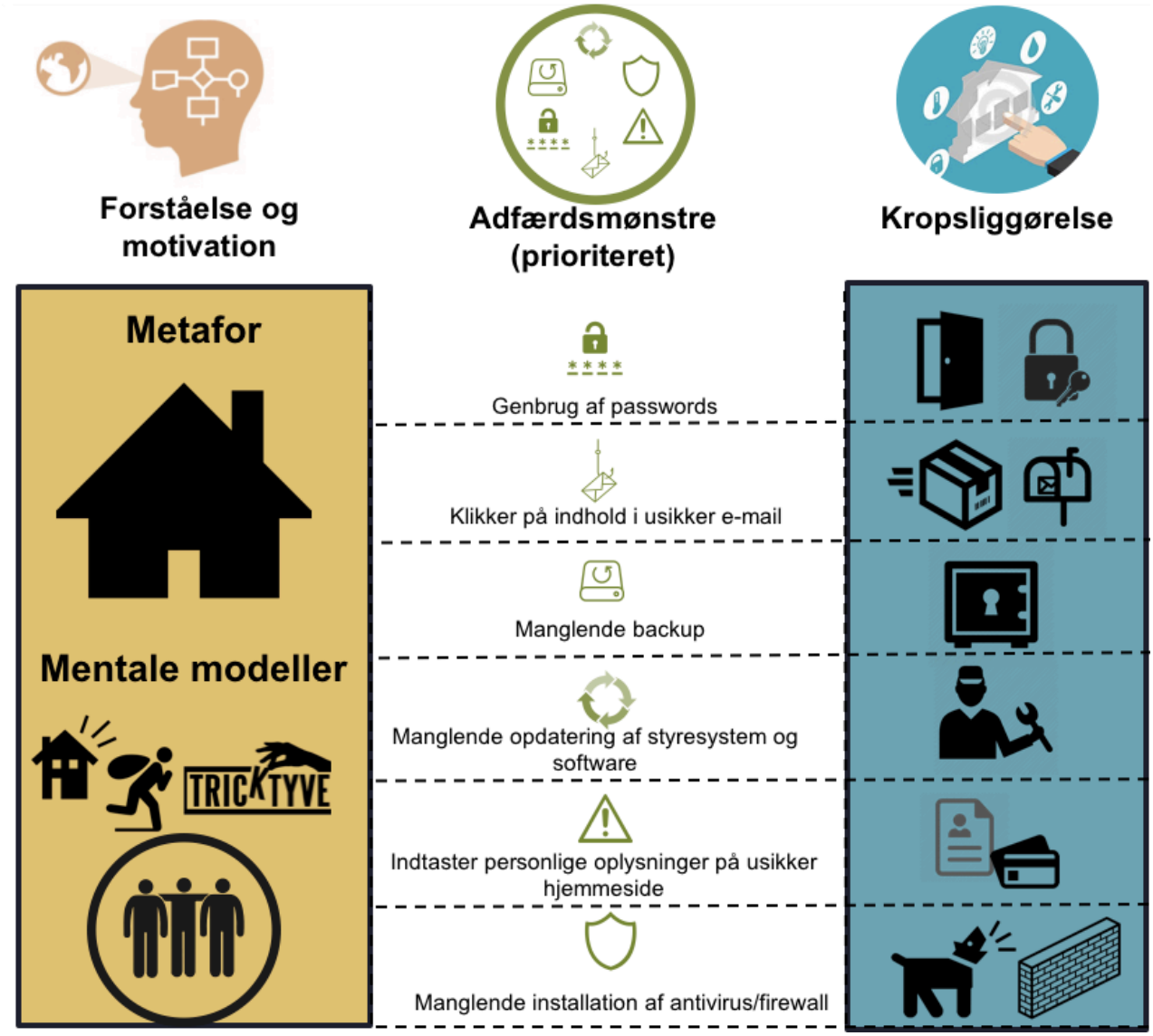
Under **Barriere**r findes de konkrete problemstillinger, som hhv. borgerne og medarbejderne udtrykte over for de konkrete råd. Her fremgår det f.eks., at borgerne ønsker en udspecificering af, hvad en "mærkelig endelse" er, i rådet til at imødegå åbning af usikkert indhold i e-mail.

Under **Forståelse og motivation** ses vores anbefalinger til, hvordan fremtidige kampagneindsatser bør kommunikere om it-sikkerhed for at øge forståelse af problemstillingen og motivationen for at handle. Vi anbefaler at bruge 'hjemmet' som overordnet metafor samt at italesætte de it-kriminelle som tricktyve/svindlere og ofrene som os alle sammen.

Under **Kropsliggørelse** ses den række konkrete måder, vi anbefaler at bruge metaforen 'hjemmet' aktivt for at understøtte forståelsen af vigtigheden ved hvert enkelt adfærdsmønster og gøre det mere overskueligt at handle. Ud over at det giver en mere sammenhængende kommunikation at tage udgangspunkt i den samme metaforiske verden, så har kropsliggørelsen også en adfærdsmæssig funktion: Når en problemstilling bliver gjort fysisk og håndgribeligt, så opleves det nemmere at handle på den, end hvis den var abstrakt. Når man så at sige kan 'se handlingen for sig', er det også mere overskueligt at foretage den. At italesætte passwords som fysiske nøgler gør det både mere forståeligt, hvorfor det er vigtigt at passe på dem, og handlingen bliver mere konkret.

På baggrund af modellen ovenfor har vi herunder i Figur 4.2 prioriteret adfærdsmønstrene, så det, hvor borgere og medarbejdere er længst fra den optimale adfærd, er øverst. Derudover har vi også angivet en række ikonografiske eksempler på konkrete måder, vi anbefaler at bringe kropsliggørelsen af adfærdsmønstrene i spil inden for den metaforiske verden 'hjemmet'. Det skal ses som en opsamling på de konkrete anbefalinger til de seks adfærdsmønstre, vi gennemgik i sidste kapitel.

Figur 4.2


Forståelse og motivation
Adfærdsmønstre (prioriteret)
Kropsliggørelse
Metafor
Mentale modeller
TRICKTYVE
Genbrug af passwords
Klikker på indhold i usikker e-mail
Manglende backup
Manglende opdatering af styresystem og software
Indtaster personlige oplysninger på usikker hjemmeside
Manglende installation af antivirus/firewall

I tabel 4.1 herunder er oplistet en række forslag til, hvordan dette kan udmøntes i konkret indhold til indsatsen.

Tabel 4.1

Adfærdsmønster	Element i "hjemmet"	Budskab
Genbrug af passwords	Nøgler/låse/døre	• "Hvis du genbruger dit kodeord skal de kriminelle kun franarre dig det én gang for at få adgang til alle dine døre." • "Du nøjes jo ikke med at *lukke* døren, når du går ud. Husk at låse forsvarligt." • "Du ville heller ikke lægge dine nøgler ude på vejen.
Åbne indhold i e-mails fra ukendt afsender	Pakkepost	• "Åbn kun indholdet i en e-mail, hvis du kender afsenderen og afsenderens adresse." • "Send aldrig personlige oplysninger tilbage til nogen – spørg altid først."
Manglende backup	Pengeskab/værdiskab	• "Sikkerhedskopiering er det samme som en gratis forsikring af alle dine digitale værdisager." • "Når du tager backup af dine data, har de ingen værdi for it-kriminelle."
Manglende opdatering	Døre og vinduer	• Gamle døre/vinduer er nemmere at bryde op • "Automatisk opdatering svarer til, at der kommer en låsesmed hjem til dig og sikrer alle dine døre og vinduer ganske gratis."
Indtaster personlige oplysninger på usikre hjemmesider	Pas, dankort, vigtige dokumenter	• "Hvis du indtaster personlige oplysninger på en usikker hjemmeside svarer det til at give den kriminelle dit dankort i hånden."
Manglende antivirus/firewall	Vagthund, murværket	• "Ligesom en vagthund opdager Antivirus/Firewall de kriminelle, før du selv gør – men du er stadig nødt til at sikre dig yderligere, hvis du vil undgå it-kriminalitet" • "Antivirus/Firewall er ligesom murværket på dit hus. Det er virkelig usmart at bo i et hus uden, men for at undgå kriminalitet, er det ikke hele løsningen – det er kun udgangspunktet for en god it-sikkerhed."

4.1 Tjekliste for Kommunikationsmateriale

Vi anbefaler kommende kampagneindsatser at følge tjeklisten nedenfor, når kommunikationsmaterialet udarbejdes. Når der er sat kryds i alle felterne, lever kommunikationen op til de anbefalinger, vi har givet på baggrund af denne for-analyse.

Tabel 4.2

Tjekliste for Kommunikationsmateriale
❑ ”Hjemmet” er blevet brugt som overordnet metafor for it-sikkerhed
❑ It-kriminelle omtales som ”tricktyve”
❑ Offeret for it-kriminalitet er alle danskere (og/eller er italesat på en måde, så den enkelte føler sig som en del af den typiske gruppe af potentielle ofre)
❑ It-kriminalitet skal bekæmpes via ”os-mod-dem”
❑ Der er ikke brugt nogen ekspertudtryk (phishing, browser, osv.)
❑ Rådene er handlingsanvisende og konkrete

4.2 Segmentering af budskaber og kanalvalg

4.2.1 Overordnet

Til borgerne

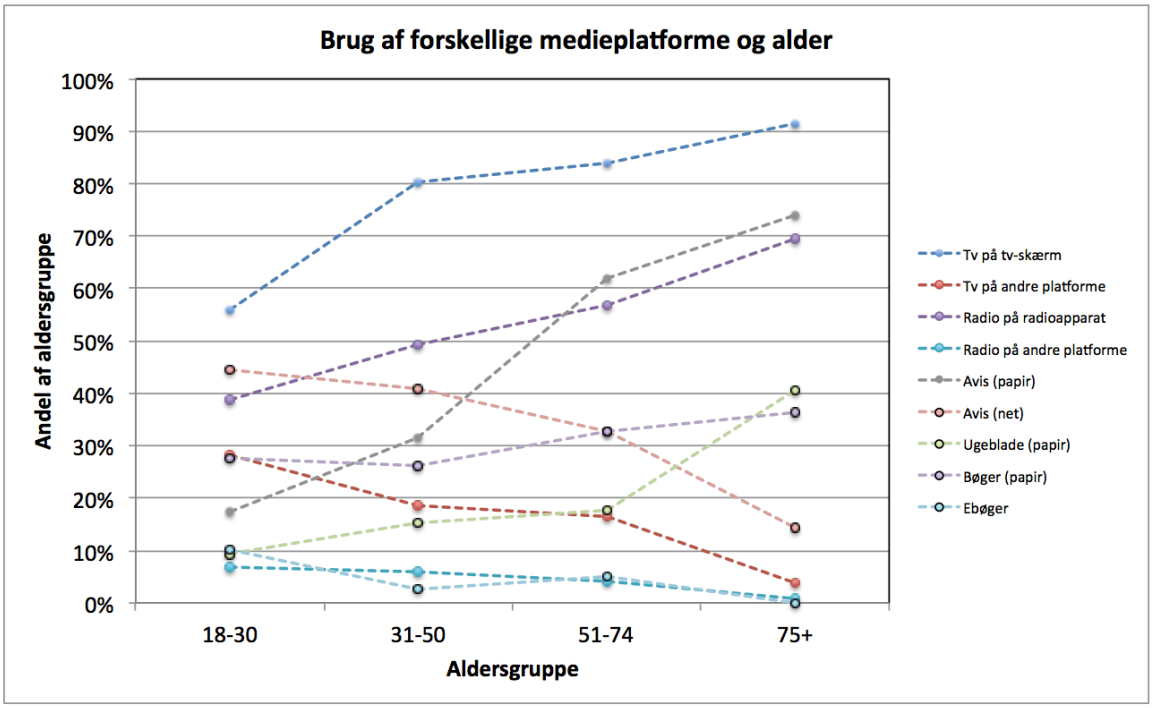
Gentagelse fremmer forståelsen. Jo flere steder, danskerne støder på det samme budskab, des mere vil indholdet alt andet lige også sætte sig i deres bevidsthed. For handleregler gælder det samme: Helt klare, kortfattede anvisninger til en bestemt adfærd skal gentages flere steder på samme måde, hvis man har ambitioner om at opnå en adfærdsændring, som kan måles på befolkningsniveau. Det er også i tråd med den centrale indsigt fra brugertestene i Fase 3, at borgerne har en høj grad af tillid til råd fra Digitaliseringsstyrelsen, og at en bred medietilstedeværelse kun vil være befordrende for denne tillid.

