Sikkerhedsrisici ved mobilbetaling
Borgernes informationssikkerhed

Rapport til Digitaliseringsstyrelsen 2013

DeiC

DKCERT

Sikkerhedsrisici ved mobilbetaling
Borgernes informationssikkerhed

Redaktion: Shehzad Ahmad og Torben B. Sørensen

Grafik og layout: Torben B. Sørensen

Rapporten er udarbejdet af DKCERT for Digitaliseringsstyrelsen

DKCERT, DeIC
DTU, Centrifugevej, Bygn. 356
2800 Kgs. Lyngby

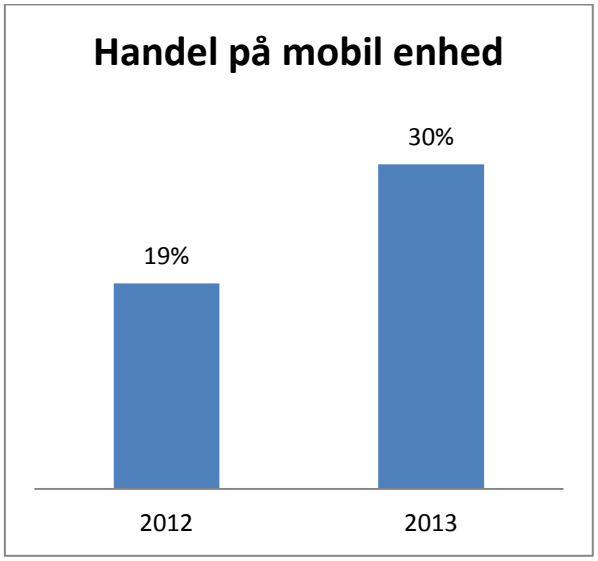
Indhold

1.Sikkerhedsrisici ved mobilbetaling

1.1. Indledning

I 2013 tog danskerne for alvor muligheden for at betale med mobiltelefonen til sig. Betalingsformidleren DIBS (Dansk Internet Betalings System) registrerede, at 423.000 nye forbrugere anvendte smartphones eller tablets til at foretage indkøb[1]. Dermed har næsten hver tredje danske forbruger handlet via en mobil enhed (se Figur 1). Undersøgelsen omfatter alle former for mobil handel, fx betaling med kreditkort i browseren på en tablet eller køb af busbillet via en app. Også Danske Bank melder om stor interesse for bankens MobilePay-løsning til overførsel af penge mellem smartphones.

For forbrugeren er der tale om en mobilbetaling, når betalingen foregår ved hjælp af mobiltelefonen. Finanssektoren har en mere begrænset definition, hvor man for eksempel ikke regner det for en mobilbetaling, når brugeren indtaster sit betalingskortnummer på en mobil webside. I denne rapport anvender vi den brugerorienterede definition, hvor en mobilbetaling er enhver betaling, som brugeren foretager ved hjælp af telefonen eller en tabletcomputer.



Figur 1: 30 procent af forbrugerne svarer ja til, at de har handlet med en smartphone eller tablet. Kilde: DIBS E-handel 2013.

Som ved andre finansielle transaktioner er sikkerhed afgørende ved mobile betalinger. De involverede parter i transaktionen skal have sikkerhed for, at betalingen når frem. Og løsningerne skal være sikret, så uvedkommende ikke kan misbruge dem til at overføre penge til sig selv.

I det følgende beskriver vi først det generelle forløb, når en kunde køber en vare, der betales med et betalingskort. Det skyldes, at mange mobilbetalinger reelt er kortbetalinger, selvom kunden ikke fysisk anvender sit betalingskort. Derefter gennemgår vi de sikkerhedsaspekter, der er fælles for alle former for mobilbetaling, før vi kommer ind på de forskellige løsninger.

1.1.1. Online betaling med betalingskort

Der indgår typisk mindst fire parter i et køb med betalingskort: En kunde, en butik, en payment service provider (PSP) og en indløser. Forløbet er gerne således:

1. Kunden vælger sin vare i en online butik. Det foregår i butikkens it-system via en webside.
2. Kunden går til betaling. Nu åbnes en webside hos PSP'en.
3. Kunden indtaster kortnummer, udløbsdato og sikkerhedskode hos PSP'en.
4. PSP'en kontrollerer strukturen af kortdata og sender transaktionen til validering hos indløseren.
5. I de fleste tilfælde sender indløseren transaktionen til kundens bank for kontrol af fx dækning eller spærring.
6. PSP'en sender besked til butikken om, at dataene og dermed betalingen er godkendt.
7. Kunden får bekræftelse på, at købet er gennemført.
8. Forretningen anmoder via PSP'en sin indløser om udbetaling, når forretningen har afsendt varen til kunden.

Forløbet er det samme, hvad enten købet foregår hjemme foran skærmen eller ude med en smartphone. Dermed er reglerne for erstatningsansvar og tilbageføring af betalinger de samme for mobilhandel som ved internethandel, når betalingskort er involveret.

[1] DIBS, 1-12-2013

1.1.2. Generelle risici ved mobile betalinger

Uanset løsningen er der en række risici, som gælder for alle metoder til mobilbetaling:

1. Enheden kan blive stjålet.
2. Uvedkommende kan bruge enheden.
3. Uvedkommende kan aflure indtastninger.
4. Uvedkommende kan opsnappe data trådløst.
5. Uvedkommende kan inficere enheden med skadelige programmer.

Risikoen for at enheden bliver stjålet, er højere, jo mere mobil en enhed er. Tyveri af en stationær computer kræver som regel, at tyven bryder ind hos offeret og fjerner pc'en. En bærbar pc kan blive stjålet sammen med den taske, den ligger i. Men på grund af størrelsen er risikoen for tyveri endnu større ved mobiltelefoner – en telefon kan stjæles fra en lomme eller taske i et ubevogtet øjeblik.

Hvis telefonen bliver efterladt, risikerer man, at uvedkommende bruger den. Hvis en app til pengeoverførsler er åben, kan personen overføre penge til sig selv.

Selv når brugeren har telefonen i hånden, er der risiko for, at andre kan kigge over skulderen. På den måde kan en angriber se passwords og andre koder, som brugeren indtaster. Dem kan angriberen udnytte, hvis han senere stjæler telefonen.

Angribere kan opsnappe den trådløse kommunikation, hvis smartphonen anvender Wi-Fi på et netværk uden kryptering.

Skadelige apps kan som regel kun installeres, hvis det lykkes angriberen at narre sit offer til at gøre det. Det sker som oftest ved at forklæde det skadelige program som en app, kunden er interesseret i. Skadelige apps kan for eksempel sende sms'er fra den inficerede smartphone, opsnappe fortrolige data eller bruge mikrofon og kamera til at optage offerets samtaler. I udlandet er der observeret flere skadelige apps, der angriber to faktor-autentifikation via sms: Appen kan opsnappe en sms, som indeholder en kode, brugeren skal indtaste i netbank på computeren for at godkende en transaktion[2]. Da bankerne i Danmark anvender NemID, som ikke bruger sms-autentifikation, udgør det ikke en risiko for traditionelle netbanker – men kan gøre det for mobilbanker, se afsnit 1.2.6.

[2] NSS 11-12-2013

1.1.3. Generelle forholdsregler

De følgende forholdsregler kan bruges til at mindske de generelle risici ved mobilbetaling.

1. Opbevar enheden sikkert, for eksempel i en inderlomme med lynlås.
2. Lås enheden med en kode, der skal indtastes eller angives på anden måde, før man får adgang til at bruge den.
3. Installer sikkerhedssoftware, der gør det muligt at slette data på afstand, hvis enheden bortkommer eller bliver stjålet. Den type program kan også hjælpe med at lokalisere enheden.
4. Gem kvitteringer og tjek kontoudtog. Gør indsigelse, når der optræder en transaktion, der ikke kan genkendes.
5. Betal med et internationalt betalingskort for at opnå den bedst mulige forbrugerbeskyttelse.
6. Hent kun apps fra de reglementerede app stores.
7. Installer sikkerhedssoftware, der beskytter mod skadelige apps.
8. Mister man enheden, skal man hurtigst muligt få spærret de betalingsløsninger, der er knyttet til den. Man skal også spærre selve mobilabonnementet.

