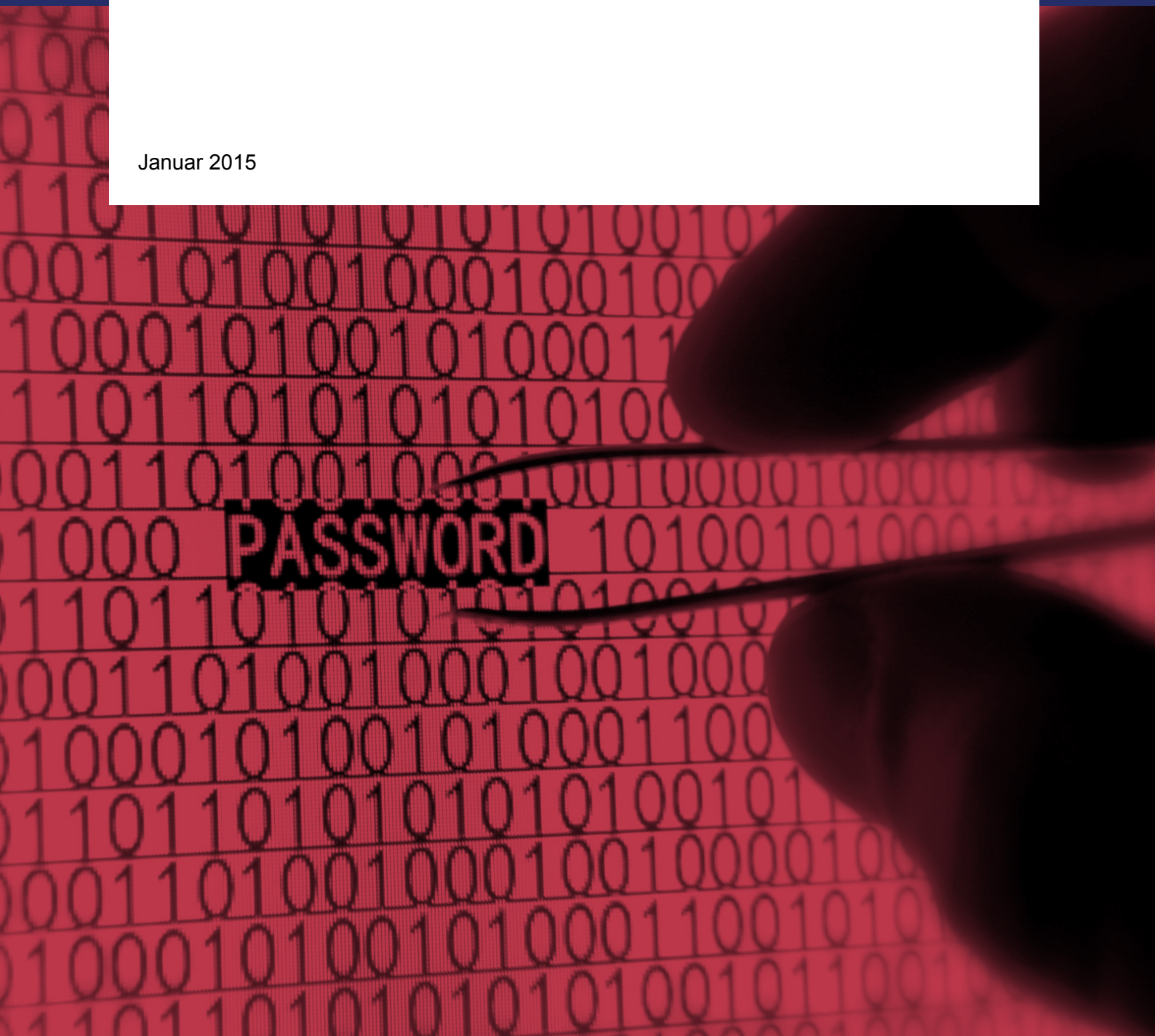
DIGITALISERINGSSTYRELSEN DKCERT DeiC DANISH e-INFRASTRUCTURE COOPERATION

Borgernes informationssikkerhed 2014

Januar 2015



1. Indledning

Formålet med denne rapport er at afdække to sider af danskernes forhold til informationssikkerhed. Den ene side handler om, hvilke sikkerhedshændelser borgerne bliver udsat for. Den anden side er deres viden om informationssikkerhed og evne til at beskytte sig mod udbredte trusler.

Rapporten er primært baseret på resultaterne fra en undersøgelse, som Danmarks Statistik foretog for Digitaliseringsstyrelsen og DKCERT i efteråret 2014. Undersøgelsen stillede en række spørgsmål til et repræsentativt udvalg af den voksne danske befolkning om deres erfaringer med informationssikkerhed. Undersøgelsen bygger på svar fra 1.111 personer i alderen 16-74 år.

Danmarks Statistik udførte en lignende undersøgelse for DKCERT i efteråret 2013. Resultaterne fra denne undersøgelse indgår i denne rapport under de punkter, hvor det er muligt at foretage en sammenligning.

Nogle af resultaterne er sat i perspektiv ved hjælp af data fra publikationen "It-anvendelse i befolkningen", som Danmarks Statistik udsendte i slutningen af oktober 2014. De sikkerhedsrelevante data fra denne publikation belyses i afsnit 3: Øvrige data.

BORGERNES INFORMATIONSSIKKERHED 2014

Digitaliseringsstyrelsen og DKCERT, DeIC
Redaktion: Shehzad Ahmad og Torben B. Sørensen
Design: Kiberg & Gormsen

DKCERT, DeIC
DTU, Asmussens Allé, Bygning 305
2800 Kgs. Lyngby

DeIC-journalnummer: DeIC JS 2015-1

2. Danskernes informationssikkerhed

Danskerne har taget digital teknologi til sig i stort omfang. Ifølge "It-anvendelse i befolkningen" har 93 procent af alle familier adgang til internet i hjemmet. 73 procent af alle husstande har en eller flere smartphones. 45 procent har en tablet.

Alle disse teknologier indebærer risici: Borgerne kan miste data, hvis udstyret går i stykker. Deres personlige oplysninger kan blive misbrugt, hvis uvedkommende får adgang til dem. Og udstyret kan blive ramt af virus, der viser uønskede reklamer eller spærrer for adgangen til systemet.

I det følgende belyser Digitaliseringsstyrelsen og DKCERT den aktuelle status for danskernes informationssikkerhed ud fra svarene i undersøgelsen.

2.1. Oplevede trusler

DKCERT har spurgt danskerne, om de har oplevet tre specifikke trusler mod deres informationssikkerhed: Virus, misbrug af personlige data og økonomisk tab som følge af en sikkerhedshændelse. Svarene fra 2014 er på niveau med dem fra 2013: Knap en tredjedel har været udsat for virusangreb, som dermed er langt den hyppigste trussel. Kun to procent har oplevet misbrug af data eller økonomisk tab. Begge er en smule mindre end året før.