For at opnå maksimal effekt af budskabskommunikationen anbefaler vi derfor, at **en række traditionelle platforme** tages i brug samtidig. Anbefalingen bunder dels i en generel research på danskernes medieforbrug, og dels i resultaterne fra brugertestene, hvor borgerne nævnte nedenstående eksempler, og at de helst så, at kommunikationen blev fordelt ud på flere platforme på én gang. Begge dele bliver udfoldet yderligere i det følgende. **Kanalanbefalingerne går på tværs af alle udvalgte adfærdsmønstre**, idet undersøgelsens omfang ikke tillod en dybere segmentering for hvert enkelt adfærdsmønster. Herunder fremgår de overordnede kanalanbefalinger og (i parentes efter hver anbefaling) det segment, som anbefalingen retter sig til:

-  Fysiske reklamepladser på busstoppesteder (60+ år), billboards (40-59 år) og på papir i landsdækkende aviser (ældre, højtuddannede og eksperter)
-  Videospots til deling på de sociale medier (lavtuddannede, begyndere, 18-39 år)
-  En aktiv facebook-strategi i form af sider, delevenligt content og evt. interaktion med borgere i form af indberetning af nye trusler og/eller gode ideer til at øge it-sikkerheden ift. et konkret adfærdsmønster (18-39 år, rutinerede)
-  En Snapchat-/Instagram-/Youtube-strategi i form af direkte interaktion med danskere om konkrete ting, man kan gøre og være opmærksom på ift. et konkret adfærdsmønster. (den yngste halvdel af 18-39 år)

På de følgende sider uddybes ovenstående i en gennemgang af danskernes medieforbrug med henblik på kanalvalget til segmenteret budskabskommunikation. Herefter gennemgås de enkelte adfærdsmønstre og budskabsanbefalingerne hertil i skemaform. **Kanalanbefalingerne er ens for de respektive segmenter på tværs af adfærdsmønstrene,** hvorfor der ikke vil være en uddybende forklaring af kanalvalget under hvert skema i enkelte adfærdsmønstre. Forklaringen af kanalvalget ligger i dette afsnit. **Ikonerne ovenfor anvendes i skemaerne for hvert adfærdsmønster i de følgende afsnit.**

Figur 4.3

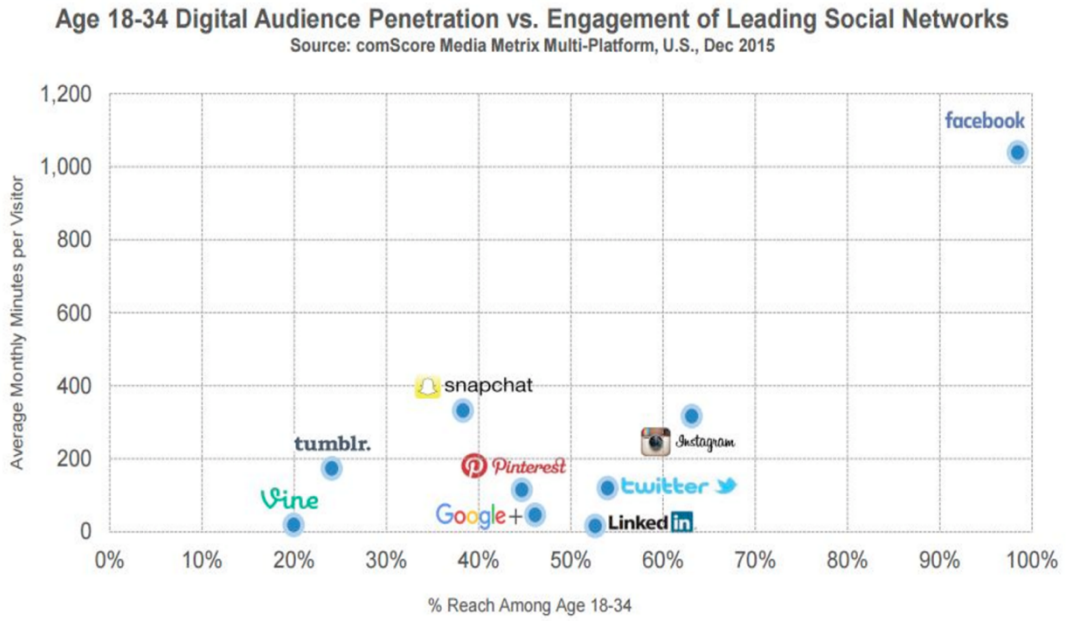


Hentet fra *http://slks.dk/fileadmin/user_upload/dokumenter/medier/Mediernes_udvikling/2015/Specialrapporter/KU_Mediebrug/Danskernes_mediebrug_2014_Rapport.pdf*

Ift. **de helt traditionelle medieplatforme** TV, radio, papiraviser er medietrykket, som Tabel 4.3 ovenfor viser, langt størst hos de ældste befolkningsgrupper. Dette understreger yderligere brugertestenes fund om, at 60+ årige foretrækker at blive kommunikeret med disse budskaber til på fysiske reklamepladser i det offentlige rum og i landsdækkende aviser.

Videospots kan selvsagt kommunikeres gennem TV-reklamer, men som digital formidlingsform er den i kraftig vækst. Det gælder især de mest populære sociale medieplatforme som Facebook, Snapchat og Youtube, som især bæres frem af smartphones globale udbredelse. Cisco estimerer, at 82 procent af al internettrafik vil bestå af videokommunikation i 2020 (Cisco, 2017). Videoer kan skabe mere opmærksomhed og fastholde den i længere tid end tekst og stillbilleder, de kan gøre kompliceret ekspertviden bredt tilgængeligt, og de er frem for alt nærhedsskabende: Alt sammen positive egenskaber, der gør videospots ideelle til budskabskommunikation blandt it-begyndere, yngre og lavtuddannede. Her er det væsentligt at holde for øje, at unge i højere grad ser ud til at være interesserede i et mere råt og håndholdt æstetisk udtryk, mens ældre efterspørger det grundigt gennemarbejdede. Uanset hvad er delevenlige videoer oplagte til at kommunikere gode råd i praksis og netop gøre it-kriminalitet til noget fysisk.

Figur 4.4



Hentet fra http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

Snapchat og Instagram er, som det kan ses i Figur 4.4 ovenfor, blandt de allermest populære digitale sociale netværk blandt unge. Snapchat er bedst til at opbygge relationer med sit relativt spontane og håndholdte udtryk, hvilket især kan udnyttes i budskabskommunikationen, hvis en ung influencer er eksponent for de åbenlyst åndssvage adfærdmønstre, danskerne har på nettet. Instagram henvender sig særligt til yngre kvinder med muligheden for at skabe en klar visuel profil ud fra hverdagslige situationer. Instagram kan bruges til at skabe et særligt æstetisk udtryk for en budskabskommunikation omkring vigtigheden af at holde sig it-sikker, som bæres frem af et særligt hashtag, og som derved opfordrer til yderligere engagement og brugerdrevet indhold.

Til den helt brede budskabskommunikation anbefales det, at man afsøger **mulige partnere** (f.eks. Microsoft DK og YouSee), der både har 1) den fornødne autoritet til at udbrede budskaberne, 2) datagrundlag for viden om danskernes usikre adfærd og 3) mulighed for at indgå i en regulær effektmåling af kampagneindsatsen.

Partnere kunne desuden mobiliseres til et offentligt støttet hackathon med det formål at udarbejde **en fælles offentlig password manager**. Dette ville kunne løse begge centrale udfordringer, der blev mødt i brugertestene i forsøget på at anbefale en password manager til borgerne: ”Hvilken én skal jeg vælge?” og ”er den nu også sikker?”.

Et muligt partnerskab findes også hos ophavsmændene bag den relativt nye mobilapp **”Mit Digitale Selvforsvar”** (bl.a. Rådet for Digital Sikkerhed og TrygFonden), som både viderebringer aktuelle info om it-trusler og konkrete handleregler. Hvis det er muligt at koble kommende kampagneindsatsers kommunikation op på denne app, så der f.eks. kan udsendes push-beskeder med konkrete handlingsanvisninger, er *outreach* potentielt meget stort. Det kan samtidig give værdi til app’en, hvis den adapterer de evidensbaserede, adfærdsvidenskabeligt funderede kommunikationsanbefalinger fra denne for-analyse.

- Brug eksisterende applikationer relateret til it-sikkerhed med stort *outreach* (f.eks. ”Mit Digitale Selvforsvar”, ”TDC MobilSikkerhed”, ”The Next Gov iOS Safety”) (højtuddannede, eksperter, midaldrende). **Dette ikon refererer (i lighed med kanalikonerne ovenfor) til denne kanal i skemaerne over budskaber, segmenter og kanaler for hvert adfærdsmønster.**

Eksisterende infrastruktur ift. kommunikation fra offentlig myndighed til borger er en anden stærk kanal. Vi anbefaler helt konkret at anvende **fremsendelse af nyt NemID** til borgeren til budskabskommunikation. Her kunne man både vedlægge et ark med budskaberne kuverten og/eller påsætte centrale budskaber på selve nøglekortet. Især sidstnævnte vil være meget effektfuldt, fordi danskerne har nøglekortet fremme ofte i deres dagligdag, og fordi NemID i forvejen er en passwordsikring i sig selv. Faktisk kommunikeres der allerede it-sikkerhed på nøglekortet i form af ”Tag ikke billeder af dit NemID”-ikonet.

Mere uformelt viser vores brugertest, at mindre it-kyndige borgere konsulterer deres mere it-kyndige venner/familiemedlemmer for råd og vejledning om it-sikkerhed. Denne indsigt kunne bringes i anvendelse i form af **kommunikation rettet specifikt til de mere it-kyndige borgere om at tage sig af deres mindre it-kyndige venner/familie** med konkrete handleregler. På den måde ville it-kyndige borgere udfylde en rolle ikke ulig den, vi lægger op til, at de it-ansvarlige skal udfylde. Brugertestene viste, at de mest it-kyndige borgere påfaldende ofte refererede til app’en ”Mit Digitale Selvforsvar”. Denne app er derfor en oplagt kanal at nå dette segment igennem. Det kunne blandt andet gøres med en udvidelse af app’ens pushbesked-funktion, så den også gav gode råd/tips til 1) Mere komplekse handleregler til at imødegå trick-mails, og 2) hvordan man bedst hjælper sine mindre it-kyndige venner/familiemedlemmer til at blive mere sikre.

Til medarbejderne

Den helt centrale forskel mellem de mange forskellige virksomheder, vi foretog brugertest hos, ligger i antallet af ansatte. Større virksomheder (dvs. med over 35 ansatte) har en fundamentalt anderledes måde at kommunikere med medarbejderne på end mindre virksomheder. Ikke overraskende handler det primært om graden af formalisering:

- Større virksomheder er mere formelle og skriftlige
- Mindre virksomheder er mere uformelle og mundtlige

For **større virksomheder** vil det fungere godt at iværksætte en bredere intern kampagneindsats med:

- Rollups
- Phishing-/ransomware-eksperimenter
- Digital kommunikation med videoer/tegnefilm og quizzer

Her ville vi anbefale (som vi også anbefalede til borgerne), at de samme få budskaber kommunikeres på en flerhed af platforme, fysiske såvel som digitale. Især er det vigtigt at få den fysiske personlige henvendelse med, fordi den ofte går tabt i større virksomheders interne kommunikation om it-sikkerhed.

Det samme ville ikke gå i **mindre virksomheder**. Her er der derimod et større behov for:

- Dialogværktøjer til interne fællesmøder/workshops
- En mere struktureret tilgang til nye medarbejderes indføring i virksomhedens sikkerhedskultur.

Nye medarbejdere er et fokuspunkt for alle virksomheder. De skal læres op i virksomhedens mere eller mindre uformelle sikkerhedskultur, og her kan budskabskommunikationen spille en væsentlig rolle for virksomhedsledelsen og it-afdelingen ift. at klæde den nye medarbejder bedst muligt på til at agere sikkert digitalt.

Til it-ansvarlige

Fælles for alle slags virksomheder er også, at **de it-ansvarlige er en oplagt budskabskanal.** Det gælder både ift. sikker digital adfærd på arbejdet og derhjemme. De it-ansvarlige har nemlig en høj stjerne blandt de brugertestede medarbejdere, hvilket måske kan skyldes den senere tids megen mediefokus på cyberangreb på virksomheder.