1.2. Løsninger til mobilbetaling

Mobile betalinger bygger på teknologier, der i forvejen er kendt fra især webverdenen. Men når det bliver muligt at betale med mobilen, opstår der nye sikkerhedsudfordringer. I det følgende gennemgår vi nogle af de mobile betalingsmuligheder på det danske marked ud fra en sikkerhedsvinkel.

DKCERT har identificeret følgende metoder til betaling med en mobiltelefon/smartphone eller tablet. Listen bygger blandt andet på Betalingsrådets Rapport om nye betalingsformer[3]. Der findes utvivlsomt flere metoder, men de vil ofte være varianter af følgende teknologiske løsninger.

1. Betaling af en ydelse med en app til formålet.
2. Overtakserede sms'er.
3. Mobilpenge.
4. Pengeoverførsel mellem to smartphones (Swipp/MobilePay).
5. Betaling på mobil-tilpassede websider.
6. Pengeoverførsel i mobil netbank.
7. Digitale tegnebøger som apps.
8. Kortbetaling med smartphones med NFC.

[3] Betalingsrådet, november 2013

Alle ovenstående metoder anvendes i Danmark i dag bortset fra nummer 8. Da det er en oplagt mulighed i fremtiden, har vi valgt også at gennemgå dens sikkerhedsaspekter.

1.2.1. Betaling af en ydelse med en app

Bilen er parkeret, og nu skal der betales for parkeringen. Brugeren finder sin smartphone frem, åbner parkeringsselskabets app og betaler. Det er et eksempel på en app, der er målrettet til betaling af en enkeltydelse. Andre eksempler er apps til køb af billetter til bus eller tog.

Der findes to typer apps til smartphones og tablets: Native apps og hybride apps. En native app er programmeret til den enkelte platform (for eksempel Android eller iOS). En hybrid app er en app, hvor dele er skrevet til platformen, men hvor meget af indholdet vises som websider inde i appen. Endelig taler nogle også om web-apps, men i praksis er de ikke apps, men websteder skræddersyet til mobilbrug. Dem gennemgår vi nedenfor under punkt 1.2.5.

Betalingen i en hybrid app foregår ligesom en kortbetaling på et almindeligt websted (se afsnit 1.1.1). Dermed er den også omfattet af de gængse regler for internethandel.

Hvis betalingen foregår i en native app, har udviklerne indlejret en betalingsfunktion. Det kan ske på flere måder: Udviklerne kan anvende et programmeringsbibliotek, der håndterer betalingsdelen, eller de kan sende betalingsoplysningerne til en webside hos en PSP. I det førstnævnte tilfælde kan systemet udarbejdes, så det lever op til de krav, de internationale kortudstedere stiller. Disse krav er formuleret i specifikationen Payment Card Industry Data Security Standard (PCI DSS)[4]. Det handler blandt andet om, at butikken ikke ser brugerens kortnummer og sikkerhedskode. Kun PSP'en har adgang til de data.

Den danske PSP DIBS oplyser til DKCERT[5], at der er et sikkerhedsproblem i en række betalingsapps på det danske marked: Hvis appen sender betalingsdataene til PSP'ens webside i stedet for at modtage dem via funktionerne i et programmeringsbibliotek, kan det indebære, at brugeren først indtaster dataene i appen. Så befinder dataene sig i en periode i butikkens app. Dermed overholder appen ikke kravene i PCI-DSS.

Det kan give problemer for butikken, hvis den bliver udsat for audit fra indløserens side. Hvis butikken bliver udsat for et hackerangreb, risikerer den at miste data om kundernes betalingskort. Det kan i sidste ende give kunderne problemer. Foreløbig har denne risiko kun været teoretisk i Danmark, der kendes ikke til eksempler på misbrug.

1.2.1.1. Forholdsregler

Man kan anbefale kunder kun at betale i apps, der er hybride eller udviklet i henhold til PCI DSS. I praksis er det dog ikke muligt for den almindelige bruger at afgøre, hvordan betalingen foregår. Da risikoen for at miste data på den måde foreløbig må anses for ret teoretisk, har DKCERT valgt ikke at anbefale den forholdsregel. Men brugere bør altid være opmærksomme på, hvem der står bag de apps, de installerer.

Det er vigtigt, at apps anvender krypteret kommunikation (HTTPS/SSL). Men også det kan være svært for forbrugeren at afgøre. Her må man trække på evalueringer fra tredjeparter, der for eksempel undersøger appens kommunikation og lagring af fortrolige data.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 1.1.3.

1.2.2. Overtakserede sms'er

Betaling med en sms er nok den ældste og mest afprøvede metode til mobilbetaling. Kunden sender en sms til et telefonnummer, som butikken oplyser. Butikken sender en sms retur til kunden. Først når kunden besvarer den, gennemføres betalingen.

Det er som regel et teleselskab, der står for betalingsløsningen. Dermed foregår afregningen over teleregningen. Ud over kunde, butik og teleselskab kan der også indgå en såkaldt indholdsaggregator i løsningen. Det er en virksomhed, der står for grænseflade og applikationer til brug ved betalingen.

En risiko ved sms-betaling er, at en angriber kan bestille varer i en andens navn. DKCERT vurderer, at metoden med at kræve en bekræftelse, før betalingen gennemføres, normalt er tilstrækkelig til at forhindre den type misbrug.

Skadelige programmer (malware) udgør en særlig risiko i forbindelse med sms-betalinger. Bagmænd

[4] PCI DSS
[5] DIBS, 3-12-2013

kan oprette overtakserede telefonnumre. Derefter inficerer de offerets smartphone med malware. Bagmændene fjernstyrer det skadelige program til at sende sms'er uden brugerens vidende. Først når teleregningen skal betales, opdager offeret misbruget.

Den type malware er primært observeret i Østeuropa. Det skyldes, at det i de lande er forholdsvis let at oprette et overtakseret nummer. Samtidig er brugerne her også mere tilbøjelige til at hente apps fra andre steder end de reglementerede app stores[6]. Derimod kender DKCERT ikke til angreb rettet specifikt mod danske kunder med overtakserede numre oprettet i Danmark.

1.2.2.1. Forholdsregler

Brugerne skal kun bekræfte sms-køb, de selv har taget initiativ til. DKCERT anbefaler, at man beskytter sin smartphone mod skadelige programmer ved kun at hente apps fra reglementerede app stores, vurdere apps kritisk og eventuelt installere antivirus på smartphonen.

Hvis telefonen bliver stjålet eller bortkommer, skal man lukke for mobilabonnementet, så uvedkommende ikke kan misbruge telefonen til sms-betaling.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 1.1.3.

1.2.3. Mobilpenge

Mobilpenge er et betalingsmiddel, hvor brugeren med sms eller via en app kan betale for varer eller tjenesteydelser. Det betalte beløb trækkes fra den bankkonto, som er tilknyttet ordningen. Her adskiller Mobilpenge sig fra traditionelle overtakserede sms'er, hvor beløbet trækkes fra teleregningen. Mobilpenge er udviklet af Nets og de danske pengeinstitutter. Foreløbig understøtter kun få butikker systemet.

Kunden kan højst bruge Mobilpenge for 1.500 kroner pr. dag. Dette maksimum er med til at begrænse risikoen for misbrug – gevinsten er forholdsvis lille for en angriber. I øvrigt skal enhver butik, der tager mod Mobilpenge, modtage en separat bekræftelse, før den må opkræve beløbet.

Risiciene ved Mobilpenge, når det anvendes til sms-betaling, er de samme som ved sms-betaling (se afsnit 1.2.2).

Når det gælder Mobilpenge som app, er der de samme risici som ved andre apps (se afsnit 1.2.1).

1.2.3.1. Forholdsregler

Hvis enheden bliver stjålet eller forsvinder, skal man spærre mobilnummerets tilknytning til bankkontoen hurtigst muligt. Det sker hos pengeinstituttet[7].

Kunden kan overveje at sætte et lavere dagligt maksimumbeløb, der må hæves via Mobilpenge.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 1.1.3.

1.2.4. Pengeoverførsel mellem to smartphones (Swipp/MobilePay)

I 2013 lancerede danske pengeinstitutter to tjenester til mobilbetaling: Danske Bank kom med MobilePay, mens de øvrige pengeinstitutter står bag Swipp. Løsningerne fungerer stort set på samme måde: Betaleren åbner appen og indtaster en personlig kode for at få adgang til den. Derefter indtastes beløbet samt modtagerens mobilnummer. Der kræves kun, at begge parter har appen, de får ikke oplyst hinandens kontonumre eller betalingskortnumre.