Tallene viser kun, hvilke sikkerhedstrusler borgerne har opdaget. Det er derfor muligt, at flere kan have været udsat for fx virusinfektioner eller misbrug af fortrolige data, uden at de har opdaget det.

2.2. Konsekvenser som følge af truslerne

De borgere der havde oplevet en af de tre sikkerhedstrusler, blev spurgt, hvilke konsekvenser det havde for deres adfærd. Den hyppigste reaktion på en trussel var at installere sikkerhedssoftware. Det gjorde 72 procent af deltagerne, hvilket er lidt færre end de 81 procent i 2013.

To ud af tre blev mere forsigtige med at dele personlige data på sociale netværk efter hændelsen. Og godt halvdelen undlod at besøge bestemte websteder som følge af deres oplevelse.

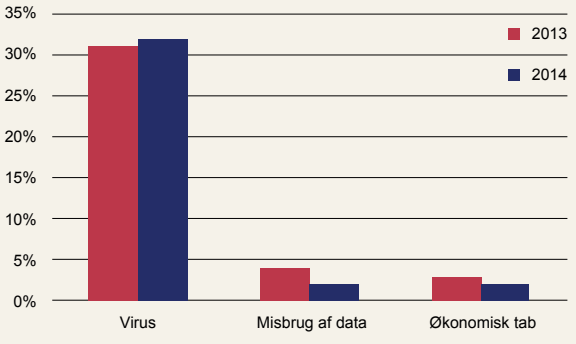
Kun otte procent afholdt sig fra at bruge offentlige selvbetjeningsløsninger, efter at de var ude for en sikkerhedstrussel. Det er lidt færre end i 2013, hvor tallet var 11 procent. En mulig forklaring kan være, at borgerne ikke ser nogen sammenhæng mellem et virusangreb og sikkerheden på en offentlig webside. Endelig har borgerne også stor tillid til det offentliges behandling af data. Det fremgår af afsnit 2.3.

Det er stadig under 10 procent, der anmelder en hændelse til politiet eller andre offentlige myndigheder.

Virus er altså den trussel, de fleste har været udsat for. På den baggrund er det naturligt, at de ramte reagerer ved at installere sikkerhedssoftware, sandsynligvis i form af antivirusprogrammer.

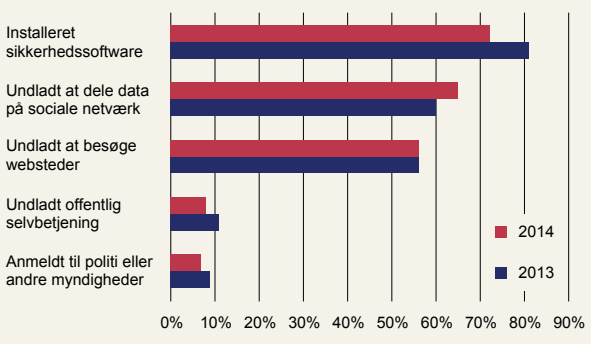
Figur 1

Borgernes oplevede sikkerhedstrusler



Figur 2

Handlinger som reaktion på sikkerhedshændelser



2.3. Kommunikation med det offentlige

Hver fjerde borger har sendt cpr-numre eller andre fortrolige oplysninger i e-mail til det offentlige. Det er på niveau med andelen i 2013. I år har DKCERT endvidere spurgt, om de pågældende borgere har krypteret e-mailen med de fortrolige oplysninger. Her svarer 24 procent ja. 55 procent svarer nej, mens resten ikke ved, hvad krypteret e-mail er.

Tallene viser, at borgerne savner viden om, hvad det er sikkert at sende i en e-mail. Som udgangspunkt bør cpr-numre og andre personfølsomme oplysninger altid sendes krypteret. Ellers er der risiko for, at uvedkommende kan få adgang til oplysningerne ved fx at aflytte et trådløst netværk.

Det er overraskende, at så mange svarer, at de har sendt krypteret e-mail. For at sende en krypteret e-mail skal man fremskaffe modtagerens offentlige nøgle og anvende den til kryptering i e-mailprogrammet. Det er vanskeligt for borgere uden særlig teknisk ekspertise. DKCERT vurderer derfor, at den reelle andel af krypteret e-mail sandsynligvis er langt mindre. En mulig forklaring kan være, at nogle borgere har anvendt andre metoder til krypteret information, fx ved at indsende data via websteder, der anvender kryptering. En anden mulighed er, at brugere af webmail har bemærket, at forbindelsen til webserveren er krypteret, og at de derfor fejlagtigt tror, at deres e-mailkommunikation også er krypteret.

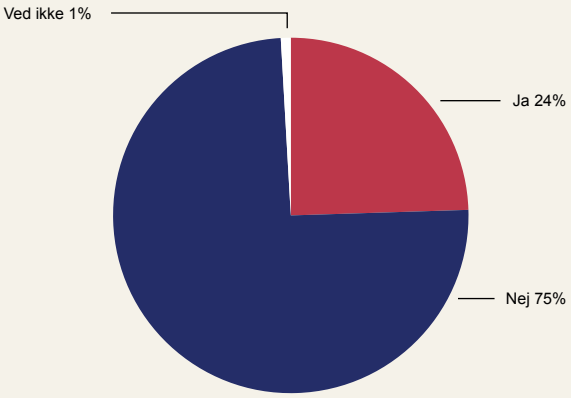
De borgere, der anvender digitale selvbetjeningsløsninger såsom indberetning til SKAT, flytteløsning eller opskrivning til børnepasning, har tillid til, at det offentlige håndterer deres data med den nødvendige fortrolighed og sikkerhed. De der ikke bruger tjenesterne, har lidt mindre tillid. Således er det kun 13 procent af tjenesternes brugere, der udtrykker lille eller meget lille tillid til behandlingen af data. Blandt ikke-brugerne er det 23 procent.

84 procent af borgerne har fra nogen til meget stor tillid til, at det offentlige behandler deres personlige data fortroligt og sikkert.

Den generelt positive holdning til det offentlige afspejles også i, at danskerne er flittige til at bruge websteder fra det offentlige. Ifølge "It-anvendelse i befolkningen" har 81 procent af danskerne besøgt offentlige myndigheders hjemmesider. Gennemsnittet for de 28 EU-lande er 37 procent.

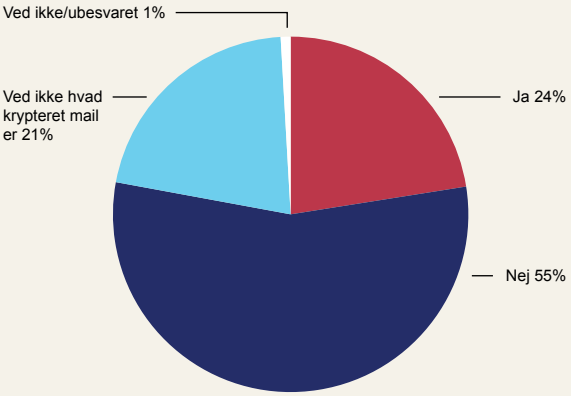
Figur 3

Har du sendt e-mail med cpr-nummer eller anden fortrolig information til offentlige myndigheder?