Vi anbefaler derfor at udarbejde et **kit til it-ansvarlige.** Brugertestene viste, at de it-ansvarlige er positivt stemte over for denne idé. Kittet kunne med fordel udformes som en fysisk førstehjælpskasse med 1) en tjekliste til, hvordan den it-ansvarlige får styr på den tekniske del af virksomhedens sikkerhed (primært relevant for mindre virksomheder), 2) tjekliste med formidlingstricks til at få styr på kollegernes it-sikkerhedsadfærd, 3) En guide til at hjælpe kollegaerne til at fortsat at holde styr på deres it-sikkerhedsadfærd, når de kommer hjem, og 4) En mulighed for at skrive sig op til løbende opdatering på ny viden om it-sikkerhed og adfærd fra ERST og DIGST.

I det følgende gennemgår vi i skemaform hvert enkelt adfærdsmønster. Skemaerne indeholder anbefalinger til kanaler og segmentering for både borgere og medarbejdere. Kanalerne er ens for virksomhederne hele vejen igennem alle adfærdsmønstrene. Det skyldes, at vi ikke pba brugertestene kunne lave så finkornede anbefalinger. Kanalanbefalingerne til borgerne anvender ikonografien fra forrige side om overordnede anbefalinger til borgerne.

4.2.2 Genbrug af passwords

Kropsliggørelse: Nøgler / Låse / Døre

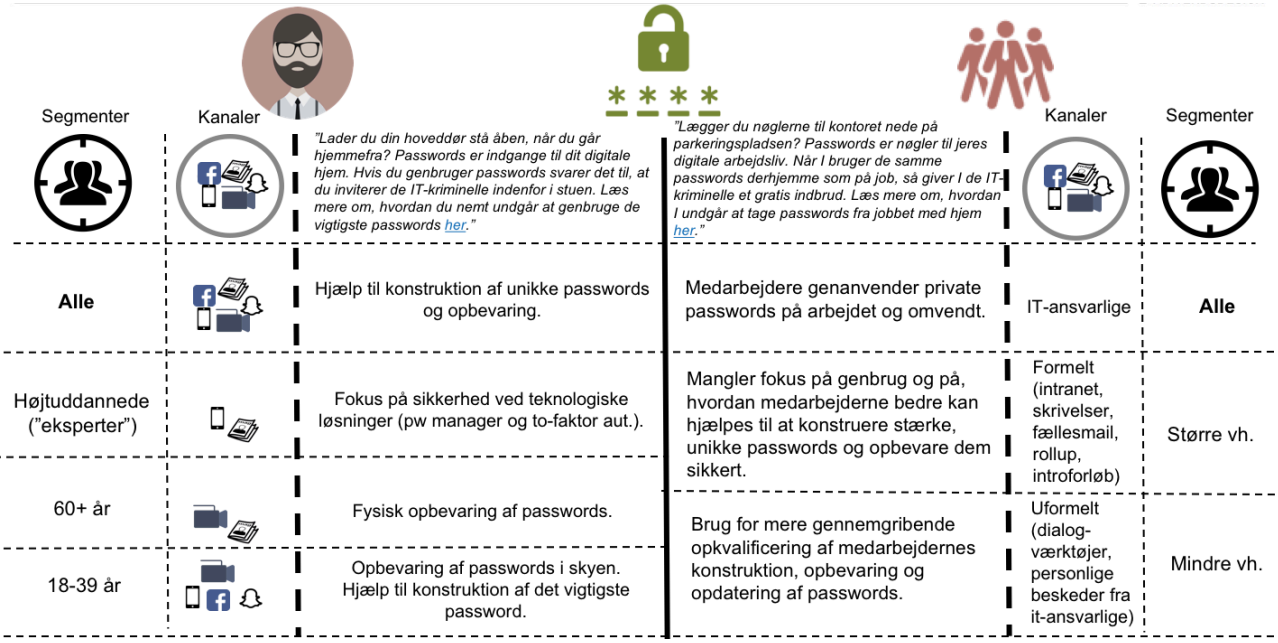
At imødegå danskernes genbrug af passwords kræver både, at de hjælpes til konstruktion af unikke passwords og til sikker opbevaring af dem.
Det gælder for borgerne generelt, men det gælder i lige så høj grad også medarbejdere, idet de ofte genanvender private passwords på arbejdet og omvendt. Denne gensidige udveksling er potentielt kompromitterende for både medarbejderens egen private og virksomhedens sikkerhed. Her gælder især, at større virksomheder har mindre fokus på medarbejdernes genbrug, og at de i mindre grad hjælper medarbejderne med at opbevare deres passwords sikkert. I de mindre virksomheder er problemet mere grundlæggende, idet der er mindre central styring med medarbejdernes passwordkonstruktion. Her har medarbejderne således i højere grad behov for en gennemgribende opkvalificering af deres password-kompetencer: Både ift. tilfredsstillende konstruktion, sikker opbevaring og jævnlig opdatering.

Blandt borgerne danner der sig to centrale segmenteringer: Uddannelse/teknologikyndighed og alder. Højtuddannede ønsker mere klar argumentation for, at teknologiske løsninger som to-faktor login og password manager er sikrere løsninger, før de ønsker at tage dem i brug. Ellers udtrykker de faktisk ønske om en teknologisk løsning på password-problemet.

De ældre (60+ år) er relativt skeptiske overfor især password manager-teknologien og ved opbevaring af passwords i skyen. I stedet efterspørger de råd og vejledning til, hvordan passwords kan gemmes fysisk på en sikker måde.

De unge (18-39 år) er mere trygge ved opbevaring af passwords i en password manager, selvom der skal argumenteres klart for, at det er en sikker løsning. Problemstillingen for denne gruppe er især, at de har relativt mange passwords. Det vurderes derfor, at den centrale udfordring for dem er at finde frem til, hvilket password der er det allervigtigste ikke at genbruge. Hvis man starter i det små med et enkelt password, er sandsynligheden større for, at de unge faktisk vil handle på råd om at undgå genbrug af passwords. Her kunne man som tidligere nævnt også inkorporere to-faktor login, da det er en funktion, som er relativt enkel at sætte op på de allermest centrale digitale platforme (f.eks. Google og Facebook).

Figur 4.5: Genbrug af Passwords


Segmenter
Kanaler
"Lader du din hoveddør stå åben, når du går hjemmefra? Passwords er indgange til dit digitale hjem. Hvis du genbruger passwords svarer det til, at du inviterer de IT-kriminelle indenfor i stuen. Læs mere om, hvordan du nemt undgår at genbruge de vigtigste passwords her."
"Lægger du nøglerne til kontoret nede på parkeringspladsen? Passwords er nøgler til jeres digitale arbejdsliv. Når I bruger de samme passwords derhjemme som på job, så giver I de IT-kriminelle et gratis indbrud. Læs mere om, hvordan I undgår at tage passwords fra jobbet med hjem her."
Kanaler
Segmenter
Alle
Hjælp til konstruktion af unikke passwords og opbevaring.
Medarbejdere genanvender private passwords på arbejdet og omvendt.
IT-ansvarlige
Alle
Højtuddannede ("eksperter")
Fokus på sikkerhed ved teknologiske løsninger (pw manager og to-faktor aut.).
Mangler fokus på genbrug og på, hvordan medarbejderne bedre kan hjælpes til at konstruere stærke, unikke passwords og opbevare dem sikkert.
Formelt (intranet, skrivelser, fællesmail, rollup, introforløb)
Større vh.
60+ år
Fysisk opbevaring af passwords.
Brug for mere gennemgribende opkvalificering af medarbejdernes konstruktion, opbevaring og opdatering af passwords.
Uformelt (dialog-værktøjer, personlige beskeder fra it-ansvarlige)
Mindre vh.
18-39 år
Opbevaring af passwords i skyen. Hjælp til konstruktion af det vigtigste password.

4.2.3 Klikker på indhold i usikre e-mails

Kropsliggørelse: Pakkepost

Der er overordnet højt fokus på problemstillingen omkring usikre e-mails – både hos borgere og medarbejdere. Dog er det et generelt kommunikationsråd, at der til borgerne ikke skal bruges ordet 'phishing'. I stedet skal det italesættes som f.eks. trick-mails i overensstemmelse med kropsliggørelsen af rådene og den anbefalede mentale model for it-kriminelle som tricktyve/svindlere.

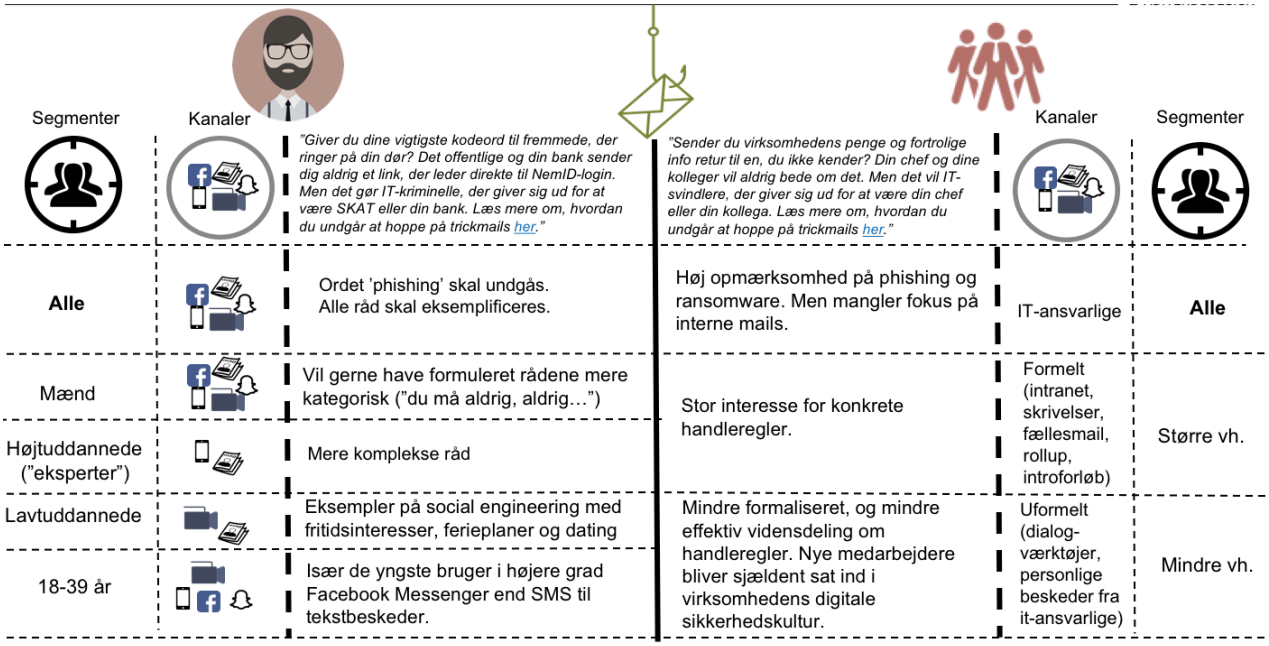
Blandt borgerne er der tre centrale segmenteringer: Køn, uddannelse/teknologikyndighed og alder. Mænd vil generelt gerne have formuleret rådene mere utvetydigt end kvinder. Højtuddannede (især den relativt høje andel af dem, der er "eksperter") efterspørger mere kompleksitet i de angivne handleregler. De skal f.eks. ikke fortælles, at de skal orientere sig ift., hvad der står efter afsenderadressens @. Det gør, at de føler sig talt ned til. I stedet efterspørger de råd, der bringer dem videre. Det kunne f.eks. være, hvordan man tjekker, at IP- og domænenavn stemmer overens med afsendernavn og –adresse. I Google Mail gøres dette relativt simpelt ved et tryk på den nedadvendte pil lige ved siden af afsenderadressen. Står der er det samme under IP og domæne som afsenderen foregiver (f.eks. et domæne fra Danske Bank), er man så godt som sikker på, at det er en oprigtig e-mail (fra f.eks. Danske Bank).

Flere lavtuddannede fortæller, hvordan de er blevet snydt gennem social engineering. Det være sig blandt andet henvendelser fra udenlandske kvinder, som foregiver at ønske romantisk/erotisk kontakt med vedkommende, men som i virkeligheden ønsker vedkommendes penge. Det samme med falske tilbud på rejser og andre forbrugsgoder. Det er derfor væsentligt for dette segment at adressere måder, hvorpå man kan undgå at blive offer for it-kriminalitet, som anvender social engineering.