I MobilePay hæves beløbet på betalerens betalingskort. Derfor skal der være et betalingskort tilknyttet ordningen. Pengene overføres til modtageren som en konto til konto-overførsel. Brugeren kan overføre op til 1.500 kroner dagligt, dog højst 50.000 kroner om året.

I Swipp foregår betalingen som en ren konto til konto-overførsel. Kunden kan maksimalt overføre 3.000 kroner pr. dag, men kan aftale et lavere beløb med pengeinstituttet.

MobilePay er den mest brugte af de to løsninger. I starten af december blev der hver dag i gennemsnit gennemført 35.000 overførsler med MobilePay. Siden åbningen har danskerne overført over 550

[6] CSO Online, 7-09-2012

[7] Nets, 26-11-2013

millioner kroner med løsningen – typisk ved mindre overførsler på i snit 225 kroner[8].

I dag er løsningen beregnet til overførsel mellem private. Danske Bank er i gang med at udvikle en egentlig betalingsløsning. Den kan få form af en app målrettet til virksomheder, der vil tage betaling ad den vej.

Figur 2: Swipp-funktionen er her indbygget i en mobilbank-applikation fra Finansnetbanken.

Den største risiko ved løsningerne er, at en angriber får fat i telefonen og misbruger den til betalinger. Her er beløbsbegrænsningen med til at mindske risikoen for misbrug. Danske Bank oplyser, at banken har haft meget lidt svindel med løsningen, og at den svindel, der har været, ikke har været som led i noget, der ligner organiseret kriminalitet[9].

I tilfælde af misbrug er forbrugeren dækket på samme måde, som hvis der var tale om et køb med kort. Hvis der er tale om misbrug, kan det fulde beløb derfor blive refunderet.

1.2.4.1. Forholdsregler

Betaleren skal indtaste en firecifret kode for at komme ind i MobilePay. DKCERT anbefaler, at denne kode ikke er den samme som den, man anvender til at låse telefonen op med.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 1.1.3.

[8] Danske Bank, 11-12-2013
[9] Danske Bank, 4-12-2013

1.2.5. Betaling på mobil-tilpassede websider

En betaling på en webside, der vises på mobilen, svarer fuldstændig til en betaling på en webside, der vises på en computer. Derfor er risiciene de samme: Man risikerer at købe hos en fupbutik, der aldrig leverer varen, eller at butikken trækker et større beløb, end man har indtastet. Her er forbrugeren dækket på samme måde som ved anden internethandel.

Når indtastningen foregår på en smartphone eller tablet, er der nogle ekstra risici. Hvis det foregår på et offentligt sted, for eksempel på en café, risikerer man, at uvedkommende aflurer dataene ved at kigge over skulderen på betaleren. Der er også risiko for, at de trådløse data opsnappes, hvis der anvendes et åbent trådløst netværk.

1.2.5.1. Forholdsregler

Borgerne bør følge gængse anbefalinger for sikker internethandel. Man skal være ekstra opmærksom på, at websteder som modtager data om betalingskort, altid bør anvende krypteret kommunikation (HTTPS). Det forhindrer, at aflytning af data via trådløse netværk kan misbruges. Det kan dog i mange mobilbrowsere være svært at se, om en forbindelse er krypteret.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 1.1.3.

1.2.6. Pengeoverførsel i mobil netbank

En mobil netbank er en app, der tilbyder nogle af de samme faciliteter, som forbrugerne kender fra netbank på computeren. Her kan man se sin saldo og overføre store beløb. Mobil netbank er blevet populær: Den 31. oktober registrerede BEC således flere besøg i banken via mobilløsningen end via netbank på computeren[10].

Den mobile netbank giver direkte adgang til kontoen. Derfor indebærer den en større risiko for tab end specialiserede apps som Swipp og MobilePay. Hvis en hacker får adgang til netbank-appen, kan han overføre store beløb til sine egne konti.

Mobilbankløsningerne anvender typisk en form for to faktor-autentifikation, hvor brugeren skal indtaste en engangskode, før der kan overføres penge. I

[10] BEC, 11-11-2013

nogle tilfælde står koden på et nøglekort, som man kender det fra NemID. Andre løsninger sender en kode via sms. Men det beskytter ikke mod misbrug, hvis smartphonen er blevet stjålet – så har tyven også adgang til de sms'er, der sendes til den.

Endnu har vi ikke set skadelige apps rettet direkte mod danske mobilbanker. I udlandet er derimod observeret en app, der giver sig ud for at være en mobilbankløsning til en række koreanske banker[11]. Hvis offeret installerer den og prøver at logge ind, får bagmændene adgang til vedkommendes loginoplysninger.

1.2.6.1. Forholdsregler

De fleste netbank-apps er beskyttet med en kode, der skal indtastes, før appen kan startes. Her er det vigtigt at vælge en anden kode end den, der bruges til at låse mobilen op med. Så er der mindre risiko for, at en tyv kan aflure koden, inden han stjæler telefonen.

Engangskoder sendt via sms er en mangelfuld sikring: Hvis telefonen er i tyvens hænder, har han også adgang til den sms, der har koden, som bruges til at godkende en overførsel. Endvidere kan sms'er opsnappes via skadelige apps som fx Zitmo (Zeus in the mobile)[12]. DKCERT vurderer derfor, at der er brug for en mere sikker løsning, fx med koder på et separat nøglekort.

For øjeblikket er det ikke muligt at anvende NemID til login på smartphones. Det ventes løst i 2014, hvor der kommer en Javascript-baseret NemID-løsning. Det muliggør to faktor-autentifikation, hvor brugeren både oplyser sin adgangskode og en engangskode fra et nøglekort. Sikkerheden i sådan en løsning kan dog først vurderes, når vi kender detaljerne om implementeringen. Nogle skadelige apps har fuld kontrol med smartphonen, så her kræves der særlige forholdsregler i designet af løsningen2.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 1.1.3.

1.2.7. Digitale tegnebøger som apps

En digital tegnebog er en elektronisk pung, der opbevarer data om forbrugerens betalingskort eller andre betalingsløsninger. Et eksempel er Google Wallet. Når brugeren skal betale, åbnes appen og brugeren vælger det betalingsmiddel, der skal betales med. Foreløbig er fænomenet stort set ukendt i Danmark, fx er det ikke muligt at bruge Google Wallet i fysiske butikker, men kun på nettet.

Det vil dog ændre sig. Teleselskaberne TDC, Telia, Telenor og 3 har dannet det fælles selskab 4T Mobile Payments, der er ved at udvikle en app til mobilbetaling. Her vil beløbet blive trukket fra teleregningen. Appen ventes at få form af en digital tegnebog[3]. Nets arbejder på en digital tegnebog, som danske banker vil kunne udbyde[13]. Danske Bank venter også, at erfaringerne fra MobilePay med tiden kan føre til en form for digital tegnebog[8].

Da en digital tegnebog kan indeholde en række betalingsmidler, er det afgørende at beskytte den mod misbrug, hvis telefonen bliver stjålet. Skadelige programmer udgør også en risiko.

1.2.7.1. Forholdsregler

Brugeren bør beskytte sin digitale tegnebog med en kode, der er en anden end den, der bruges til at låse telefonen op. Endvidere skal det være muligt at lukke tegnebogen fra en computer, hvis telefonen bortkommer.

Derudover gælder de generelle anbefalinger for sikkerhed på smartphones som nævnt i afsnit 1.1.3.

1.2.8. Kortbetaling med NFC

Nogle smartphones er udstyret med NFC (Near Field Communication). Det er en kontaktløs teknologi, der gør det muligt at overføre data trådløst på op til 10 centimeters afstand. NFC kan også indbygges direkte i et kort, det kendes fra Rejsekortet. Når en smartphone har NFC, kan det kombineres med en digital tegnebog, som sender kortinformation ud via NFC. Teknologien er endnu ikke i brug i Danmark. Der er ikke nogen teknisk hindring for, at man kan lægge dankortet ind i en digital tegnebog og bruge det som kontaktløst kort. Men der er ingen konkrete planer om det.

Risikoen her er den samme som ved digitale tegnebøger. Derudover foregår der en trådløs kommunikation, som i teorien kan opsnappes. Den er dog krypteret, og en angriber skal placere sig ganske tæt på for at kunne få fat i data fra NFC-kommunikationen. Derfor anser DKCERT den risiko for meget lille.