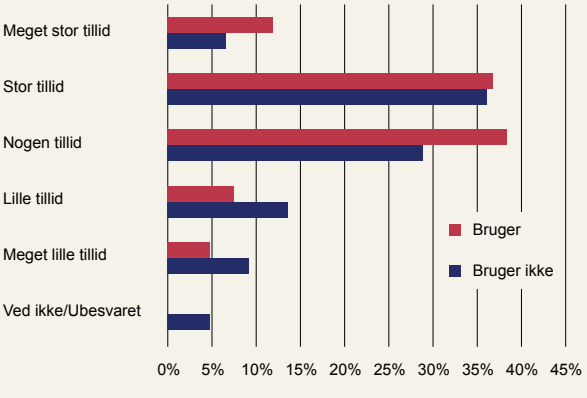
Figur 4

Borgere, der har sendt fortrolige data til myndighederne som krypteret e-mail



Figur 5

Tillid til behandling af data hos brugere og ikke-brugere af digitale selvbetjeningsløsninger



2.4. Privatlivsbeskyttelse på sociale medier

72 procent af deltagerne i undersøgelsen har en profil på sociale medier som Facebook, Twitter, Instagram eller LinkedIn. Dem har DKCERT spurgt om deres kendskab til mediets beskyttelse af personlige oplysninger.

30 procent har læst privatlivspolitikken for det sociale medie, de anvender. 75 procent har manuelt ændret på privatlivsindstillingerne. Og 58 procent mener at vide, hvem der har rettighederne til de billeder, de lægger op på tjenesten.

Det er positivt, at så mange brugere aktivt ændrer på privatlivsindstillingerne. Tallene viser dog ikke, om de har åbnet for øget adgang eller begrænset adgangen til deres personlige data. Men en anden undersøgelse tyder på det sidste: "It-anvendelse i befolkningen" oplyser, at 38 procent af internetbrugerne har afholdt sig fra at afgive personlige oplysninger til sociale medier af sikkerhedsmæssige årsager.

Borgerne er altså bevidste om de konsekvenser for privatlivsbeskyttelsen, det kan have at bruge sociale netværk. Årsagen er sandsynligvis, at emnet jævnligt debatteres. Når Facebook ændrer på netværkets betingelser for brugen, afføder det ofte en stribe kommentarer og bud på formuleringer, der har til formål at afbøde skadevirkningerne.

2.5. Cookies

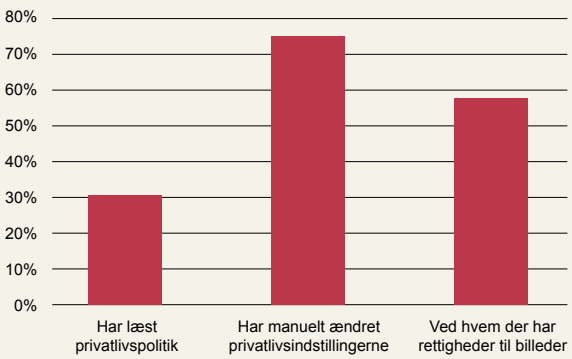
78 procent af deltagerne svarer, at de ved, hvad en cookie er. Ud af dem mener 82 procent, at de er opmærksomme på betydningen af at acceptere en cookie, når de besøger en webside. 60 procent af dem sletter jævnligt cookies og historik i browseren.

Her har EU's såkaldte cookiedirektiv sandsynligvis været med til at øge opmærksomheden. Reglerne medfører, at borgerne jævnligt møder en besked om, at et websted bruger cookies til at spore deres færden. Dermed bliver de cookies, der tidligere var usynlige, gjort synlige.

Når hele 60 procent jævnligt sletter cookies og historik, kan det ses som et tegn på øget bevidsthed om informationssikkerhed og privatlivsbeskyttelse. Om det så også giver borgerne en reel fordel, er mere tvivlsomt. Cookies er kun en af flere metoder til at følge brugernes adfærd. Andre teknikker som skjulte billedfiler, registrering af IP-adresser og fysisk placering bliver anvendt som supplement til eller i stedet for cookies.

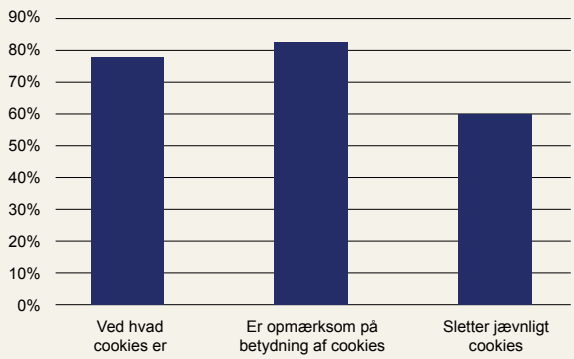
Figur 6

Brugere af sociale netværk og deres kendskab til privatlivsbeskyttelsen



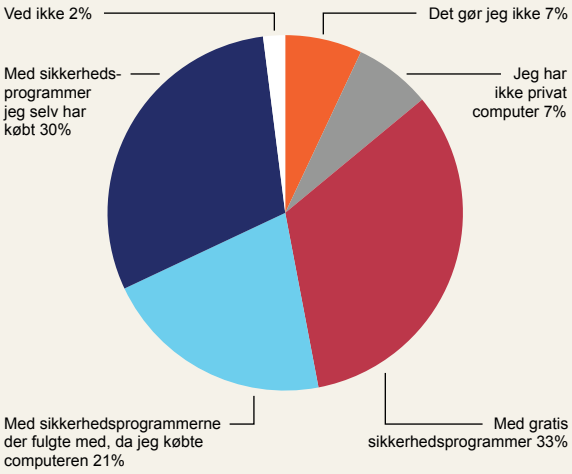
Figur 7

Borgere der kender begrebet cookie



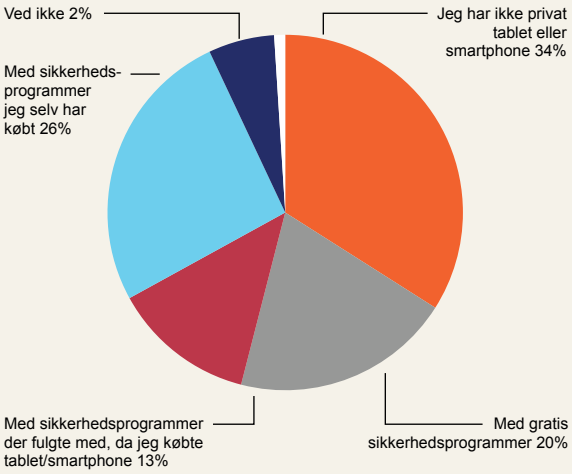
Figur 8

Hvordan beskytter du din private computer og data på den?