Et af rådene ift. trick-mails gik på SMS: Nemlig, at det offentlige og banker aldrig vil bede én om at sende personlige info retur i en SMS. For de yngste (dvs. primært under 25 år) bør dette råd imidlertid snarere gå på Facebook Messenger. I så fald bør rådet mere handle om aldrig at besvare personlige henvendelser fra personer, man ikke kender, end om kommunikation med det offentlige og banker.

Fokus på phishing og ransomware er meget højt blandt alle de virksomheder, der indgik i brugertestene. Dog var der – selv i de større og mere formaliserede virksomheder – påfaldende lidt bevidsthed om, at interne e-mails også udgør en potentiel vej ind for it-kriminelle. Det er især det, der er tilfældet med det ofte omtalte fænomen CEO-fraud. Især større virksomheder mangler handleregler til at imødegå dette. De mindre virksomheder mangler i højere grad hjælp til at introducere nyansatte til virksomhedens sikkerhedskultur og konkrete handleregler.

Figur 4.6: Klikker på indhold i usikre e-mails



4.2.4 Manglende Backup

Kropsliggørelse: Værdiskab

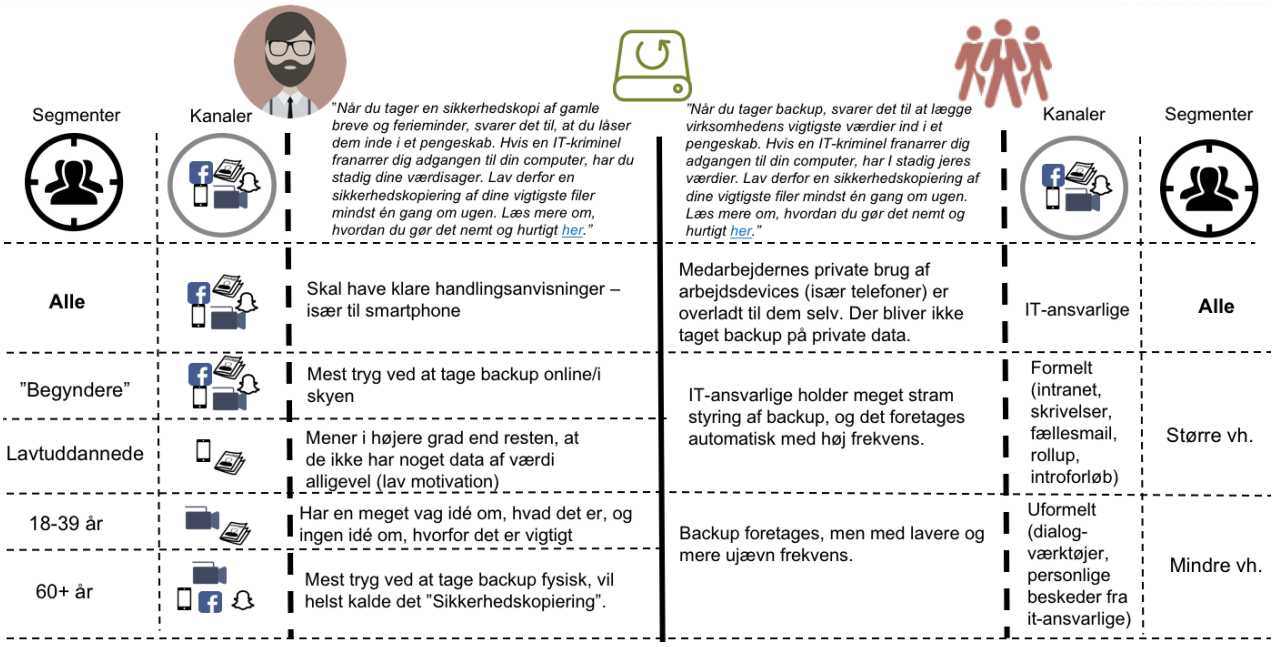
I forhold til manglende backup er der igen et signifikant overlap mellem borgere og medarbejdere, idet medarbejdere i høj grad bruger deres arbejdscomputer/-telefon til private gøremål. Der er derfor meget privat data lagret på enheder, som ellers er tilvejebragt fra arbejdspladsen. I mindre virksomheder er der desuden den problemstilling, at backup ikke er systematiseret og derfor tages sjældent og med ujævne mellemrum. Til sidstnævnte skal der således kommunikeres klart på vigtigheden af at gøre backup til en ugentlig/daglig vane, og hvordan det gøres helt konkret på den mindst indgribende måde.

Borgerne skal generelt have helt klare handlingsanvisninger til, hvordan man tager backup. Det gælder især smartphonen, som næsten ingen i brugertestene angiver, at de tænker over, at man bør tage backup af. Unge (18-39 år) vil helst have handleregler til, hvordan man nemmest tager backup i skyen, mens de ældre ønsker hjælp til at tage "sikkerhedskopier" fysisk, f.eks. på en ekstern harddisk.

Herunder er der dog også en subgruppe af begyndere, som slet ikke ved, hvad backup vil sige, og hvad det skal gøre godt for. Denne gruppe skal i højere grad fortælles om fordelene ved at tage backup, og hvad det overhovedet er. Her kan kropsliggørelsen af backup som et værdiskab vise sig meget værdifuld i budskabskommunikationen.

Dertil er der en udfordring i forhold til de lavtuddannede, som i videre udstrækning end de øvrige borgere i brugertesten angiver, at de ikke har noget data af værdi. Denne gruppe skal kommunikeres til på en måde, der gør dem bevidste om, at alle har noget, der er værd at stjæle. Her kan den mentale model for det typiske offer som os alle sammen vise sig meget værdifuld.

Figur 4.7: Manglende Backup



4.2.5 Manglende Opdatering af Software og Styresystem

Kropsliggørelse: Låse/hængsler på døre/vinduer

I dette adfærdsmønster er der igen en problemstilling med medarbejderes private brug af især digitale mobilenheder stillet til rådighed af arbejdspladsen.

Større virksomheder udviser i brugertestene visse forbehold overfor automatisk opdatering af styresystemer, idet de angiveligt involverer potentielle produktivitetstab. Disse virksomheder skal derfor vejledes i, hvordan de kan opdatere styresystem uden at forstyrre den øvrige produktion – for det kan lade sig gøre.

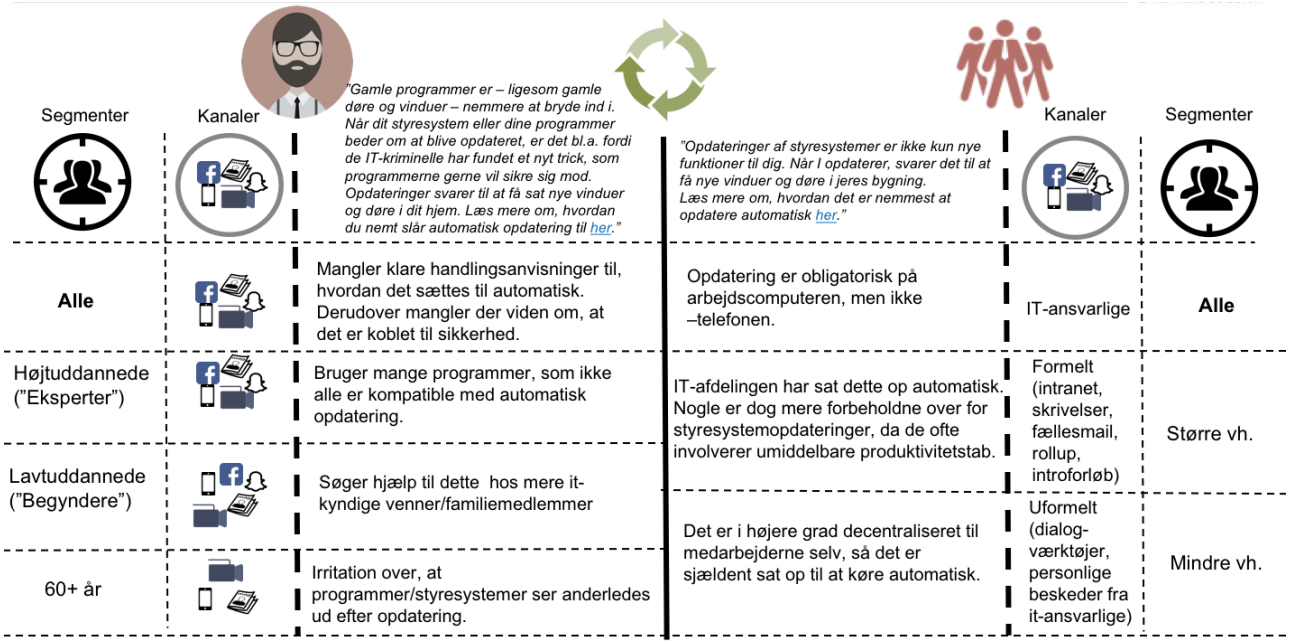
I mindre virksomheder er automatiseringen af opdateringer overladt til den enkelte medarbejder. Her skal budskabskommunikationen derfor søge – analogt til borgerkommunikationen – at gøre medarbejderne opmærksomme på, at automatisk opdatering er en godt værktøj til at holde sikkerheden i top. Alternativt kan kommunikationen anvise fordelene ved at samle ansvaret for denne handling hos én it-ansvarlig.

Borgerne efterspørger først og fremmest konkrete anvisninger til, hvordan opdatering opsættes automatisk. På nyere Windows-computere (dvs. med operativsystemet Windows 10) er automatisk opdatering standardindstillet. Det er det dog ikke på Apple-produkter. På iPhone og iPad er det nemt at slå til: 1) Tryk på Indstilling, 2) [Dit navn], 3) Slå automatisk opdatering til for hver af dine apps og operativsystem. På Mac-computere er det tilsvarende enkelt: 1) Tryk på ”Systemindstillinger”. 2) Vælg”App Store”, 3) Markér alle fem tjekbokse i vinduet.

Højtuddannede (specifikt ”eksperter”) angiver, at de bruger mange programmer, som ikke nødvendigvis er kompatible med automatisk opdatering. Her bør fokus derfor være på styresystemopdateringer som ovenstående.

En væsentlig problemstilling, som primært 60+ årige borgere har ytret sig om, er, at opdateringer ikke altid kun handler om ’indmaden’. I mange tilfælde ændres layout og opsætning ganske markant oven på en opdatering. Flere i denne gruppe udtrykker irritation over dette, og det bør budskabskommunikationen tage højde for. En helt simpel måde at gøre dette på, er at komme bekymringen i forkøbet ved at beskrive den i budskabskommunikationen og dermed vise borgeren, at vedkommende ikke er alene om denne bekymring. At kommunikere til folk i øjenhøjde gør, at de føler sig set og hørt – og det er befordrende for motivation for handling, især når handlingen involverer uundgåelige irritationsmomenter. En sætning kunne f.eks. lyde: ”Vi ved, hvor irriterende det er, at nogle programmer ser helt anderledes ud efter en opdatering. Det føles lidt som at starte forfra. Men opdateringer af programmer er ofte til for at holde dig it-sikker. På samme måde som at nye låse til døre og vinduer i dit hjem er med til at forebygge indbrud, er dine programmer og styresystemer mere sikre, når de er opdaterede.”