[11] FireEye, 26-11-2013
[12] DKCERT, 2011
[13] Nets, 22-8-2013

1.2.8.1. Forholdsregler

Forholdsreglerne er de samme som ved digitale tegnebøger.

1.3. Konklusion og anbefalinger

Mobilbetaling er et område i vækst. Det tog for alvor fart i 2013, dels med et stigende antal transaktioner på mobile websider, dels med introduktionen af MobilePay og Swipp.

Når flere penge udveksles mobilt, bliver området interessant for de kriminelle. Derfor er det vigtigt for borgerne at vide, hvilke nye risici mobilbetaling medfører.

Ud fra ovenstående gennemgang kan det måske se ud som om, der er store risici ved de forskellige former for mobilbetaling. Men en risiko skal altid afvejes i forhold til det tab, man risikerer at lide. De fleste af teknologierne skal ikke sammenlignes med, hvad man kan i sin netbank – de skal ses som en afløser for pengepungen.

Med en digital tegnebog kan man opbevare sine betalingskort i smartphonen. Har man dem i sin fysiske pung, er de lige til at misbruge, hvis pungen bliver tabt eller stjålet. Misbruget er dog begrænset til situationer, hvor brugeren ikke skal indtaste sin pinkode. I smartphonen skal tyven først gætte den rette kode, før han kan bruge de lagrede oplysninger. Så her er sikkerheden faktisk lidt bedre i smartphonen i forhold til den gammeldags portemonnæ.

Løsninger som Swipp og MobilePay minder også mere om en pung end en netbank: Her kan man kun overføre et begrænset beløb pr. dag. Måske er 1.500 kroner lidt mere, end de fleste går rundt med i kontanter. Til gengæld bliver beløbet dækket, hvis der sker misbrug, fordi der teknisk set er tale om en kortbetaling. Så også her er forbrugeren bedre stillet, end hvis en pung med 1.500 kroner bliver stjålet.

En anden fremtidsmulighed er virtuelle valutaer. Der har i 2013 været megen opmærksomhed omkring Bitcoin, der er en virtuel valuta. Det er muligt at veksle Bitcoins til andre valutaer, men kursen er ikke låst fast. I fremtiden kan man forestille sig, at Bitcoins kan opbevares i brugerens digitale tegnebog. Det er endnu for tidligt at sige, hvilken rolle den type valuta vil spille på betalingsmarkedet, herunder mobilbetalinger. Men det er et område, som skal følges i de kommende år.

DKCERT ser ikke mobilbetalinger som en forestående sikkerhedsmæssig katastrofe. Men vi ser samme mønster som ved tidligere nye teknologier: Først tager forbrugerne dem til sig. Derefter opdager de teknologiens uheldige sider. Derfor er der brug for at opstille en række anbefalinger, der kan sikre, at teknologiens sikkerhedsrisici undgås.

1.3.1. Anbefalinger

Efterhånden som mobiltelefonen bliver et betalingsinstrument, er der brug for anbefalinger om sikker omgang med den. Brugerne skal passe lige så godt på mobilen som på deres pengepung.

DKCERT anbefaler følgende forholdsregler:

1. Opbevar enheden sikkert, for eksempel i en inderlomme med lynlås.
2. Lås enheden med en kode, der skal indtastes eller angives på anden måde, før man får adgang til at bruge den.
3. Installer sikkerhedssoftware, der gør det muligt at slette data på afstand, hvis enheden bortkommer eller bliver stjålet. Den type program kan også hjælpe med at lokalisere enheden.
4. Gem kvitteringer og tjek kontoudtog. Gør indsigelse, når der optræder en transaktion, der ikke kan genkendes.
5. Betal med et internationalt betalingskort for at opnå den bedst mulige forbrugerbeskyttelse.
6. Hent kun apps fra de reglementerede app stores.
7. Installer sikkerhedssoftware, der beskytter mod skadelige apps.
8. Mister man enheden, skal man hurtigst muligt få spærret de betalingsløsninger, der er knyttet til den. Man skal også spærre selve mobilabonnementet.

Anbefalingerne skal opdateres, når teknologierne udvikles. For eksempel skal NemID indgå, når det bliver muligt at bruge det på smartphones.

2. Borgernes informationssikkerhed

2.1. Indledning

Formålet med dette kapitel er at afdække, om borgerne har oplevet sikkerhedshændelser. En sikkerhedshændelse kan for eksempel være et virusangreb, tab af data som følge af en smadret harddisk eller svindel via e-mails.

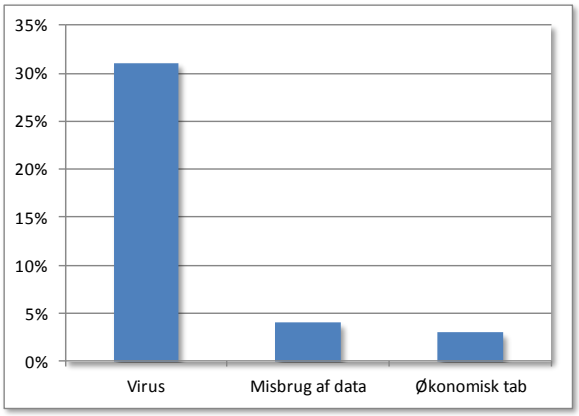
Har borgerne oplevet sikkerhedshændelser, undersøger vi, hvilke konsekvenser det fik for borgernes videre kontakt med det offentlige. Endelig ser vi på, hvad borgerne generelt ved om informationssikkerhed.

Den primære kilde til oplysningerne er en kvantitativ undersøgelse, som Danmarks Statistik foretog i januar 2014 på vegne af DKCERT. Undersøgelsen bygger på svar fra 981 personer, der udgør et repræsentativt udsnit af den voksne befolkning (16-74 år) i Danmark. Lidt over halvdelen af svarene blev indhentet via telefon, resten er fra spørgeskemaer på web.

Svarene fra undersøgelsen er suppleret med data indsamlet i forbindelse med rapporten It-anvendelse i befolkningen 2013 fra Danmarks Statistik[14] samt øvrige kilder.

Efter en gennemgang af undersøgelsens resultater opstiller vi en række konkrete anbefalinger til sikker adfærd på nettet og computeren og til håndtering af sikkerhedshændelser.

2.2. Oplevede sikkerhedshændelser



Figur 3: Tre typer trusler borgerne har oplevet.

Vi har spurgt borgerne, om de har oplevet tre konkrete trusler mod deres informationssikkerhed: Virus eller anden skadelig software, misbrug af personlige oplysninger og økonomisk tab som følge af it-sikkerhedsproblemer.

Virus er den mest udbredte af de tre trusler: 31 procent har haft virus eller andre former for skadelige programmer på deres computer. Det svarer til resultatet fra undersøgelsen "It-anvendelse i befolkningen 2013", hvor 28 procent af internetbrugerne havde haft virus inden for de sidste 12 måneder.

Kun fire procent af deltagerne i undersøgelsen oplevede misbrug af personlige oplysninger. Tre procent har haft et økonomisk tab som følge af it-sikkerhedsproblemer. De tal svarer ganske godt til resultaterne i forskningsrapporten "Kriminalitet i en digitaliseret verden" fra oktober 2013[15] . Ifølge den har fire procent af danskerne inden for en 12 måneders periode været udsat for identitetstyveri, betalingskortmisbrug eller handelsbedrageri på nettet.

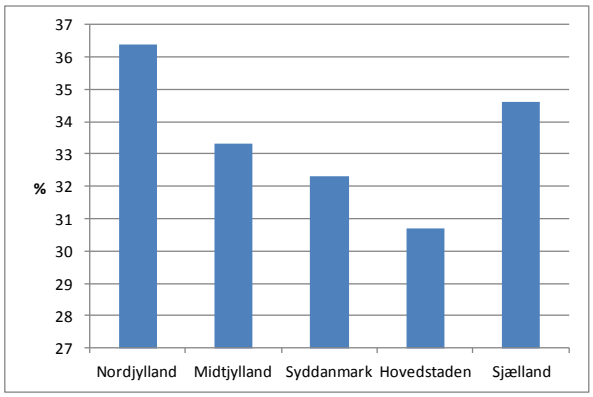
Generelt viser svarene kun, hvad borgerne har opdaget. Flere kan således have haft virus eller have fået misbrugt personlige data uden at være klar over det. DKCERT anslår derfor, at der reelt er flere borgere, der har haft virus eller fået misbrugt personlige data.