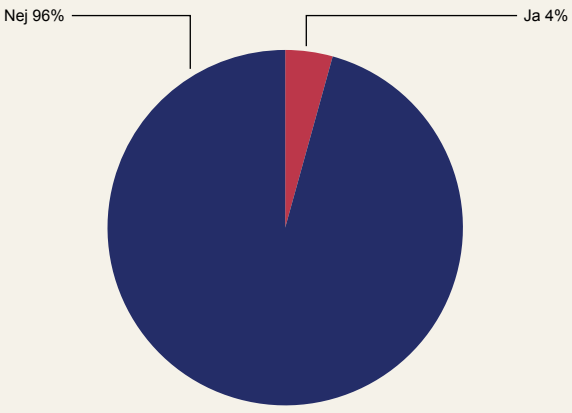
Figur 9

Hvordan beskytter du din smartphone eller tablet?



Figur 10

Har du prøvet at downloade en app eller andet indhold til din smartphone eller tablet, som viste sig at være skadeligt?



2.6. Beskyttelse mod skadelig software

84 procent af borgerne har en eller flere computere, som de beskytter med sikkerhedssoftware. Nogenlunde lige mange anvender gratis sikkerhedsprogrammer og kommercielle produkter. Tallene har stort set ikke ændret sig fra undersøgelsen i 2013.

Mens kun syv procent ikke beskytter deres computer, er det 34 procent, der ikke beskytter deres smartphone eller tablet med sikkerhedssoftware. Den mest almindelige måde at beskytte enheden på er ved hjælp af software, der fulgte med ved købet.

Den lille interesse for antivirus til smartphones og tablets kan hænge sammen med, at brugerne ikke opfatter skadelig software som en reel trussel. Den opfattelse understøtter tallene: Kun fire procent har prøvet at downloade en app eller andet indhold til smartphone eller tablet, der viste sig at være skadeligt. Dog er det muligt, at nogle borgere ikke har opdaget et angreb, netop fordi der ikke kører antivirus på enheden. Men tal fra internationale undersøgelser tyder også på, at smartphones og tablets sjældent bliver inficeret. Det fremgår blandt andet af artiklen "The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers", som et forskerhold fra Georgia Tech udgav i 2013. Forskerne analyserede data fra et stort mobilnetværk for at finde ud af, hvor ofte smartphones og andre enheder på netværket kommunikerede med servere, der bruges til at fjernstyre inficerede enheder. Det viste sig, at under 0,0009 procent af enhederne gjorde det og dermed måtte antages at være inficerede. Så skønt andre statistikker påpeger en voldsom vækst i mængden af skadelig software rettet mod smartphones, ser det ud til, at bagmændene har meget begrænset succes med at få installeret de skadelige programmer hos brugerne.

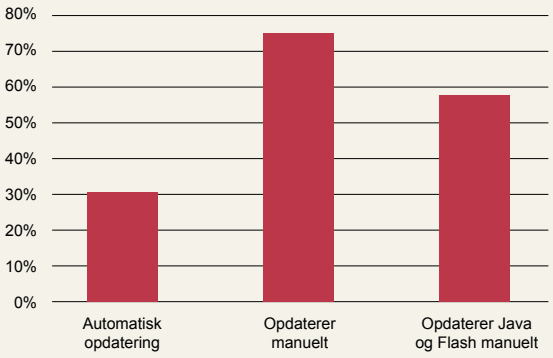
2.7. Opdatering af software

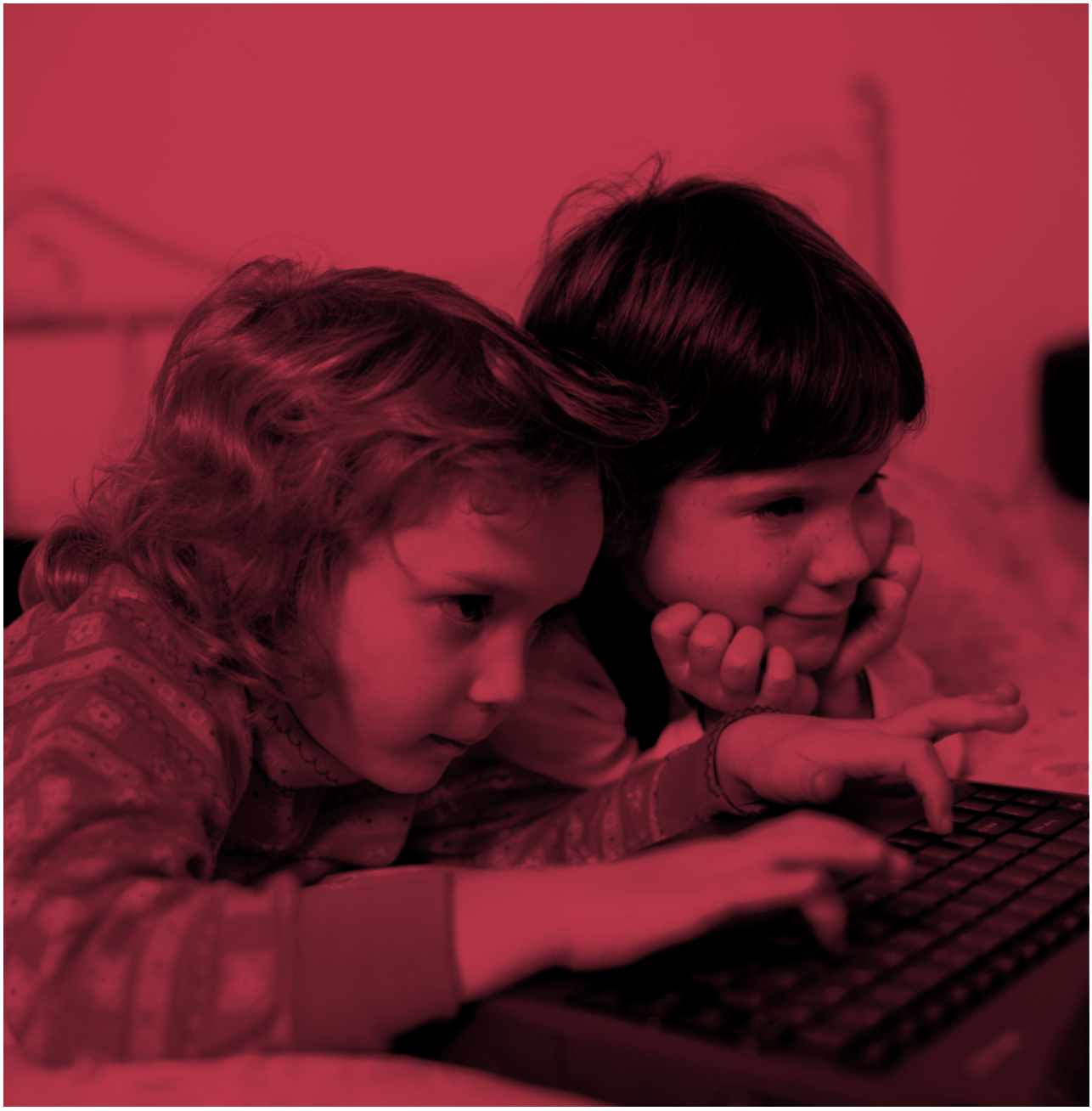
88 procent af deltagerne svarer ja til, at de holder programmerne på deres computer opdateret. Ud af dem har 76 procent slået automatisk opdatering til. 55 procent svarer, at de opdaterer programmer manuelt. Og 79 procent sørger for at opdatere Java og Flash manuelt.