Figur 4.8: Manglende Opdatering af Software og Styresystem



4.2.6 Indtaster Personlige Oplysninger på Usikre Hjemmesider

Kropsliggørelse: Personlige ID-kort/værdipapirer (f.eks. pas, kreditkort)

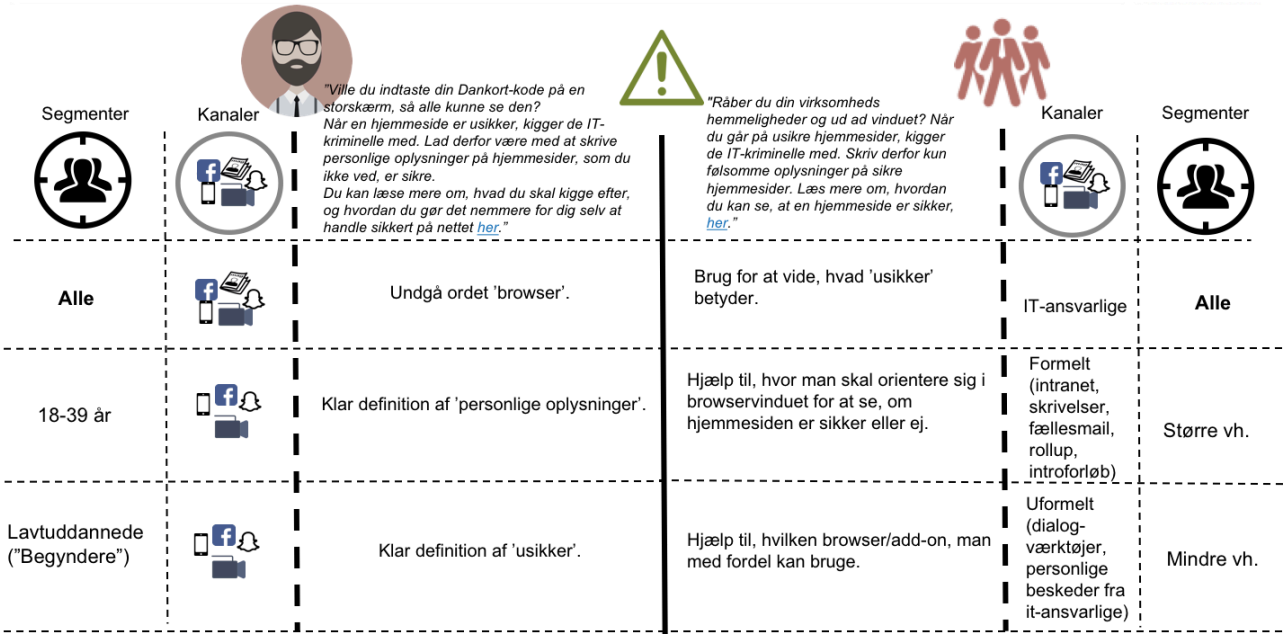
Her støder vi igen på et ekspertord, som senere kampagneindsatser bør undlade at bruge: 'Browser'. En signifikant del af befolkningen forstår simpelthen ikke, hvad ordet betyder, og derfor vil det fremmedgøre mange fra kommunikationen, hvis dette ord anvendes.

Medarbejderne mangler en definition af, hvad 'usikker' egentlig betyder for, hvad de bør/ikke bør gøre på en hjemmeside i en arbejdssammenhæng. I større virksomheder er browsere valgt for medarbejderen, og ofte bruges der flere forskellige, hvorfor der her snarere bør kommunikeres med hjælp til orientering i browservinduet: Hvor skal man kigge hen for at afgøre, om en hjemmeside er usikker eller ej. I mindre virksomheder, hvor valget af browser i højere grad er op til den enkelte medarbejder selv, kan den mere specifikke information om, hvordan visuelle cues f.eks. kan hjælpe én til at vurdere hjemmesiders sikkerhed hurtigere og bedre, og hvordan man får det installeret.

Blandt borgerne er den yngste gruppe (18-39 år) ret uvidende om, hvad 'personlige oplysninger' vil sige. De skal derfor informeres mere om dette, f.eks. gennem konkrete eksempler, som de kan relatere til (f.eks. kreditkort).

Lavtuddannede har et større behov end de øvrige for at få en klar definition af 'usikker'. Det gælder mest i forhold til, hvad det egentlig betyder for ens adfærd på den pågældende hjemmeside. Men også i forhold til, hvad 'usikker' mere konkret er. Her kunne man med fordel kommunikere klarere på, at 'usikker' er lig med 'nogen kigger med', dvs. 'overvågning'.

Figur 4.9: Indtaster Personlige Oplysninger på Usikre Hjemmesider



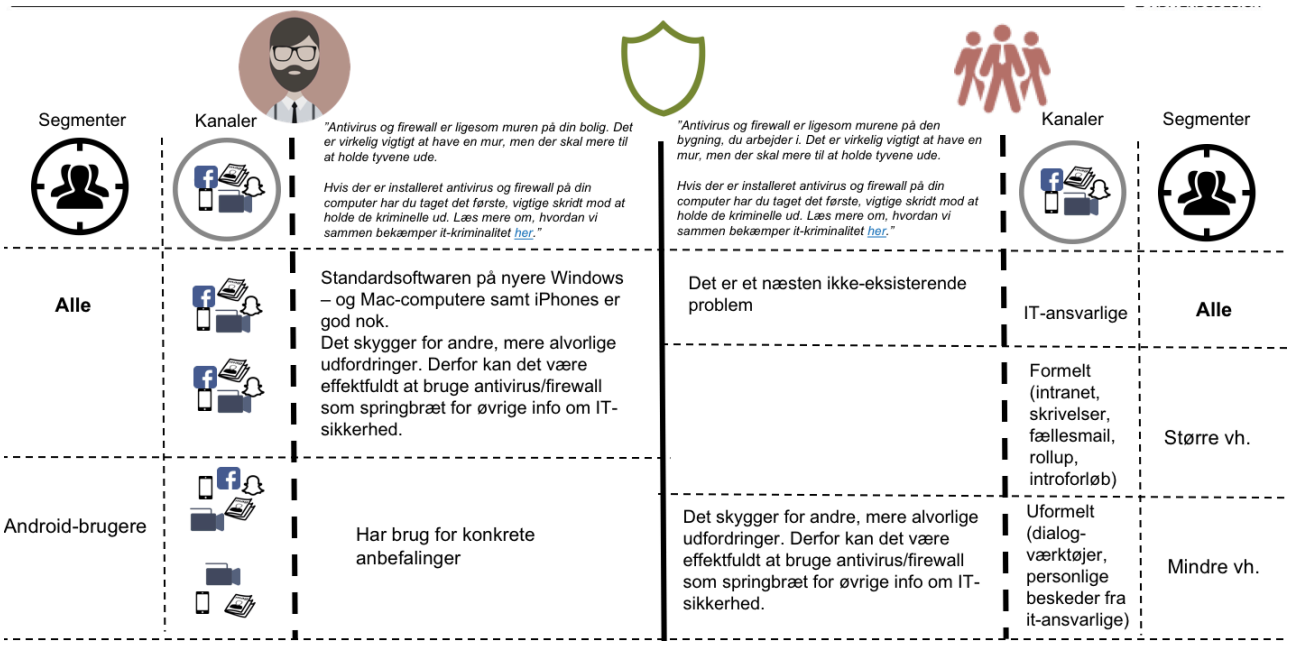
4.2.7 Manglende Installation af Antivirus/Firewall

Kropsliggørelse: Vagthund / Murværk

Det gælder for både borgere og medarbejdere, at dette adfærdsmønster er det blandt de udvalgte, som danskerne har færrest problemer med at forstå og udføre korrekt. Det er især et resultat af, at antivirus/firewall-standardsoftware på nyere Windows- og Mac-computere samt iPhones er noget af det bedste på markedet (Casey 2016). Faktisk er det kun Android-brugere, som har behov for konkret vejledning til investering i den rigtige antivirus/firewall. For medarbejdere i både mindre og større virksomheder gælder det, at it-afdelingen allerede har styr på dette punkt. Budskabskommunikationen til medarbejderne skal derfor alene adressere det, de skal gøre, når de kommer hjem fra arbejde.

For danskerne generelt gælder det, at antivirus/firewall fylder så meget i forståelsen af it-sikkerhed, at det potentielt kan komme til at skygge for de øvrige – og mere alvorlige – udvalgte adfærdsmønstre. Der er en udbredt opfattelse af, at antivirus/firewall er nok til at holde it-kriminaliteten for døren, mens det i virkeligheden alene tjener som et nødvendigt udgangspunkt for den enkelte borger og medarbejders it-sikkerhed. Derfor anbefales det, at kommunikationen om antivirus/firewall bruges som udgangspunkt for at sige til danskerne, at det er godt at have, men at det ikke er nok i sig selv. Det er godt udgangspunkt, men ikke hele løsningen. Derfor er kropsliggørelsen af antivirus/firewall som husmuren gavnlig, fordi den kommunikerer ret klart, at det er meget afgørende at have, men at det ikke alene holder de it-kriminelle ude.

Figur 4.10: Manglende Installation af Antivirus/Firewall



5.0 Kampagnestrategiske anbefalinger

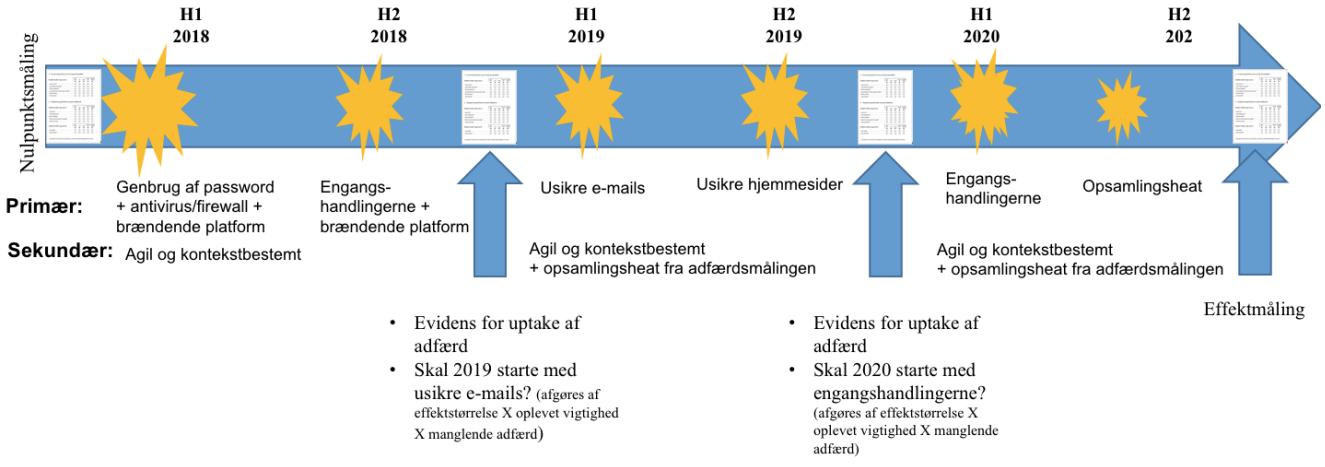
Generel kampagnestrategi

Den generelle kampagnestrategi for så komplekst et adfærdsproblem som digital sikkerhed bør baseres på evidens. Først og fremmest for at bruge ressourcer bedst i relation til problemets adfærdsmæssige rod og forventet effekt. Men også for at samle flest mulige interessenter bag fælles tiltag gennem enighed om hvilket adfærdsmønstre, der giver bedst mening at regulere og hvordan. Hertil kommer, at data og indsigter typisk danner grundlag for god og fokusskabende PR. Over en tre-årig periode og med så dynamisk et problemfelt indebærer en evidensbaseret strategi løbende målinger. Problemet vil med al sandsynlighed ændre sig flere gange undervejs.

/KL.7 anbefaler nedenstående kampagnestrategi (Figur 5.1) baseret på indeværende for-analyse af problemet samt egen årelange erfaring med evidensbaserede indsatser. På mere relationelle og dialogiske platforme hos partnere og f.eks. it-ansvarlige, er det nødvendigt med en mere differentieret tilgang (uddybes senere i dette kapitel).

Dertil anbefaler /KL.7 **præcision og sekventiel udrulning af budskaber snarere end 'mange råd' fra begyndelsen**. Grundlæggende skyldes denne anbefaling, at kampagnens fokus bør være på at skabe handling, ikke alene viden. At få brugere til at handle, kræver ofte begrænsning af råd, kompleksitet og ikke mindst at gøre råd meget handlingsorienterede i stedet for rent oplysende.

Figur 5.1



Den løbende kommunikation falder i to spor. **Det primære spor begynder med en indsats på to adfærdsmønstre: genbrug af passwords og installering af antivirus/firewall**. Førstnævnte er udvalgt, fordi det er en mest alvorlige problemstilling, som danskerne er mindst bevidste om vigtigheden af. Sidstnævnte er udvalgt, fordi dette adfærdsmønster allerede er etableret, men af danskerne *opleves* som det eneste vigtige, hvorfor det er afgørende at få slået fast, at der skal mere end antivirus/firewall til for at forebygge it-kriminalitet. Samtidig etableres **den brændende platform** – dvs. udbredelse af budskabet om it-sikkerheds aktuelle vigtighed, som bevirker, at det er afgørende at handle nu – gennem undersøgelser af hvor mange danskere, der frygter digital

kriminalitet, letforståelige illustrationer og forklaringer af, hvad den digitale trussel indebærer. Her inddrages denne for-analyses hovedindsigter om, at IT-kriminalitet skal gøres fysisk, den overordnede metafor for hjemmet skal bruges sammen med kropsliggjorte konkrete handlinger, samtidig med at den it-kriminelle skal italesættes som en tricktyv/svindler og offeret som os alle sammen. Det kræver identificérbare cases af alm. borgere og medarbejdere, der er kommet galt af sted med store konsekvenser; fremhævelse af spektakulære sager som Wannacry og aktuelt Goldeneye-angrebet på Mærsk; samt udtalelser fra autoriteter og specialister.