Tallet om økonomisk tab antages at være mere retvisende – hvis man mister penge, skal man nok opdage det. Ifølge undersøgelsen "It-anvendelse i befolkningen 2013" vokser mængden dog af danskere, der lider økonomisk tab på grund af it-trusler. Så selvom andelen er lille, er mængden stigende.

Vi har ikke spurgt om spam, der traditionelt har været den mest udbredte gene for internetbrugerne. Det skyldes, at spam i sig selv ikke udgør et sikkerhedsproblem.

[14] Danmarks Statistik, november 2013

[15] Kriminalitet i en digitaliseret verden, 2013

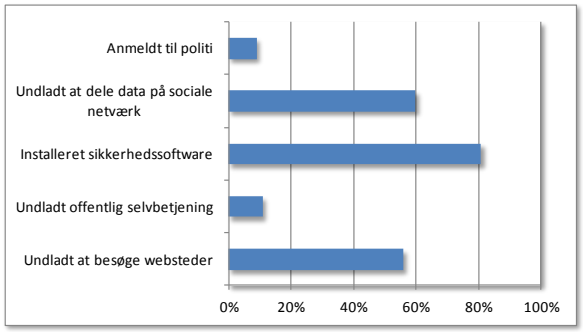


Figur 4: Nordjyder oplever oftere sikkerhedsproblemer.

Samlet set svarer 33 procent, at de har oplevet et eller flere af de tre sikkerhedsproblemer.

Der er nogle mindre udsving i svarene, når vi opdeler dem på geografi. Således har over 36 procent af borgerne i Nordjylland oplevet it-sikkerhedsproblemer. DKCERT har ikke en forklaring på fænomenet, men bemærker, at nordjyderne også er dårligst til at tage sikkerhedskopi: Kun 28 procent sikkerhedskopierer dataene på deres pc.

2.3. Konsekvenser af sikkerhedshændelser



Figur 5: Handlinger, borgerne har udført som konsekvens af de trusler, de oplevede.

Hvad gør man, når man er udsat for en sikkerhedshændelse? Langt de fleste installerer sikkerhedssoftware. Det svarer 81 procent af dem, der var udsat for en af de tre trusler, at de har gjort.

Seks ud af ti ramte blev mere forsigtige med, hvilke data de delte på sociale netværk som fx Facebook.

Trusler kan være så skræmmende, at de direkte afholder borgerne fra at bruge tjenester på nettet. Vi har spurgt, om borgerne har holdt sig fra to slags tjenester: Dels bestemte websteder, dels specifikt offentlige selvbetjeningsløsninger (som fx Skat Tastselv). Lidt over halvdelen undlod at besøge bestemte websteder efter sikkerhedshændelsen. 11 procent afholdt sig fra at bruge offentlig digital selvbetjening.

Det giver god mening at holde sig fra at besøge bestemte websteder, hvis man har fået virus efter at have været på fx et pornowebsted eller et med piratkopier. Derimod er det sværere at argumentere for, at man skal undlade at bruge offentlig selvbetjening efter en sikkerhedshændelse.

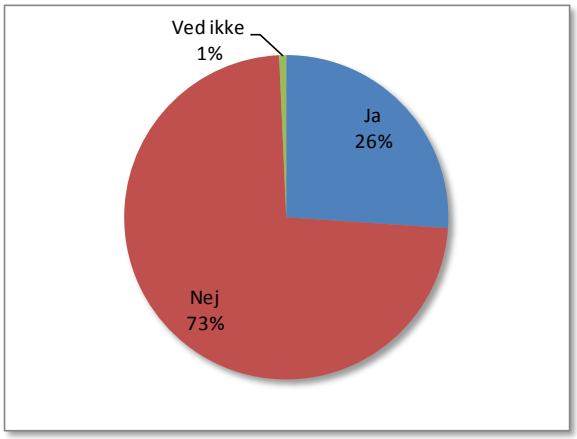
Tallene viser derfor, at nogle borgere har brug for at forstå, hvad der udgør risikoadfærd på nettet, og hvad der ikke er det.

Ni procent har anmeldt sikkerhedshændelsen til politiet eller andre instanser.

I alt har 95 procent af de borgere, der blev udsat for en it-sikkerhedshændelse, ændret adfærd eller taget forholdsregler for at undgå, at det sker igen.

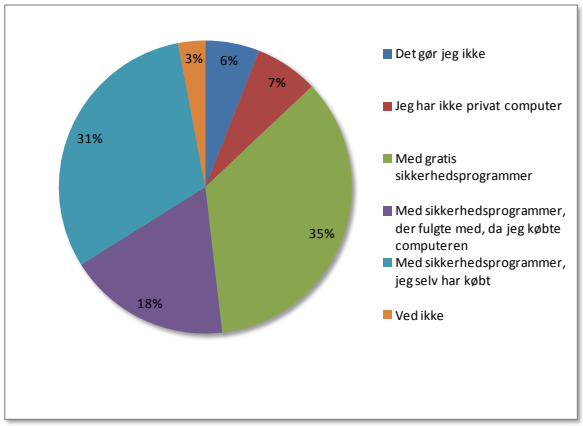
2.4. Viden om informationssikkerhed

Ud over at spørge til de sikkerhedshændelser borgerne har været udsat for, har vi også undersøgt deres viden om it-sikkerhed.



Figur 6: 26 procent sender følsomme data som ukrypterede e-mails.

Datatilsynet anser personnumre som en oplysning af fortrolig karakter. Derfor anbefaler tilsynet, at personnumre sendes krypteret over nettet. Men 26 procent af borgerne svarer, at de har sendt cpr-nummer eller andre personlige oplysninger i e-mail til det offentlige. Da krypteret e-mail er meget lidt udbredt, er det efter DKCERTs vurdering sandsynligt, at disse følsomme data er sendt ubeskyttet.

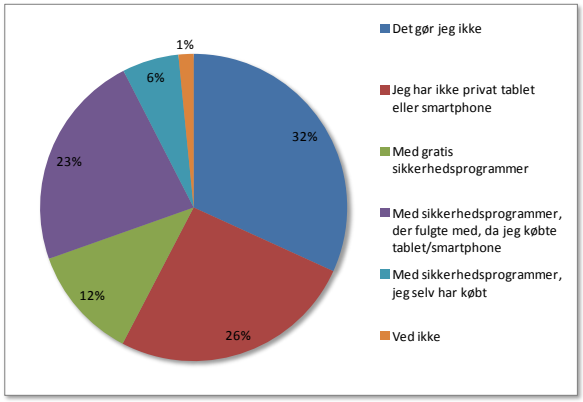


Figur 7: Langt de fleste beskytter deres computer.

"It-anvendelse i befolkningen 2013" viste, at 86 procent af internetbrugerne anvender sikkerhedssoftware. Vores undersøgelse giver nærmere detaljer om valget af produkter. Således viser det sig, at en tredjedel vælger at beskytte sig med gratis programmer. 18 procent bruger de sikkerhedsprogrammer, der fulgte med ved køb af pc'en. Det er ofte tidsbegrænsede programmer: Efter en periode skal man betale for at fortsætte med at modtage opdateringer af virusdefinitioner.

Knap en tredjedel af brugerne har selv investeret i sikkerhedssoftware ud over det, der fulgte med ved købet af computeren. Kun seks procent svarer, at de ikke beskytter deres computer med antivirus eller lignende.

Svarene illustrerer, at pc-teknologien er gammel og moden. Folk har hørt om antivirus de sidste 20 år, så de er klar over, at det er nødvendigt. For at sætte emnet i perspektiv stillede vi de samme spørgsmål om sikkerhedssoftware til smartphones og tablets.



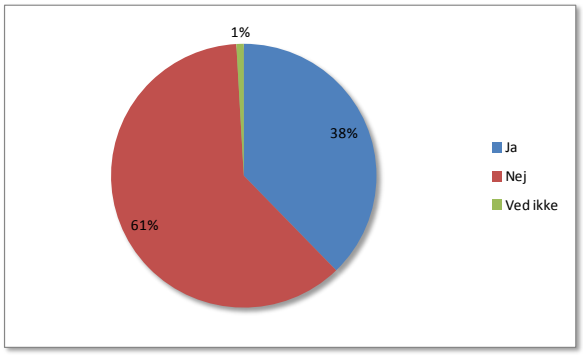
Figur 8: Mere end hver tredje beskytter ikke data på sin smartphone eller tablet.