Tallene er positive, da en opdateret computer udgør en langt mindre sikkerhedsrisiko end en med gamle softwareversioner. Det er også positivt, at over halvdelen opdaterer software manuelt, selvom nogle af dem også har slået automatisk opdatering til. Den automatiske opdateringsfunktion opdaterer nemlig ikke alle programmer.

Figur 11

Brugere der holder programmerne på deres pc opdateret





2.8. Sikkerhed på trådløse netværk

Et trådløst netværk kan benyttes af enhver, der er inden for rækkevidde af dets radiosignaler, medmindre det er beskyttet med adgangskode og kryptering. 24 procent oplyser, at de har et trådløst netværk uden adgangskode i deres hjem. Det er en lille stigning i forhold til de 20 procent fra 2013.

En mulig forklaring kan være udbredelsen af smartphones og tablets. Det giver lidt ekstra besvær at skulle indtaste en adgangskode, når netværket skal bruges første gang. Besværet er større, når koden skal indtastes på en enhed uden tastatur. Når gæster i hjemmet gerne vil låne netværket til deres egne enheder, er det også nemmere at give dem adgang uden en adgangskode.

Der er også 24 procent, som bruger trådløse netværk uden adgangskode uden for hjemmet – for eksempel på cafeer, i lufthavne, på hoteller og lignende. Ofte vil et netværk med adgangskode være mere sikkert. Det gælder, hvis det anvender kryptering. Men nogle netværk på hoteller og cafeer kræver en adgangskode, men krypterer ikke kommunikationen.

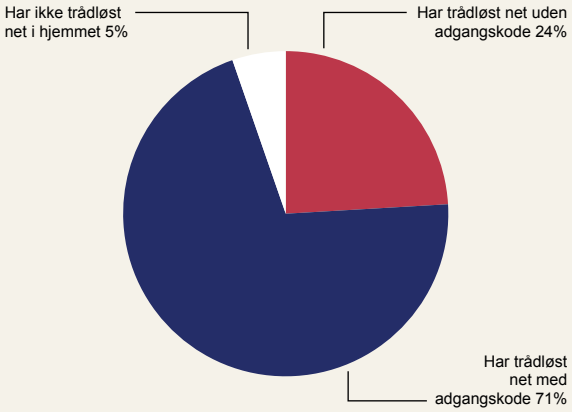
Så en adgangskode er ikke i sig selv bevis for, at kommunikationen er beskyttet. Denne distinktion er borgerne ikke nødvendigvis klar over, medmindre de bemærker, at netværket er markeret som ubeskyttet, når de kobler sig på det på pc'en eller telefonen.

DKCERT har også spurgt borgerne, hvordan koden til deres trådløse netværk er sat op. Her svarer kun fire procent, at det ikke har nogen kode. DKCERT kan ikke forklare uoverensstemmelsen mellem dette tal og de 24 procent, der oplyser, at de ikke bruger adgangskode. Halvdelen af brugerne har selv indtastet en kode, mens 40 procent bruger den kode, udstyret blev leveret med.

Det kan være et sikkerhedsproblem at bruge den kode, som udstyret leveres med. Hvis koden er indstillet af producenten af den trådløse router, vil den ofte være den samme for alle eksemplarer af apparatet. Dermed er den let at gætte. Mange routere leveres dog af internetudbydere og teleselskaber. De udstyrer dem ofte med koder, der er unikke for hver kunde og dermed sværere at gætte.

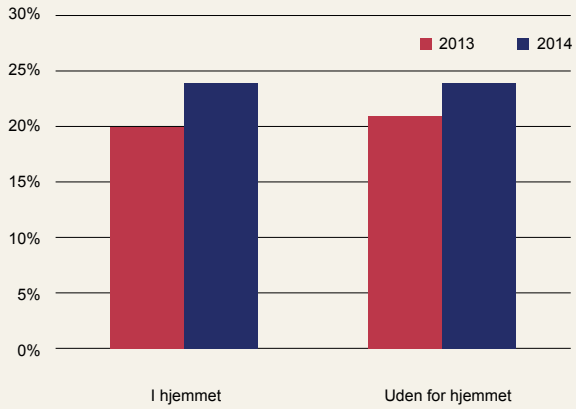
Figur 12

24 procent har usikre trådløse netværk



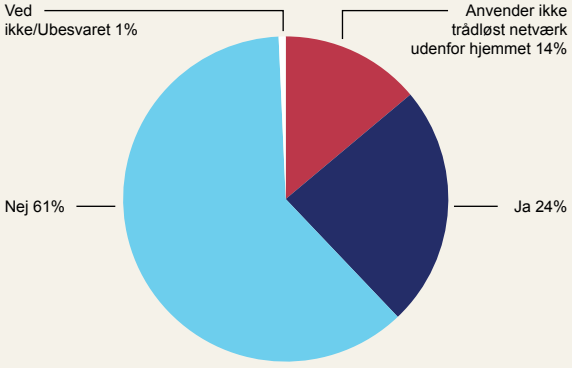
Figur 13

Lidt flere anvender usikre trådløse netværk



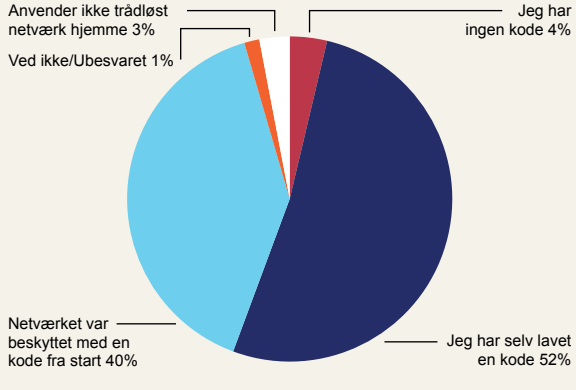
Figur 14

24 procent bruger usikre trådløse netværk uden for hjemmet



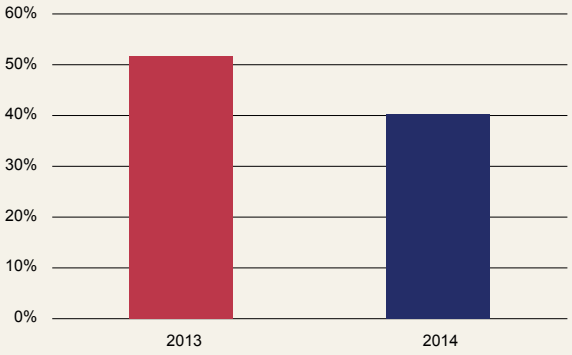
Figur 15

Hvordan er adgangskoden til dit trådløse netværk i hjemmet sat op?