Målet med at etablere den brændende platform er at gøre indifferens overfor truslen meget vanskelig og udnytte adfærdsvidenskabelige principper som *identifikation* ('det kunne ske for mig'), *saliency bias* (spektakulære begivenheder er lettere at erindre og fører til overdreven risikooplevelse), *flokadfærd* (når vi kan få majoriteten af danskere til at svare, at de anser it-kriminalitet for at være fysisk kriminalitet, kan det anvendes kommunikativt), *autoritet* ('de dygtigste virksomhedsledere, meningsdannere og specialister tager dette meget seriøst, så det bør jeg nok også').

Det er altså et relativt ambitiøst projekt at etablere den brændende platform. Det kræver tværmediale indsatser og etablering af partnerskaber. Derfor anbefaler /KL.7, at der alene kommunikeres på et eller to adfærdsmønstre, mens dette arbejde pågår, idet der samtidig skal etableres et løbende beredskab til nyindkomne trusler.

Formidlingsformer i H1 2018

- **Borgere**

Fysiske reklamepladser på busstoppesteder, billboards og i landsdækkende papiraviser bør fokusere på at etablere den brændende platform, suppleret af kommunikationen omkring passwords til de mest centrale segmenter for denne formidlingsform: De højtuddannede, eksperterne samt alderssegmenterne 40-59 år og 60+ år.

De højtuddannede og eksperterne skal adresseres på en lødig og myndig måde. Eksempelvis kunne spalteplads i Weekendavisen, Berlingske og Information anvendes til at kommunikere konkrete råd til, hvad teknologiske løsninger kan gøre for password-sikkerheden, og hvordan man nemmest selv tager det i brug. I denne formidling kan den brændende platform godt indtage en mindre fremtrædende rolle, idet dette segment allerede er bevidste om alvorligheden af problemstillingen og er motiverede for at handle.

At etablere den brændende platform kan ikke gøres uden en mere massiv PR-indsats. Den centrale udfordring er, at medietrykket skal balancere mellem det, der skaber opmærksomhed og gør at danskerne husker det, og det, der kan opfattes som useriøst hysteri og dermed får en del til at ignorere budskaberne. En god og lødig måde at kommunikere i avisspalterne til det midaldrende og ældre segment ville være at udarbejde en kortfattet særudgave/indstik til f.eks. Politiken, som fokuserer på alvorligheden af it-sikkerhedsproblematikken, at antivirus/firewall ikke kan stå alene, og på, hvor meget sikker konstruktion, opbevaring og opdatering kan gøre. Her er der også fin plads til at kommunikere overbevisende ind i den metaforiske verden omkring 'Hjemmet' og give meget konkrete, handlingsanvisende råd relateret til genbrug af passwords. For at skabe yderligere styrke i metaforikken, kunne man overveje i stedet at lave denne indsats i boligmagasiner som f.eks. Bolius' Bedre Hjem.

Videospots og aktiv tilstedeværelse på sociale medier kan anvendes til at skabe mere personlige fortællinger, som kan gøre den brændende platform endnu mere troværdig for de yngre (18-39 år) og de lavere uddannede.

Førstnævnte skal gøres opmærksom på vigtigheden af at passe på deres personlige oplysninger, sociale medie-konti og e-mails med stærke passwords – ikke med skrækhistorier om unge mennesker, som har fået stjålet deres identitet og alle deres penge, men med almindelige hverdagshistorier om, hvor absurd vi opfører os i vores digitale tilværelse. Dette kunne med fordel gøres på Facebook, Instagram og Snapchat med unge influencers, der fortæller disse historier. Her er det centrale budskab, at man kun behøver at have unikke passwords på sine vigtigste steder på nettet. Dette er også med til at etablere den brændende platform for de yngre, fordi det opildner til en generel opmærksomhed på, hvad der egentlig er 'mit' vigtigste sted på nettet. Dette centrale budskab kan f.eks. formidles gennem test på Facebook, hvor man kan afprøve sine password-kundskaber. Hvis man fokuserer på Facebook og Google-mail, er anbefalingen, at de unge benytter sig af muligheden for to faktor-login. Med et bredere fokus bør anbefalingen være at benytte sig af en password manager til at opbevare og opdatere de vigtigste passwords.
De lavere uddannede samt begyndere skal adresseres med overbevisende kommunikation om, at de også har noget, som er værd at stjæle, og at deres password-sikkerhed derfor også er vigtig.

Samarbejde med "Mit Digitale Selvforsvar", som hvis alt går vel allerede er aftalt og klappet af i H2 2017, kan her indledes ift. passwords med henblik på at bygge ovenpå med de senere indsatser i hele perioden 2017-2020.

- **Virksomheder**

Fokusér på at udvikle et førstehjælpskit til **passwords** i samarbejde med it-ansvarlige i hhv. mindre og større virksomheder.

Kittet skal fokusere på, hvordan den it-ansvarlige kan være med til at øge medarbejdernes kompetenceniveau ift. passwordkonstruktion og –opbevaring.

Her er en central udfordring, at de it-ansvarlige er eksperter, som ikke vil tage et kit i brug, med mindre at de selv har været med i udviklingen af det, og at det kommunikere til dem i myndig tone. Det er derfor afgørende, at første kvartal bliver brugt på udvikling, mens andet kvartal kan bruges til konkret udsendelse.

Formidlingsformer i H2 2018

- **Borgere**

/KL.7 anbefaler, at **indsatsen i anden halvdel af 2018 skal fokusere på de to centrale éngangshandlinger: Automatisk backup og automatisk opdatering.**
Budskaberne om vigtigheden af at udføre disse to handlinger skal nå danskerne gennem et stort PR-fremstød, hvor eksperter og brugere helt konkret demonstrerer, hvordan man udfører dem. Ideelt orkestreres det som **en national it-sikkerhedsdag**, hvor vi får flest mulige danskere til at gennemføre disse handlinger på præcist den dag.
Den nationale digitale sikkerhedsdag kan gentages hvert år på samme dato, for at se, om man kan skabe en vedholdende dag for dette. Derudover kommer de øvrige adfærdsmønstre, løbende ét ad gangen. De øvrige adfærdsmønstre udvælges ud fra den foregående målings data, som viser, hvor behov og effekt er størst.

Arbejdet med den brændende platform anbefales fortsat i dette halvår.

Fremsendelse af nyt NemID anbefales benyttet til samlet kommunikation om brændende platform, passwords og engangshandlinger. En væsentlig udfordring er her, at det er plastikkortet, man som modtager er interesseret i, mens et evt. vedlagt A4-ark nemt ignoreres. Derfor kunne en strategi være enten at printe råd direkte på nøglekortet, eller alternativt at fremsende et fælles NemID til alle danskere kun med vejledning til password og engangshandlinger. Sidstnævnte kunne med fordel fremsendes på den nationale it-sikkerhedsdag.

- **Virksomheder**

Fokusér på at udvikle et førstehjælpskit til **engangshandlingerne** i samarbejde med it-ansvarlige i hhv. mindre og større virksomheder.

Kittet skal fokusere på, hvordan den it-ansvarlige kan være med til at øge medarbejdernes forståelse af den sikkerhedsmæssige vigtighed i at opdatere og tage backup på arbejdsenheder, de bruger privat, og på at opøve deres kompetenceniveau ift. at sætte begge op automatisk.

Her er en central udfordring, at de it-ansvarlige er eksperter, som ikke vil tage et kit i brug, med mindre at de selv har været med i udviklingen af det, og at det kommunikere til dem i myndig tone. Det er derfor afgørende, at tredje kvartal bliver brugt på udvikling, mens fjerde kvartal kan bruges til konkret udsendelse som et tillæg til det allerede eksisterende kit.

Virksomheder, der allerede har kittet fra H1 2018 om passwords, kan få dette som et tillæg, mens de virksomheder, der ikke har, får begge i en samlet pakke. Vi foreslår, at denne progression går igen i løbet af hele perioden 2017-2020, således at der helt konkret bygges oven på den hidtidige indsats fra halvår til halvår.

Formidlingsformer i H1 2019

- **Borgere**

På baggrund af erfaringerne med budskabsformidlingen i H1 2018 anbefales en fortsættelse heraf i regi af usikre e-mails. Desuden er det en væsentlig prioritet at gentage den nationale it-sikkerhedsdag.

- **Virksomheder**

Fokusér på at udvikle et førstehjælpskit til **usikre e-mails** i samarbejde med it-ansvarlige i hhv. mindre og større virksomheder.

Kittet skal fokusere på, hvordan den it-ansvarlige kan være med til at øge medarbejdernes kompetenceniveau ift. at identificere og håndtere e-mails med usikkert indhold.

Her er en central udfordring, at de it-ansvarlige er eksperter, som ikke vil tage et kit i brug, med mindre at de selv har været med i udviklingen af det, og at det kommunikere til dem i myndig tone. Det er derfor afgørende, at første kvartal bliver brugt på udvikling, mens andet kvartal kan bruges til konkret udsendelse.

Virksomheder, der allerede har det eksisterende kit, kan få dette som et tillæg, mens de virksomheder, der ikke har, får det hele i en samlet pakke.

Formidlingsformer i H2 2019

- **Borgere**

På baggrund af erfaringerne med budskabsformidlingen i H1 2018 og H1 2019 anbefales en fortsættelse heraf i regi af usikre hjemmesider.

- **Virksomheder**

Fokusér på at udvikle et førstehjælpskit til **usikre hjemmesider** i samarbejde med it-ansvarlige i hhv. mindre og større virksomheder.

Kittet skal fokusere på, hvordan den it-ansvarlige kan være med til at øge medarbejdernes kompetenceniveau ift. at identificere og håndtere e-mails med usikkert indhold.

Her er en central udfordring, at de it-ansvarlige er eksperter, som ikke vil tage et kit i brug, med mindre at de selv har været med i udviklingen af det, og at det kommunikere til dem i myndig tone. Det er derfor afgørende, at tredje kvartal bliver brugt på udvikling, mens fjerde kvartal kan bruges til konkret udsendelse.

Virksomheder, der allerede har det eksisterende kit, kan få dette som et tillæg, mens de virksomheder, der ikke har, får det hele i en samlet pakke.

Formidlingsformer i H1 2020

- **Borgere**

Her bør fokus være på at konsolidere den nationale it-sikkerhedsdag som kulmination på endnu en runde med kommunikation om engangshandlingerne.

- **Virksomheder**

Fokusér på at opdatere og tilrette det eksisterende førstehjælpskit i samarbejde med it-ansvarlige i hhv. mindre og større virksomheder med henblik på samlet udsendelse i H2.

Formidlingsformer i H2 2020

- **Borgere**

På baggrund af de hidtidige erfaringer med kampagneindsatserne 2018-2020 anbefales her et større opsamlingsheat, hvor hele rækken af adfærdsmønstre adresseres samlet.

- **Virksomheder**

Fokusér på at udsende det opdaterede og tilrettede førstehjælpskit i samarbejde med it-ansvarlige i hhv. mindre og større virksomheder.

Det sekundære spor er først og fremmest designet til at kunne agere agilt, når f.eks. et nyt verdensomspændende angreb bør udnyttes som en platform for kommunikation og tiltag, som omvendt løbende designes til at imødegå de specifikke trusler og nødvendige handlinger. Derudover er sporet med til at samle op på de adfærdsmønstre, hidtidige tiltag ikke tilstrækkeligt har at flytte ifølge seneste måling.

Partnerstrategi

Det er essentielt at samle flest mulige nøgleinteressenter om kampagnens budskaber og tiltag. Både for at maksimere tilstedeværelse og lokal tilpasning, men også for at modvirke støj fra forskelligartede kampagner. Dette kræver lydhørhed overfor store erhvervs- og forbrugerorganisationers behov og dagsordener, men også at synliggøre hvordan en national strategi understøtter deres egne dagsordener og mål. /KL.7 har i forbindelse med for-analysen været i kontakt med f.eks. Det Digitale Råd, Yousee, og Dansk Erhvervs it-ansvarlige og mødt meget stor interesse for inddragelse i udrulning af tiltag. Det forventes at møde samme reaktion fra DI, Forbrugerrådet Tænk og andre væsentlige aktører, som /KL.7 har samarbejdet med i andre sammenhænge.