Her svarer næsten hver tredje, at de ikke beskytter enheden og dataene på den. Hvis man udelader de 26 procent, der ikke har smartphone eller tablet, er det 43 procent af brugerne, der ikke beskytter deres udstyr.

Af de resterende har de fleste valgt at bruge den sikkerhedssoftware, der fulgte med, da de købte enheden.

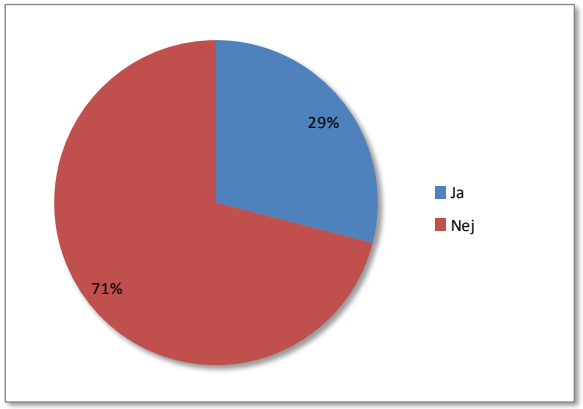
Tallene kan være udtryk for, at mange stadig opfatter en smartphone som en telefon. De tænker ikke på den som en lille computer, der indeholder en lang række personlige data: Familiebilleder, kontaktinformationer, sms'er, e-mails og passwords til en række onlinetjenester.

Sikkerhedssoftware som antivirus, firewall og antispyware beskytter computeren eller smartphonen mod angreb. Men der er også brug for at beskytte data mod at gå tabt. Det kan fx ske, hvis enheden går i stykker eller bliver stjålet. Så er det vigtigt at have en sikkerhedskopi.



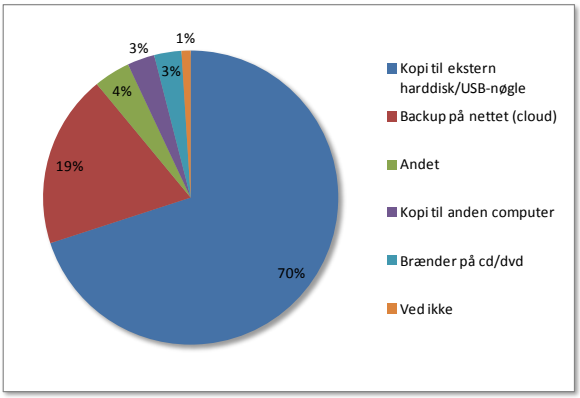
Figur 9: 38 procent tager sikkerhedskopi af data på deres private computer.

38 procent af de borgere, der har en computer, tager sikkerhedskopi af data. 61 procent gør det ikke.



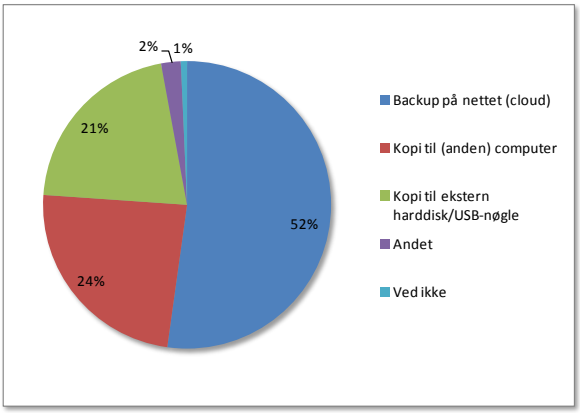
Figur 10: 29 procent tager sikkerhedskopi af data på deres smartphone eller tablet.

Men kun 29 procent af dem, der har en smartphone eller tablet, tager sikkerhedskopi.



Figur 11: Ekstern harddisk er den mest populære metode til sikkerhedskopiering af computer.

To tredjedele af de brugere, der tager sikkerheds-kopi af deres computer, bruger en ekstern harddisk eller USB-nøgle. Den næstmest populære metode er cloud-backup, hvor data kopieres ud på en server på internettet.

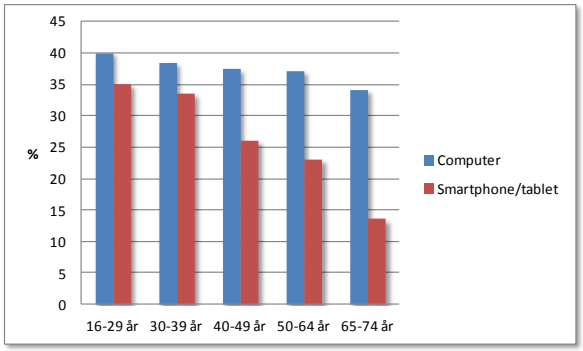


Figur 12: Cloud fører, når man skal sikkerhedskopiere data på en smartphone.

Også her er billedet anderledes for smartphones: Godt halvdelen af dem, der tager sikkerhedskopi, gør det via en cloud-tjeneste. Resten er nogenlunde ligeligt fordelt mellem kopi til en computer og ekstern disk.

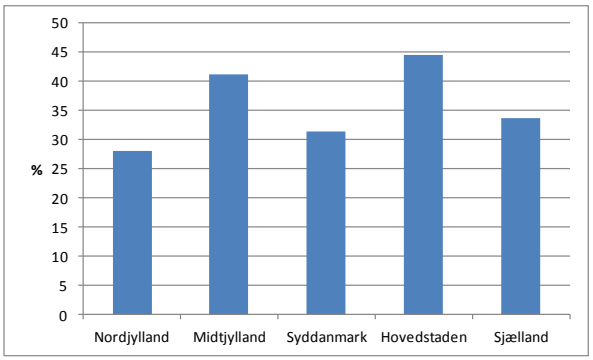
Svarene om sikkerhedskopier viser, at her er et alvorligt problem for borgerne: De risikerer at miste deres private data, fordi de ikke har styr på sikkerhedskopieringen.

Men de viser også noget interessant, når det gælder fremtiden: De unge er nemlig bedre til at tage sikkerhedskopi end de ældre. Blandt de 16-29-årige er der således 40 procent, der sikkerhedskopierer deres computerdata. Smartphone-brugere under 40 år er væsentligt bedre til at tage sikkerhedskopi end de ældre brugere.



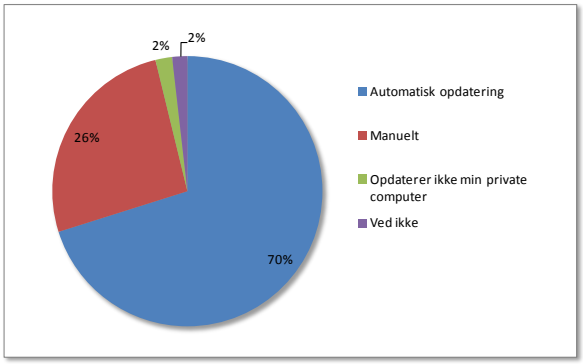
Figur 13: Procent der tager sikkerhedskopi fordelt på alder.

Københavnerne er bedst til at sikkerhedskopiere deres data. 45 procent tager jævnligt sikkerheds-kopi af data på deres computer. I Nordjylland er andelen nede på 28 procent.



Figur 14: Borgere i hovedstaden sikkerhedskopierer mere end andre.

De fleste vellykkede angreb udnytter sårbarheder i software. Derfor er det afgørende for sikkerheden, at software på borgernes computere og andre enheder holdes opdateret. På den måde bliver sikkerhedshuller lukket, så snart softwareproducenten har udsendt en rettelse.



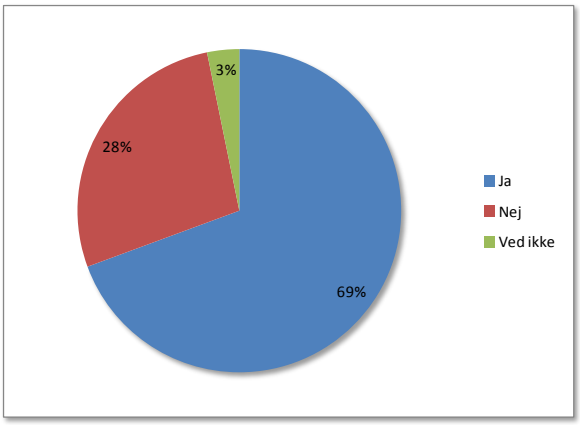
Figur 15: 70 procent bruger automatisk opdatering.