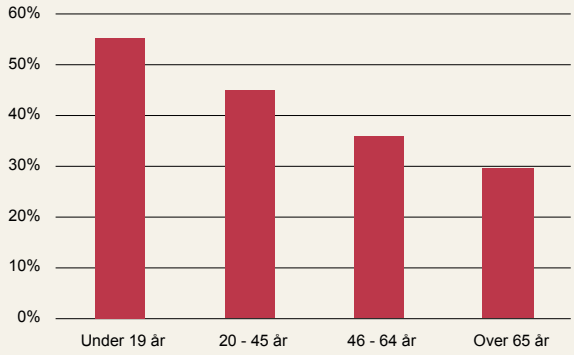
Figur 16

Borgere der anvender samme password til flere onlinetjenester



Figur 17

Genbrug af passwords på tværs af tjenester fordelt efter alder



2.9. Sikkerhed på onlinetjenester

Det giver øget sikkerhed, hvis brugerne anvender forskellige passwords til de forskellige onlinetjenester, de anvender. På den måde får et brud på sikkerheden på én tjeneste ikke konsekvenser for de øvrige tjenester. Hvis brugeren har anvendt samme password til mange tjenester, skal blot en af dem være udsat for en lækage, før angribere kan afprøve passwordet på brugerens øvrige tjenester.

Det er danskerne blevet mere opmærksomme på. I 2013 svarede 52 procent, at de brugte samme kode til flere tjenester. Den andel faldt i 2014 til 41 procent.

Yngre borgere er mest tilbøjelige til at genbruge passwords på tværs af tjenester. Det gør 56 procent af borgerne under 20 år. Hos de ældste i undersøgelsen er det kun 30 procent. En forklaring kan være, at de ældre borgere bruger færre tjenester og derfor har mindre udfordringer med at huske, hvilke koder de har brugt til hvilke tjenester.

2.10. Sikkerhedskopiering

39 procent af borgerne tager jævnligt sikkerhedskopi af data på deres computer. Tallet er uændret i forhold til 2013. 27 procent tager sikkerhedskopi af deres smartphone eller tablet.

Når det gælder metoderne til backup, er der derimod sket nogle ændringer. I 2014 tager 24 procent backup på nettet via cloud-løsninger. I 2013 var det 19 procent. Tilsvarende er der færre, som kopierer til en ekstern harddisk eller USB-nøgle: 62 procent mod 70 procent året før.

En årsag til bevægelsen mod cloud er sandsynligvis, at det er mindre krævende. En cloud-backup kan foregå automatisk i baggrunden, mens brugeren selv aktivt skal slutte sin eksterne harddisk til og starte backupproceduren ved den anden metode.

Kun 27 procent tager sikkerhedskopi af data på deres smartphone eller tablet. Det er lidt færre end i 2013, hvor 29 procent gjorde det. Årsagen kan være, at flere har anskaffet en smartphone eller tablet, og at de endnu ikke har oplevet problemer med tab af data fra dem.

De der sikkerhedskopierer deres smartphone eller tablet, gør det primært via cloud-backup. 13 procent kopierer data over til en computer. Det er næsten en halvering i forhold til 2013, hvor 24 procent brugte den metode. Kopiering til ekstern harddisk eller USB-nøgle er også faldet lidt.

2.11. Evne til at beskytte sig

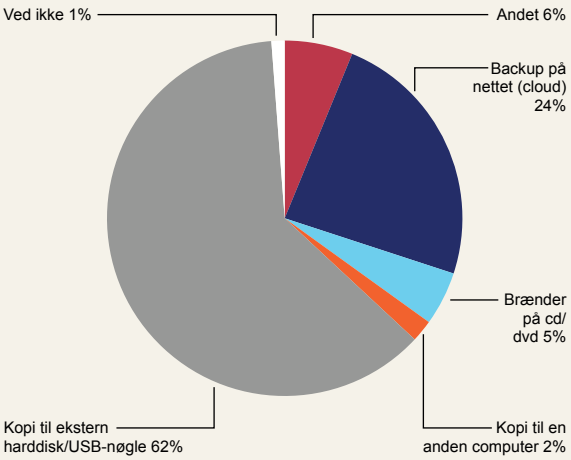
Flere borgere føler sig i stand til at beskytte sig mod virus og andre skadelige programmer. I 2013 svarede 70 procent, at de mente, de kunne beskytte sig mod den form for trusler. I 2014 sagde 85 procent ja til samme spørgsmål.

Tallet svarer fint til, at "It-anvendelse i befolkningen" oplyser, at 86 procent af internetbrugerne anvender sikkerhedsprogrammer såsom antivirus.

Der er også mindre stigninger i mængden af borgere, der ser sig i stand til at beskytte sig mod phishing og e-mails med vedhæftede filer eller links. Der er dog stadig 57 procent, som ikke ved, hvad phishing er. Det kan undre, da der de senere år har været en del medieomtale af phishing og advarsler mod det.