Desuden anbefaler /KL.7 at afsøge mediepartnere til at sætte ekstra fokus på sagen. Dette kræver ofte en form for eksklusivitet på dele af indsigter og 'serveret' på temaer. Omvendt opnås stor opmærksomhed på problemet, som vil være meget dyr at skabe gennem medieindrykning. Samtidig kan en mediepartner skabe redaktionelle formater, hvor menneskene bag problemet udfoldes for større identifikation og dybde. Jf. Berlingskes forsøg med at få adgang til al data på to politikere, som skabte stor opmærksomhed og debat om overvågning. /KL.7 har tidligere samarbejdet med både Politiken og DR på lignende problemfelter, og anbefaler at **afsøge både en erhvervs- og en forbrugerrettet mediepartne**r, hvis muligt, eller en mediepartner som Berlingske, der ville kunne dække begge.

Konkret anbefaler /KL.7 at **samle nøgleinteressenter i efteråret 2017** til præsentation og drøftelse af fund og strategiudkast, inden første kampagne iværksættes. Inddragelse af nøgleinteressenter bør som minimum indgå som krav i et evt. udbud af kampagneaktiviteter, så det vindende bureau sikrer sig, at tiltag er præsenteret for og gerne afstemt med de vigtigste interessenter.

Budskaber og redskaber til partnere og øvrige interessenter (f.eks. it-ansvarlige)

Som tidligere nævnt kan budskaber aktiveres mere agilt sammen med interessenter. F.eks. kunne rådgivere på kommende kampagner afsætte ressourcer til at imødekomme lokale ønsker og udvikle versioneringer eller tilbyde rådgivning om dette, til virksomheder, myndigheder og organisationer, som ønsker hjælp til at styrke deres egen indsats. Disse ressourcer kan være til rådighed gennem et fast kampagnekontor eller gennem et 'swat team' der besøger interessenter og holder oplæg om indsatsen og rådgiver om lokale tiltag.

Vi anbefaler desuden at udvikle sikkerhedspakker til organisationer og sikkerhedsansvarlige, som både understøtter lokale indsatser, men samtidig muliggør en vis fleksibilitet i relation til lokale udfordringer og ønsker. /KL.7 har som eksempel udviklet beoer- og beboerformandskit for TrygFonden for at modvirke indbrud, baseret på udbredte forestillinger, handlevillighed og

motivation, nøgleinteressenters dagligdag og ressourcer samt ekspertvurderinger af størst effekt med mindste mulig indsats. Få kontaktdata og feedback løbende, samt data på brug og uptake.

Alle pakker og værktøjer, som kampagnen udvikler, bør sikres et 'liv efter kampagnen'. Det er nødvendigt for at sikre størst mulig effekt af tiltagene.

Vores erfaringer fra TrygFonden-projektet viser, at de færreste beboerformænd ønsker at drive processer, men kun at initiere dem. Sikkerhedspakken rettet til formænd blev derfor indrettet til at gøre det lettere for formanden at engagere folk, men uden at træde ind i "privatsfæren" hos medlemmerne – det skal være værktøjer, der kan skabe handling for beboerne selv.

På samme måde anbefaler vi, at kittet til it-ansvarlige udarbejdes med tanke på, at de it-ansvarlige skal igangsætte handlinger hos medarbejderne – både professionelt og privat – men at de ikke har ansvaret efterfølgende.

Desuden viste TrygFonden-projektet, at beboerformændene tog vel imod information om, hvordan de kunne hjælpe beboerne til selvhjælp, men at *tonen* skulle holdes så myndig som muligt. Ellers føler beboerformændene, at de bliver talt ned til – og det skal man undgå, når man taler til eksperter, som selv finder glæde i at videreformidle komplekst stof. Brugertestene i denne for-analyse viser, at de it-ansvarlige har en lignende selvopfattelse. Vi anbefaler derfor at kommunikere på samme måde til de it-ansvarlige.

Metrik og metodeudvikling

Kampagnen bør løbende måle på effekten af indsatsen. Dvs. at der måles på, om de seneste budskaber og tiltag har ført til tilstrækkelige adfærdsændringer og hvilke. På den måde giver målingerne pejlemærker for, hvilke budskaber der bør prioriteres den følgende periodes primære og sekundære spor, samtidig med at indsatsen evalueres.

Det anbefales at afsætte en væsentlig del af budgettet til metode, idet der skal udvikles metoder der kan kortlægge den faktiske adfærd (og dens konsekvenser), og ikke kun den adspurgte adfærd. Eller i bedste fald metoder, der bringer os tættest muligt på at dokumentere adfærden ved andet end f.eks. antal downloads og visninger.

KPI'er

Den væsentligste KPI bør være, at eventuelle digitale redskaber, der udvikles, bruges efter kampagnens ophør. Danskernes udfordringer ift. it-sikkerhed forsvinder ikke af, at kampagnen ophører. Ved at måle på brug efter kampagnens ophør, måles der på bæredygtig adfærd. Derudover er det relevant at inddrage en KPI ift. at nedbringe de estimerede problemstørrelser på adfærdsmønstrene hver især så meget som muligt. Det er et naturligt succeskriterium, at danskerne kommer tættere på at handle på de kritiske adfærdsmønstre.

Litteraturliste

Aiken, M. (2016). The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online.

Alhadeff, A., Blau, A. (2016). The Problem With Your Computer's Security Warnings. Hentet fra: http://www.ideas42.org/blog/problem-computers-security-warnings/

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A., & Passingham, N. (2015). Awareness is only the first step. *A framework for progressive engagement of staff in cyber security, Hewlett Packard, Business white paper*.

Blau, A., Stern, M. (2016). Reframing Mental Models of Cybersecurity. Hentet fra: http://www.ideas42.org/blog/reframing-mental-models-cybersecurity/

Bouton, M.E. (2007). *Learning and behavior: A contemporary synthesis*. MA Sinauer: Sunderland

Casey, Henry T. (2016). Why Apple Doesn't Need Antivirus Software. Tom's Guide. Hentet fra: https://www.tomsguide.com/us/iphones-dont-need-antivirus-software,news-23111.html

Cisco (2017). *Visual Networking Index: Forecast and Methodology, 2016–2021*. Hentet fra: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html

Chapin, John; Grace Coleman (2009). Optimistic Bias: What you Think, What you Know, or Whom you Know?. *North American Journal of Psychology*. 11 (1): 121–132.

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. *gov. uk report*.

Coventry, L. M., Jeske, D., Blythe, J. M., Turland, J., & Briggs, P. (2016). Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance. *Frontiers in Psychology*, *7*.

Digitaliseringsstyrelsen og DKCERT (2017). Danskernes Informationssikkerhed 2016. Hentet fra: https://www.digst.dk/~/media/Files/Informationssikkerhed/Informationssikkerhed-efter-ISO27001/Rapporter/Danskernes-informationssikkerhed-2016.pdf

Eysenck, M. W. (2012). Fundamentals of cognition. New York: Psychology Press

Fallows, J. (2011). Cyber-Security Can't Ignore Human Behavior. The Atlantic. Hentet fra: https://www.theatlantic.com/technology/archive/2011/03/cyber-security-cant-ignore-human-behavior/72826/

Forrester, J. W. (1971). Counterintuitive behavior of social systems. *Technology Review.*

Kahneman, D., Knetsch, J. L., Thaler, R. H. *(1991). "Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias". Journal of Economic Perspectives. 5 (1): 193–206.*

KMD (2016). "Analyse: Offentligt ansatte slår fortrolige oplysninger op af nysgerrighed". *KMD Analyse Briefing. Hentet fra https://www.kmd.dk/~/media/documents/kmd-analyse/kmd-analyse-briefing---informationssikkerhed-i-det-offentlige---juni-2016-pdf.pdf?la=da-dk*

Krol, K., Spring, J. M., Parkin, S., & Sasse, M. A. (2016, May). Towards robust experimental design for user studies in security and privacy. In *Learning from Authoritative Security Experiment Results (LASER) Workshop*.

Lewis, Alan (17 April 2008). *The Cambridge Handbook of Psychology and Economic Behaviour*. Cambridge University Press. p. 43

Milgram, Stanley (1963). "Behavioral Study of Obedience". *Journal of Abnormal and Social Psychology*. 67 (4): 371–8

Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. Psychological Review. 63 (2): 81–97.

Morgan, M. G. (2002). *Risk communication: A mental models approach*. Cambridge University Press. P. 21.

Mosley, D. (2006). Some Psychological Factors of Successful Phishing. Hentet fra: http://www.infosecwriters.com/text_resources/pdf/Phishing_DMosley.pdf

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), 597-611.

Proofpoint (2016). The human factor report 2016. Hentet fra: https://www.proofpoint.com/us/resources/white-papers/human-factor-report

Ropeik, David (2010). How Risky Is It, Really?: Why Our Fears Don't Always Match The Facts.

The Royal Society (2016). Progress and research in cybersecurity, Supporting a resilient and trustworthy system for the UK. Hentet fra: https://royalsociety.org/~/media/policy/projects/cybersecurity-research/cybersecurity-research-report.pdf

Bilag

Vedlagt findes transskriberinger af ekspert-interview og brugertest samt survey-rapport.

Herunder er de 18 identificerede adfærdsmønstre oplistet i skemaform med kildeangivelser på både psykologisk forskning og rapportmateriale:

Adfærdsmønster	Psykologiske barrierer	Kilder
Genbruger simpelt password på flere login-sider	Mental båndbredde, status quo-bias,	Eysenck 2012, Kahneman et al. 1991, DKCERT-undersøgelsen 2016, Pfleeger & Caputo 2012, Blau et al. 2016
Mangler at installere antivirus/firewall	Overdreven tiltro til egen fremtidige sikkerhed, tabsaversion	Chapin & Coleman 2009, Kahneman & Tversky 1992, DKCERT-undersøgelsen 2016
Udskyder opdatering af software	Habituering, manglende feedback og belønning,	Bouton 2007, Eysenck 2012, DKCERT-undersøgelsen 2016, Proofpoint 2016, Blau et al. 2016, Blau et al. 2016
Undlader/glemmer at logge ud af konti/computer efter endt brug	Tabsaversion, habituering, genkendelse og autoritetstro,	Kahneman & Tversky 1992, Bouton 2007, Milgram 1963,
Undlader at læse "User Agreement"- og "Terms and conditions"-dokumenter	Genkendelse og autoritetstro, tabsaversion, overdreven tro på egen sikkerhed i fremtiden,	Milgram 1963, Kahneman & Tversky 1992, Chapin & Coleman 2009, DKCERT-undersøgelsen 2016, Mosley 2006, Pfleeger & Caputo 2012,
Forsømmer at slå deling af private oplysninger fra	Manglende heuristikker for personlige oplysninger, overdreven tro på egen sikkerhed i fremtiden, tabsaversion,	Lewis 2008, Chapin & Coleman 2009, Kahneman & Tversky 1992, DKCERT-undersøgelsen 2016, Blau et al. 2016,
Ignorerer sikkerhedsadvarsler	Habituering, mønstergenkendelse, mental båndbredde	Bouton 2007, Eysenck 2012, Eysenck 2012.
Undlader/glemmer at tage backup af essentielle data	Overdreven tro på egen sikkerhed i fremtiden, tabsaversion	Chapin & Coleman 2009, Kahneman & Tversky 1992, DKCERT-undersøgelsen 2016
Ingen timeouts på smartphone/computer	Overdreven tro på egen sikkerhed i fremtiden, tabsaversion	Chapin & Coleman 2009, Kahneman & Tversky 1992,

Ingen skærmbeskytter på bærbar ved arbejde i det offentlige rum	Overdreven tro på egen sikkerhed i fremtiden, tabsaversion	Chapin & Coleman 2009, Kahneman & Tversky 1992,
Deler konti med flere mennesker	Tabsaversion, genkendelse og autoritetstro	Kahneman & Tversky 1992, Milgram 1963, KMD 2016,
Henter "gratis" smartphone-apps, som normalt koster penge, fra uofficielle app-butikker	Tabsaversion, manglende heuristik for usikre apps, mønstergenkendelse, genkendelse og autoritetstro,	Kahneman & Tversky 1992, Lewis 2008, Eysenck 2012, Milgram 1963, Proofpoint 2016,
Bruger usikre hjemmesider	Tabsaversion, manglende heuristik for usikre hjemmesider,	Kahneman & Tversky 1992, Lewis 2008, DKCERT-undersøgelsen 2016, Mosley 2006
Klikker på pop-up reklamer	Tabsaversion, genkendelse og autoritetstro,	Kahneman & Tversky 1992, Milgram 1963, Pfleeger & Caputo 2012,
Åbner ukendt USB-stik	Tabsaversion, manglende heuristik for usikre USB-stik,	Kahneman & Tversky 1992, Lewis 2008, KMD 2016,
Logger på trådløst internet uden kode	Tabsaversion, genkendelse og autoritetstro,	Kahneman & Tversky 1992, Milgram 1963, Mosley 2006, Blau et al. 2016,
Klikker på ukendt link	Genkendelse og autoritetstro, tabsaversion, manglende heuristik for usikre link	Milgram 1963, Kahneman & Tversky 1992, Lewis 2008, Proofpoint 2016, Mosley 2006, Blau et al. 2016
Åbner indhold i e-mail fra ukendt (eller tilsyneladende kendt) afsender	Genkendelse og autoritetstro, mønstergenkendelse	Milgram 1963, Eysenck 2012, DKCERT-undersøgelsen 2016, KMD 2016, Proofpoint 2016, Mosley 2006, Mosley 2006, Pfleeger & Caputo 2012, Blau et al. 2016
Deler private oplysninger	Tabsaversion	Kahneman & Tversky 1992, DKCERT-undersøgelsen 2016, Pfleeger & Caputo 2012,