70 procent holder deres computer opdateret ved hjælp af automatisk opdatering. Det vil typisk sige, at de har slået funktionen automatiske opdateringer til under Windows Update.

26 procent foretrækker at opdatere software manuelt, mens kun tre procent svarer, at de ikke holder computeren opdateret.

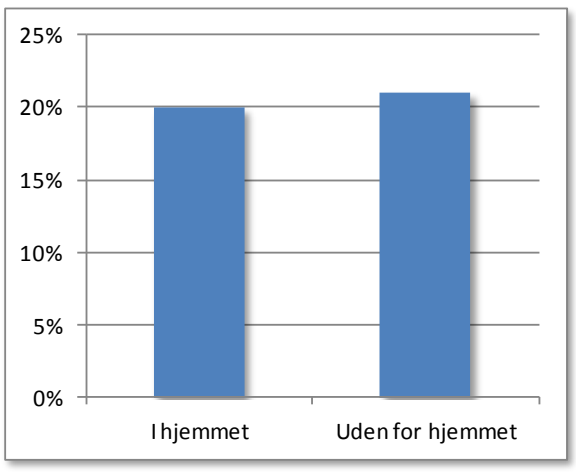
Automatisk opdatering er en nyttig funktion. Men den kan give en falsk tryghed. Funktionen dækker nemlig ikke alle programmer. Windows Update sørger således kun for at opdatere Microsoft-programmer. Andre programmer har deres egne automatiske opdateringsfunktioner, mens nogle stadig skal opdateres manuelt.

En del borgere er klar over, at automatiske opdateringer ikke nødvendigvis sikrer, at alt er opdateret. 28 procent føler sig ikke sikre på, at alle programmer der skal opdateres, rent faktisk også bliver det.



Figur 16: Føler borgerne sig sikre på, at alt der skal opdateres, bliver det?

Spørgsmålet er både stillet til dem, der anvender automatisk opdatering, og de øvrige.

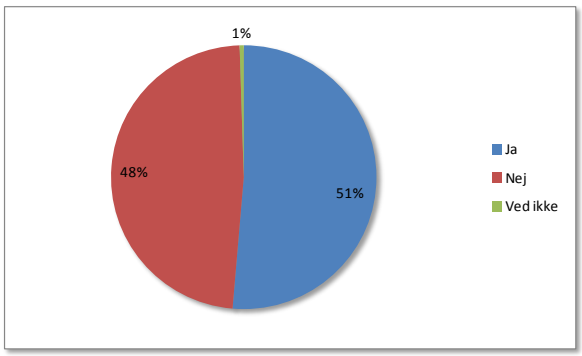


Figur 17: Hver femte bruger trådløse netværk, som ikke kræver adgangskode.

Når man bruger et trådløst netværk, skal man nogle gange indtaste en adgangskode. Det betyder som regel, at kommunikationen er krypteret. Er den ikke det, kan enhver der er inden for netværkets radiorækkevidde aflytte kommunikationen. Derfor er adgangsbeskyttelsen en vigtig sikkerhedsfunktion på trådløse netværk.

Hver femte anvender trådløse netværk uden kryptering. Andelen er stort set den samme, hvad enten det gælder bopælens eget netværk eller trådløse net ude i byen.

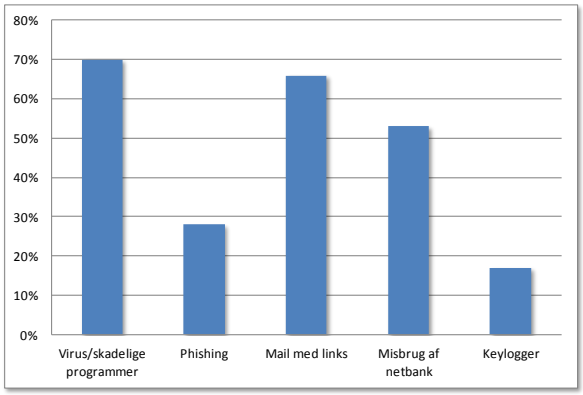
Ud over risikoen for aflytning på det pågældende netværk indebærer det også en anden risiko. Når en enhed en gang har været på et trådløst net, husker den det ofte. Når den senere ikke er på et net, søger den efter de netværk, som den har brugt før. Det kan hackere udnytte ved at opsnappe, hvilke netværk der søges efter. Derefter lader deres udstyr som om, det er det pågældende netværk. Ofte vil offerets enhed slutte sig til netværket uden videre. Det kan man beskytte sig mod ved at sætte sin enhed til at glemme netværket, når man er færdig med at bruge det.



Figur 18: Bruger samme adgangskode til flere tjenester.

Mere end halvdelen af borgerne anvender den samme adgangskode til flere forskellige tjenester. Det kan fx være deres netbank, webmail, Facebook og andre onlinetjenester.

Det udgør en sikkerhedsrisiko. Hvis angribere får fat i brugernavn og password til en enkelt tjeneste, kan de hurtigt afprøve kombinationen på andre tjenester. På den måde kan et brud på sikkerheden på en onlinebutik, hvor man en enkelt gang har købt noget, føre til, at fremmede får fat i ens mails eller andre fortrolige oplysninger.



Figur 19: Borgere der ved, hvordan de skal beskytte sig mod bestemte trusler.

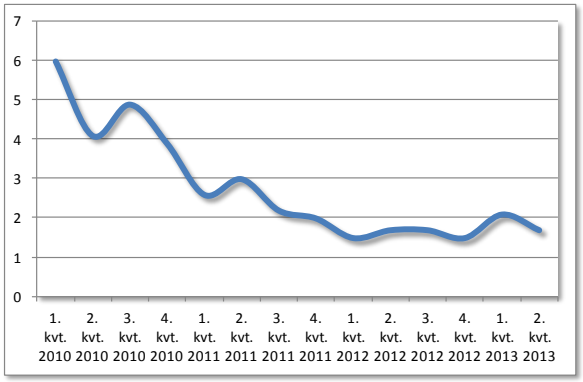
Endelig har vi spurgt borgerne, om de føler sig i stand til at beskytte sig mod fem konkrete trusler: Virus og andre skadelige programmer, phishing, e-mails med vedhæftede filer eller links, misbrug af netbank og keyloggere. For virus og e-mails ved over to ud af tre, hvad de skal gøre. Derimod kan kun 28 procent beskytte sig mod phishing.

Det er dog ikke nødvendigvis korrekt. 47 procent svarer nemlig, at de ikke ved, hvad phishing er. Så det er muligt, at de godt kan genkende en svindelmail og undlade at reagere på den, selvom de ikke kender begrebet phishing.

Kun 17 procent kan beskytte sig mod keyloggere, der opsnapper tastetryk. Men også her er det nok tegn på uvidenhed: 61 procent ved ikke, hvad en keylogger er. Da en keylogger oftest installeres af et skadeligt program, vil de som regel være beskyttet i kraft af deres antivirusløsning. Det samme gælder for misbrug af netbank – også her foregår misbruget som regel via skadelig software på offerets computer.

2.5. Internationalt perspektiv

For at sætte tallene i perspektiv inddrager vi her statistikker fra Microsofts Security Intelligence Report[16]. Rapporten fører statistik over mængden af computere, som firmaets "Værktøj til fjernelse af skadelig software" renser for infektioner. Værktøjet er et program, der kører hver måned på de pc'er, hvor automatiske opdateringer er slået til. Programmet kan fjerne en række af de mest udbredte virus og andre skadelige programmer.



Figur 20: Computere renset pr. 1.000 computere i Danmark 2010-2013.

Tallet angives som antallet af computere pr. 1.000 computere, der blev renset for skadelig software. I den seneste rapport, der dækker andet kvartal 2013, var tallet for Danmark 1,7.

Til sammenligning var gennemsnittet på verdensplan 5,8. Der er imidlertid store udsving: fra 31,5 i Irak til 1,1 i Japan. Men Danmark ligger blandt landene med den laveste mængde infektioner.

2.6. Konklusion på undersøgelsen

Virus og andre skadelige programmer er den trussel, borgerne i vores undersøgelse hyppigst er udsat for. Derimod har kun få borgere fået misbrugt personlige oplysninger eller haft økonomisk tab som følge af it-sikkerhedshændelser.