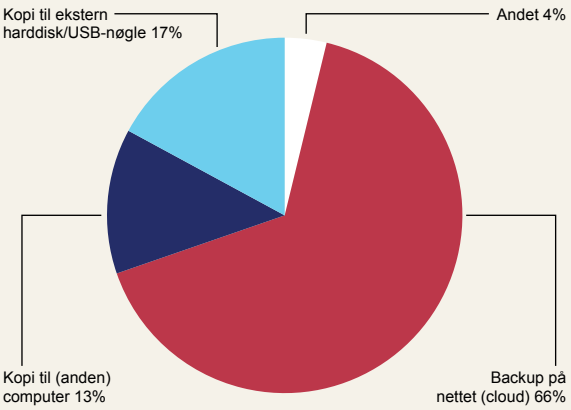
Figur 18

Metoder til sikkerhedskopiering af computer



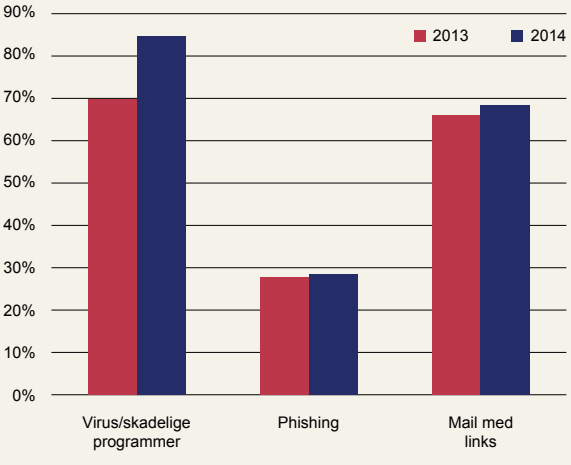
Figur 19

Metoder til sikkerhedskopiering af smartphone/tablet



Figur 20

Borgere der kan beskytte sig mod bestemte trusler



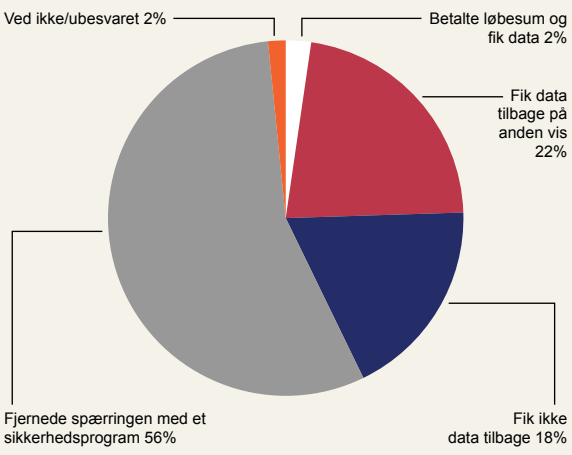
2.12. Angreb med ransomware

Verden over er der det seneste par år set en stigning i angreb med såkaldt ransomware. Det er skadelig software, der spærrer for adgangen til en computer. Nogle varianter krypterer data på harddisken med en hemmelig nøgle. Bagmændene kræver løsepenge for at udlevere nøglen, så offeret kan få adgang til sine data igen.

Otte procent af deltagerne i undersøgelsen havde været udsat for ransomware. Over halvdelen af dem slap imidlertid for at betale løsesummen: De brugte et sikkerhedsprogram til at få adgang til data igen og fjerne ransomwareprogrammet. Kun to procent af ofrene betalte løsesummen. 18 procent fik aldrig deres data tilbage.

Figur 21

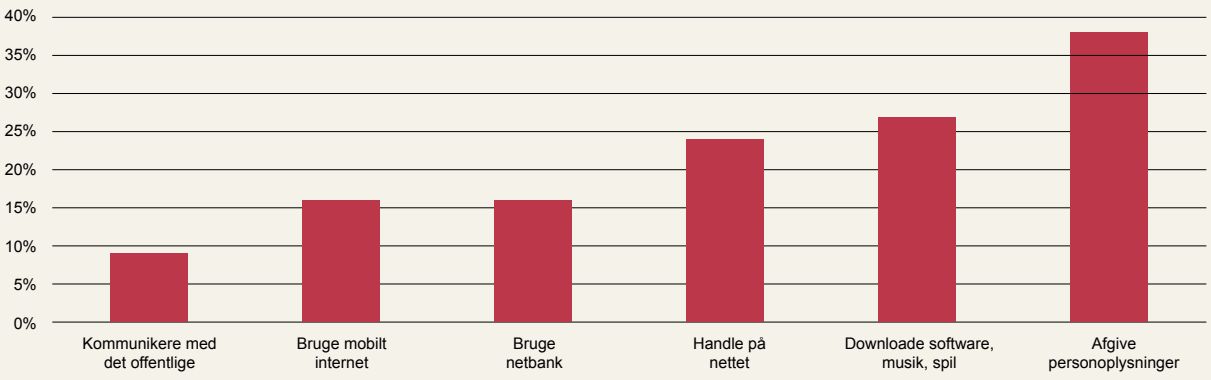
Metoder til at få data tilbage efter angreb med ransomware

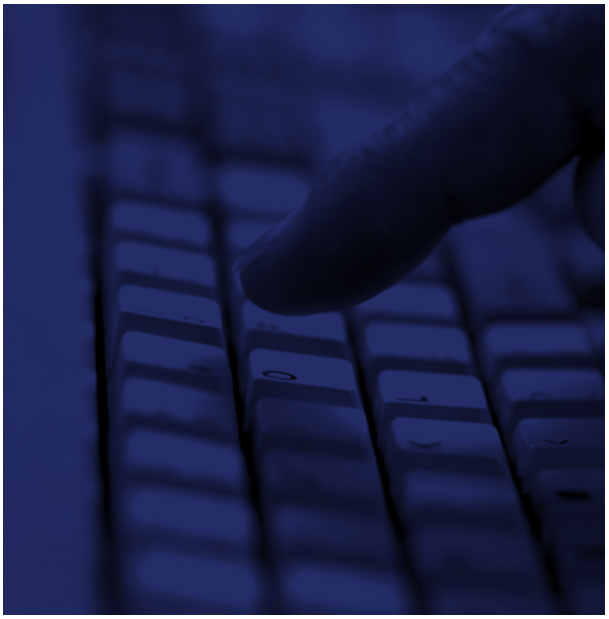


3. Øvrige data

”It-anvendelse i befolkningen” har spurgt internetbrugere mellem 16 og 89 år, om bekymringer for sikkerheden har afholdt dem fra at udføre bestemte handlinger. Ni procent har undladt at kommunikere med det offentlige, mens hele 38 procent har undladt at afgive personoplysninger til sociale netværk.

Figur 22
Andel af internetbrugere, der har undladt at udføre disse handlinger på grund af bekymringer om sikkerheden
Kilde: ”It-anvendelse i befolkningen”





4. Konklusioner

4.1. Sikkerhed på pc'en

Undersøgelsen viser, at danskerne har godt styr på informationssikkerheden, når det gælder deres private computere. Over 80 procent beskytter således deres computer med antivirusprogrammer og andre typer sikkerhedsprogrammer. 88 procent sørger for at holde programmerne på deres computer opdateret. Sikkerhedsprogrammer og softwareopdateringer er to af de vigtigste midler mod infektion med skadelige programmer eller angreb udefra.

Når det gælder tab af data, er danskerne derimod dårlige til at beskytte sig. Kun 39 procent tager jævnligt sikkerhedskopi af data på deres computer. Tallet er stort set uændret i forhold til 2013. Der kan dog være en positiv udvikling på vej: Flere tager sikkerhedskopi via tjenester på internettet (cloud-backup) i stedet for at gøre det manuelt med en ekstern harddisk. Det har den fordel, at det er mere sandsynligt, at sikkerhedskopien er opdateret. Cloud-systemerne tager typisk kopier løbende, så man højst risikerer at miste filer fra de seneste timer. Med en ekstern harddisk skal brugeren huske at slutte den til for at starte sikkerhedskopieringen. Derfor går der ofte dage eller uger imellem, at det sker.

Der er stor aldersmæssig spredning, når det gælder sikkerhedskopiering. Aldersgruppen 20-45 år er bedst til at tage sikkerhedskopi, mens både de yngste og de ældste i undersøgelsen ligger meget lavt.

4.2. Sikkerhed på trådløse netværk

Hver fjerde dansker bruger usikre trådløse netværk. Det udgør en alvorlig sikkerhedsrisiko. Et netværk uden adgangskode er ikke beskyttet med kryptering. Det betyder, at enhver der er inden for rækkevidde af radiosignalerne, kan opsnappe informationer sendt af andre på samme netværk.