Herunder er interviewguide til brugertest:

Borgere:

Introduktionsspørgsmål

- *Fortæl mig, hvad du ved om IT-sikkerhed (eventuelt frames som "sikkerhed på Internettet"). [Skal gerne transskriberes ord for ord]*
- *Hvor har du din viden om IT-sikkerhed fra?*

Spørgsmål til teksten [Brugeren får vist tekst med budskaber]

- *Fortæl mig, hvad der stod i teksten, så godt du kan.*
- *Hvad ville du gøre først?*
- *Hvordan vil du handle på rådene?*
- *Hvor kunne du forestille dig at læse disse råd?*

Opfølgende spørgsmål til teksten

- *Er det ny information for dig, at IT-kriminelle ved mere om din psykologi end om kompliceret kodning? Hvis "ja", hvordan?*
- *Giver det mening for dig at sige, at en usikker computer inviterer IT-kriminelle ind i stuen? Hvorfor/hvorfor ikke?*

Faktuelt spørgsmål til allersidst:

- *Hvor mange timer bruger du ca. dagligt på…*
  - *… at se TV?*
  - *… på sociale medier?*
  - *… læse aviser på internettet?*
  - *… læse og besvare e-mails?*

Medarbejdere

Introduktionsspørgsmål:

- *Hvad er din stilling i virksomheden? [notér også køn og alder?*
- *Fortæl mig, hvad du ved om IT-sikkerhed. [Skal gerne transskriberes ord for ord]*
- *Gør du noget bestemt for at sikre dig, at dine informationer er godt beskyttede?*
- *Hvor meget fylder IT-sikkerhed i jeres virksomhed?*

Spørgsmål til e-mailen:

- *Forestil dig, at den it-ansvarlige på din arbejdsplads sender denne e-mail ud til dig. [Teksten vises til testpersonen]*
- *Hvordan forstår du rådene i e-mailen? Giver de mening for dig – hvorfor/hvorfor ikke?*
- *Beskriv hvordan du vil handle på baggrund af rådene.*
- *Hvis du skulle i gang med at udføre de 5 skridt i tjeklisten, hvad ville du så starte med at gøre? Og hvorfor?*

Opfølgende spørgsmål efter genfortælling af e-mailen:

- *Er det ny information for dig, at IT-kriminelle ved mere om din psykologi end om kompliceret kodning? Hvis "ja", hvordan?*
- *Giver det mening for dig at sige, at computeren kan sikres lige som dit hjem? Hvorfor/hvorfor ikke?*
- *Hvis ikke informationen skulle sendes som en e-mail, hvordan ville det så være bedst at få den rundt i hele din virksomhed?*

IT-Ansvarlige

Introduktionsspørgsmål:

- *Fortæl mig, hvad du ved om IT-sikkerhed. [Skal gerne transskriberes ord for ord]*
- *Hvor meget fylder IT-sikkerhed i dit daglige arbejde?*
- *Hvad er de største udfordringer i forhold til IT-sikkerhed i jeres virksomhed?*

Spørgsmål til e-mailen:

- *Hvordan forstår du e-mailen?*
- *Tjekliste 1 beskriver de vigtigste ting, du som it-ansvarlig skal sørge for ift. den digitale sikkerhed på din*

arbejdsplads. Hvordan forstår du rådene i Tjekliste 1?
- *Hvordan vil du udføre de ting, der anbefales i Tjekliste 1? Giver rækkefølgen mening?*
- *Tjekliste 2 henvender sig til medarbejderne i din virksomhed og de ting, de selv skal gøre for at øge deres digitale sikkerhed. Vurderer du, det giver mening at sende Tjeklisten ud til dine medarbejder – hvorfor/hvorfor ikke?*

Opfølgende spørgsmål efter genfortælling af e-mailen:
- *Er det ny information for dig, at IT-kriminelle ved mere om din psykologi end om kompliceret kodning? Hvis "ja", hvordan?*
- *Giver det mening for dig at sige, at computeren kan sikres lige som dit hjem? Hvorfor/hvorfor ikke?*
- *Hvis ikke informationen skulle sendes som en e-mail, hvordan ville det så være bedst at få den rundt i hele din virksomhed?*
- *Har du nogle råd eller anbefalinger til noget, som kunne gøre IT-sikkerheden bedre i virksomheder som din?*

Fravalgte adfærdsmønstre

De følgende adfærdsmønstre er alle fravalgt som fokusområder, da de enten indebærer en mindre alvorlig risiko eller vurderes at være urealistiske at ændre.

Deler konti med andre

Angela Sasse påpeger at dette adfærdsmønster udgør et mellemstort problem, og at det gælder både for borgere og ansatte. Rasmus Theede refererer til en nylig undersøgelse, der viste, at danske offentligt ansatte med it som kerneområde deler passwords med hinanden. Årsagen er, at det simpelthen er nemmere og mere belejligt at dele konti for mange i mange situationer. Og det ser flere af eksperterne som vanskeligt at gøre noget ved. Adfærdsmønsteret er fravalgt, fordi det både udgør et relativt mindre problem end de øvrige og er relativt svært at gøre noget ved med handlingsanvisende massekommunikation.

Eksperter, der fremhæver adfærdsmønsteret: Angela Sasse, Rasmus Theede.

Ignorerer sikkerhedsadvarsler

Vi modtager mange sikkerhedsadvarsler fra diverse antivirusprogrammer og anden software i løbet af en almindelig dag. Forskningen viser imidlertid, at mængden af 'falske alarmer' gør os indifferente overfor dem (Fallows 2011). Christian Jæhger peger på, at en af de væsentligste problemer her er timing: Advarsler skal komme på et tidspunkt, hvor man ikke er i gang med "et-eller-andet andet". Man må således helst ikke være i gang med dagens øvrige gøremål, idet man modtager advarslen. Herudover skal de også være udtryk for reelle trusler, som man rent faktisk bør forholde sig til. Jan Kaastrup gør dog opmærksom på, at disse to krav er vanskelige at honorere. For det første er det en ganske svær opgave, at sikre at en advarsel gives netop i en situation hvor folk ikke er i gang med noget andet. For det andet er det ofte svært på forhånd at forudsige hvad der er kritisk at forholde sig til, og hvad der senere hen skal vise sig at være mindre kritisk. Sammenholdt med, at dette adfærdsmønster er blandt de mindre alvorlige, har vi fravalgt det i det videre arbejde.

Eksperter, der fremhæver adfærdsmønsteret: Anders Kjærulf, Angela Sasse, Christian Jæhger.

Læser ikke ”User Agreements”/”Terms and Conditions”
Flere eksperter peger på, at det er problematisk, at danskerne i vid udstrækning ikke læser disse dokumenter. Spørgsmålet er dog, om det overhovedet er muligt at gøre noget ved – og det er der lige så bred enighed om, at man ikke kan. Angela Sasse har foretaget flere studier, der alle sammen peger på, at det er meningsløst at få folk til at læse disse dokumenter. De er både umådeligt lange og bevidst vanskelige for en lægmand at forstå. Rasmus Theede spørger dertil retorisk, hvad folk skal gøre, i fald de når så langt som til at have læst det hele. Det er yderst vanskeligt at se meningsfulde handlingsanvisende budskaber til dette adfærdsmønster, og derfor er det fravalgt, selvom det udgør en væsentlig problemstilling.

Eksperter, der fremhæver adfærdsmønsteret: Angela Sasse, Kim Aarenstrup,

Klikker på pop up-reklamer
Angela Sasse placerer denne adfærd i midterkategorien hvad angår konsekvenser. Fristende tilbud, som pludselig dukker op på din skærm, kan være vanskelige at ignorere – især fordi de opfordrer til impulsive handlinger, som vi er mere tilbøjelige til at foretage på nettet (Aikens, 2016). Mange klikker på dem, men andelen falder ifølge Angela Sasse, fordi disse reklamer i forhold til phishing e-mails og ransomware er relativt kluntet udført og bliver mere gennemskuelige for folk. Herudover forventer man eksempelvis at modtage mails fra sine kolleger eller det offentlige, mens man ikke har nogen forventninger om at pop-ups skal indeholde noget man skal reagere på. Af denne årsag er det nemmere for folk at gennemskue, når pop-ups er til for at narre dem. Kombinationen af at konsekvenserne ved at klikke på pop-ups ikke er ret store, og det faktum at folk har nemmere ved at gennemskue dem, gør at dette adfærdsmønster er fravalgt.

Eksperter, der fremhæver adfærdsmønsteret: Angela Sasse.

Anvender usikkert USB-stik
Det er forbundet med store konsekvenser at stikke et usikkert USB-stik ind i sin computer – især hvis computeren er forbundet til et lokalt netværk på en arbejdsplads el.lign. Ifølge flere eksperter er det dog ikke en særligt udbredt angrebsstrategi. Det ses mest i forbindelse med større organiserede angreb, f.eks. i forbindelse med international efterretningsvirksomhed. Almindelige mennesker – medarbejdere og såvel som borgere – vil imidlertid relativt sjældent opleve det. Dertil mener Rasmus Theede, at det er meget vanskeligt at ændre adfærden i en konkret praktisk kontekst: For hvordan sikrer man sig helt nøjagtigt, at et usb-stik ikke indeholder noget usikkert, uden at stikke den ind i en computer? Adfærdsmønsteret er derfor fravalgt.

Eksperter, der fremhæver adfærdsmønsteret: Rasmus Theede, Christian Jæhger, Anders Kjærulff

Bruger offentligt WIFI
Det er en meget udbredt problemstilling, at danskerne logger på usikre netværk i det offentlige rum. Potentielt kan det kompromittere personfølsom info fra både NemID og Dankort, når netværket ikke med kodeord og kryptering lukker af for uvedkommende, og derfor er truslen fra denne adfærd ret alvorlig. Et angreb kræver dog, at den cyberkriminelle befinder sig inden for netværkets fysiske rækkevidde. Sandsynligheden for at få kompromitteret sin sikkerhed ved at bruge et offentligt tilgængeligt WIFI er derfor ikke ret stor. Dette adfærdsmønster er fravalgt, fordi truslen herfra forekommer sjældnere end de trusler, der går på tværs af netværk.

Eksperter, der fremhæver adfærdsmønsteret: Angela Sasse

Glemmer at logge ud af device/computer
Dette adfærdsmønster er placeret i kategorien ”Mindre konsekvenser” – også selvom det kan være alvorligt nok at få ens device/computer overtaget af en fremmed med onde intentioner. Truslen herfra opstår imidlertid bare så sjældent, at det ikke er et problem, almindelige mennesker vil støde på. Ligesom med usikre usb-stik og offentlig WIFI afhænger denne trussel af den IT-kriminelles fysiske tilstedeværelse. Og det gør den mere usandsynlig end øvrige trusler. Faktisk går Christian Jæhger så langt som til at sige, at truslen er mere repræsentativ for et amerikansk tv-serie-univers end en fysisk dansk hverdag. Så selvom det sandsynligvis er muligt at ændre folks adfærd i denne sammenhæng, ville det ikke gøre nær så stor en forskel for danskernes overordnede informationssikkerhed som en påvirkning af de udvalgte adfærdsmønstre.

Eksperter, der fremhæver adfærdsmønsteret: Christian Jæhger

Ingen timeouts på device/computer
Samme som ”Glemmer at logge ud af device/computer” (se ovenfor).

Mangler skærmfilter på laptop
Samme som ”Glemmer at logge ud af device/computer” (se ovenfor).