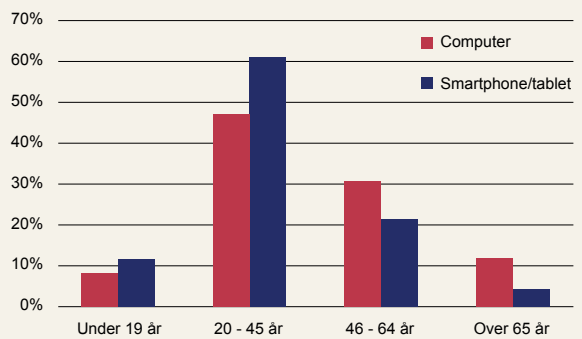
Trådløse netværk uden adgangskode udgør en ekstra risiko på smartphones og andet mobilt udstyr. Når enheden én gang har været tilsluttet et bestemt netværk, husker den det og kobler sig automatisk på det, næste gang det er i nærheden. Det kan angribere udnytte. Enheden udsender nemlig jævnligt signaler, hvor den spørger, om et af de kendte netværk er i nærheden. Angriberens udstyr kan svare med netværkets navn. Derefter kobler enheden sig til angriberens udstyr. Nu kan angriberen udføre et man-in-the-middle-angreb, der opsnapper alle data mellem offerets enhed og de servere, den kommunikerer med. Det kan man beskytte sig imod ved at sætte enheden til at glemme netværket, når man er færdig med at bruge det.

4.3. Sikkerhed på smartphones

Smartphones og tablets er en nyere teknologi end pc'er. Det medfører, at borgerne er mindre opmærksomme på sikkerhedskravene – de har ikke opbygget de samme gode vaner med sikkerhedsprogrammer, som de har på pc-siden. Det fremgår af, at kun 45 procent beskytter deres smartphone eller tablet med sikkerhedssoftware. Behovet ser dog heller ikke ud til at være så stort: Kun fire procent har prøvet at downloade en app eller andet indhold, der var skadeligt.

Figur 23

Sikkerhedskopiering fordelt på aldersgrupper



4.4. Ransomware

Otte procent af deltagerne i undersøgelsen har været udsat for ransomware. Det er ganske mange i betragtning af, hvor udbredt sikkerhedssoftware er. Årsagen kan enten være, at ransomware-programmet er sluppet forbi et antivirusprogram, eller at pc'en ikke var beskyttet med antivirus.

Ud af de ramte er det kun to procent, der har valgt at betale løsesummen og få data tilbage. 18 procent fik ikke deres data tilbage.

Tallene viser, at truslen fra ransomware bør tages alvorligt. Den er ikke katastrofalt stor, men den er til at få øje på. Halvdelen af de ramte fjernede ransomware med sikkerhedsprogrammer. Den andel venter DKCERT vil falde i de kommende år, efterhånden som bagmændene udvikler mere effektive ransomware-programmer med stærkere kryptering.

4.5. Privatlivsbeskyttelse og datasikkerhed

41 procent bruger samme adgangskode til flere onlinetjenester. Det indebærer en øget risiko for deres informationssikkerhed. Til gengæld kan man glæde sig over, at andelen er faldet fra 52 procent i 2013.

Stadig flere tjenester på nettet tilbyder to-faktor-autentifikation. Det betyder, at brugeren foruden brugernavn og adgangskode for eksempel også skal oplyse en engangskode, når vedkommende bruger en ny enhed til at koble sig på tjenesten. Engangskoden kan ofte have form af en sms-besked eller en talkode, der genereres af en app. Den kan også have form som det nøglekort, de fleste NemID-brugere anvender. DKCERT mener, at to-faktor-autentifikation mindsker risikoen for misbrug af personlige data væsentligt.

Kun 24 procent har sendt fortrolige data såsom cpr-numre til det offentlige via e-mail. Ud af dem oplyser en fjerdedel, at de har anvendt krypteret e-mail. De øvrige har dermed sendt data ukrypteret. Det udgør især en risiko, hvis mailen er sendt over et usikkert trådløst netværk, så uvedkommende kunne opsnappe den.

21 procent af dem, der har sendt fortrolige oplysninger til det offentlige, ved ikke, hvad krypteret e-mail er. Dermed tyder tallene på, at en stor del af borgerne ikke er klar over de risici, som det medfører at sende e-mails ukrypteret.
Borgerne har generelt høj tillid til, at det offentlige behandler deres data korrekt, både når det gælder sikkerhed og fortrolighed. Tilliden er lavest hos dem, der ikke anvender offentlige selvbetjeningsløsninger.

4.6. Opsamling

Borgerne har god informationssikkerhed på deres pc'er, når det gælder sikkerhedssoftware og opdateringer. De savner at få styr på sikkerhedskopiering på både pc'er og andre enheder.

På smartphones og tablets bruger hver tredje ikke antivirus. Da virus ikke er udbredte på platformene, er det ikke nødvendigvis et alvorligt problem.

Hver fjerde borger bruger trådløse netværk på en usikker måde.

57 procent ved ikke, hvad phishing er. Det er dog muligt, at de blot ikke kender betegnelsen, men ved, hvad den dækker over (websteder der prøver at lokke fortrolige oplysninger fra ofrene ved at give sig ud for at være nogen, de har tillid til). Flertallet har god forståelse for de konsekvenser for privatlivsbeskyttelsen, som det kan have at bruge sociale netværk.

Et stort flertal har tillid til, at det offentlige behandler deres data sikkert og fortroligt.

5. Anbefalinger til borgerne

Ud fra resultaterne af undersøgelsen har Digitaliseringsstyrelsen og DKCERT disse anbefalinger til borgerne. Formålet er at øge deres informationssikkerhed.

1. Brug sikkerhedssoftware som antivirus og firewall.
2. Hold programmer opdateret.
3. Tag sikkerhedskopi af dine data.
4. Undlad at klikke på links i e-mails, du får tilsendt uopfordret.
5. Undersøg adressen på et websted, før du udfylder formularer med fortrolige oplysninger. Oplys generelt kun fortrolige oplysninger på netsteder, du har tillid til.
6. Beskyt dit trådløse netværk med adgangskode.
7. Undgå at sende følsomme data over åbne trådløse netværk (netværk uden kryptering).
8. Brug VPN (virtuelt privat netværk), når du bruger åbne trådløse netværk.
9. Kontroller at det trådløse netværk, du kommunikerer med, ikke er en efterligning.
10. Hvis du har brugt et åbent trådløst netværk, så sæt din telefon/computer til at glemme det.
11. Brug forskellige passwords til alle tjenester. Du kan evt. holde styr på dine passwords med et password manager-program.
12. Slå to-faktor-autentifikation til på web-tjenester.
13. Indstil privatlivsindstillingerne på sociale netværk, så de passer til dine krav.
14. Oplys ikke fortrolige og personlige oplysninger på sociale netsteder, debatsider og chatrum.

6. Kilder

It-anvendelse i befolkningen, Danmarks Statistik, 2014:
http://www.dst.dk/pubpdf/18686/itbef

The Core of the Matter: Analyzing Malicious Traffic in Cellular Carriers, Georgia Tech, 2013:
http://www.cc.gatech.edu/~traynor/papers/lever-ndss13.pdf

DIGITALISERINGSSTYRELSEN

DKCERT

DeiC DANISH e-INFRASTRUCTURE COOPERATION