Det passer godt til de forholdsregler, som borgerne tager: Kun fem procent oplyser, at de ikke bruger en form for antivirus eller anden sikkerhedssoftware. At de så alligevel kan blive ramt, kan skyldes, at sikkerhedssoftware ikke beskytter mod alt. Desuden kan nogle af de ramte være dem, der ikke anvender sikkerhedssoftware, eller hvor den ikke bliver opdateret.

Skønt 31 procent borgere med virusangreb kan lyde højt, ligger Danmark internationalt blandt de seks lande med færrest tilfælde af skadelig software.

Hvor danskerne er gode til at beskytte deres computere mod virus, er de dårligere til at beskytte sig selv. Halvdelen bruger således samme password til flere tjenester. Dermed udsætter de sig for risiko for, at uvedkommende får adgang til deres data.

Et andet eksempel på dårlig beskyttelse af personlige data er, at 26 procent sender fortrolige oplysninger med e-mail til det offentlige. Hvis det sker på et

[16] Microsoft Security Intelligence Report

usikkert netværk, kan uvedkommende opsnappe dataene.

61 procent af borgerne vil miste data, hvis deres computer bliver stjålet eller går i stykker. De tager nemlig ikke jævnligt sikkerhedskopi af deres data. Procentsatsen svarer til, at 2,3 millioner danskeres private data ikke er sikret med sikkerhedskopiering.

Endnu værre ser det ud for smartphones og tablets: Her er det 71 procent, der ikke sikkerhedskopierer. I nogle tilfælde kan der dog være en sikkerhedskopi, som brugeren ikke kender til. For eksempel kan en telefon være sat op til at anvende et adressekartotek på en server i skyen. Så er navne og telefonnumre stadig tilgængelige, selvom telefonen går tabt.

Geografisk set tyder undersøgelsen på, at borgere i hovedstadsområdet har bedre styr på it-sikkerheden end borgere i resten af landet. Især Nordjylland stikker ud, når det gælder mængden af sikkerhedsproblemer – og de er tilsvarende dårligst til at tage sikkerhedskopi.

Samlet er det DKCERTs opfattelse, at danskerne har ganske godt styr på skadelig software og hvordan man beskytter sig imod den. Derimod er der alvorlige problemer med sikringen af data via sikkerhedskopiering. Og borgerne savner også viden om, hvordan de beskytter og behandler fortrolige data. Sikkerheden er bedre på computere end på nye enheder som smartphones og tablets.

2.7. Anbefalinger

Vores undersøgelse har afdækket et behov for bedre beskyttelse af data på mobile enheder. Men også de traditionelle computere giver sikkerhedsmæssige udfordringer, primært inden for sikkerhedskopiering.

Vi har her samlet nogle anbefalinger til borgerne om, hvordan de kan forbedre deres it-sikkerhed. Vi har opdelt dem i to grupper: Råd om sikkerhed på mobile enheder og generelle råd.

2.7.1. Sikkerhed på mobilen

DKCERT anbefaler følgende forholdsregler i forbindelse med borgernes anvendelse af mobile enheder:

1. Beskyt din telefon med en kode.
2. Brug kun trådløse netværk (Wi-Fi) med kryptering.
3. Hvis du bruger et ubeskyttet trådløst netværk, så indstil telefonen til at glemme det, når du er færdig.
4. Luk for abonnementet og tilknyttede betalingstjenester, så snart telefonen bliver stjålet eller tabt.
5. Tag sikkerhedskopi af data på mobile enheder.

2.7.2. Generel sikkerhed

Derudover anbefaler DKCERT følgende grundlæggende forholdsregler til sikker adfærd på nettet og computeren.

6. Hold alle programmer opdateret.
7. Anvend sikkerhedsprogrammer (antivirus, antispyware, firewall).
8. Vær forsigtig med vedhæftede filer eller links, du får tilsendt uopfordret.
9. Tag jævnligt sikkerhedskopi af dine data.
10. Brug sikre passwords på mindst otte tegn. De skal bestå af store og små bogstaver, tal og gerne specialtegn.
11. Brug ikke samme password til forskellige tjenester.
12. Følg ikke links i mails, der beder om fortrolige oplysninger.
13. Hent kun apps og andre programmer fra kilder, du har tillid til.

3.Bilag 1: Spørgsmål bag undersøgelsen

Her følger de spørgsmål, Danmarks Statistik har stillet til et repræsentativt udsnit af den voksne danske befolkning.

Bloknavn	**Beskrivelse af blok/modul**			
Variabel-navn	Spørgsmålstekst	Svarkategorier	Spm1=1 { Filter }	Bemærkning
BlokA	**IT-sikkerhed på privat computer, smartphone og tablet**			
Ax	1. Har du været ude for nogle af følgende it-sikkerhedsproblemer?			
A1	1A Computer inficeret med virus eller andre typer skadelige programmer	1 Ja 2 Nej		
A2	1B Misbrug af dine personoplysninger på nettet	1 Ja 2 Nej		
A3	1C Økonomisk tab som følge af it-sikkerhedsproblem	1 Ja 2 Nej		
BlokB	**2 Har du som følge af de oplevede it-**		BlokA.A1 = 1 or	Filteret læses således. Hvis spørgsmål A1 eller A2 eller A3 i

	sikkerhedsproblemer …		BlokA.A2 = 1 or BlokA.A3 = 1	BlokA er lig med 1 stilles alle spørgsmålene i denne blok.
B1	2A Undladt at besøge bestemte websteder?	1 Ja 2 Nej	BlokA.A1 = 1 or BlokA.A2 = 1 or BlokA.A3 = 1	
B2	2B Undladt at anvende digitale selvbetjeningsløsninger fra det offentlige (fx Skat Tastselv, melde flytning)	1 Ja 2 Nej	BlokA.A1 = 1 or BlokA.A2 = 1 or BlokA.A3 = 1	
B3	2C Installeret eller opgraderet sikkerhedssoftware (fx antivirus)	1 Ja 2 Nej	BlokA.A1 = 1 or BlokA.A2 = 1 or BlokA.A3 = 1	
B4	2D Undladt at dele oplysninger om dig selv på sociale netværk	1 Ja 2 Nej	BlokA.A1 = 1 or BlokA.A2 = 1 or BlokA.A3 = 1	
B5	2E Anmeldt sikkerhedsproblem til politi eller andre?	1 Ja	BlokA.A1 = 1 or	

		2 Nej	BlokA.A2 = 1 or BlokA.A3 = 1	
B6	3. Har du sendt cpr-nummer eller andre personlige oplysninger i e-mail til det offentlige?	1 Ja 2 Nej		
B7	4. Hvordan beskytter du din private computer og data?	1 Med sikkerhedsprogrammer, der fulgte med, da jeg købte computeren. 2 Med sikkerhedsprogrammer, jeg selv har købt. 3 Med gratis sikkerhedsprogrammer 4 Det gør jeg ikke. 5 Jeg har ikke privat computer		
B8	5. Hvordan beskytter du din smartphone eller tablet og data på den?	1 Med sikkerhedsprogrammer, der fulgte med, da jeg købte tablet/smartphone. 2 Med sikkerhedsprogrammer, jeg selv har købt. 3 Med gratis sikkerhedsprogrammer 4 Det gør jeg ikke. 5 Jeg har ikke privat tablet eller smartphone	A6 = 4	
B9	6. Hvordan holder du programmerne på din private computer opdateret? LÆS OP		BlokB.b7 = 1,2,3,4	(Alle der har privat computer)
B10	6AB. Har du slået automatisk opdatering til eller opdaterer du manuelt?	1 Automatisk opdatering 2 Manuelt 3 Opdaterer ikke min private computer	BlokB.b7 = 1,2,3,4	(Alle der har privat computer)
B11	6C. Føler du dig sikker på, at alle programmer	1 Ja	BlokB.b7 = 1,2,3,4	(Alle der har privat computer)

	der skal opdateres, bliver opdateret?	2 Nej		
B12	7A. Anvender du trådløse netværk, der ikke kræver adgangskode hjemme?	1 Ja 2 Nej		
B13	7B.Anvender du trådløse netværk, der ikke kræver adgangskode udenfor hjemmet?	1 Ja 2 Nej		
B14	8.Bruger du samme adgangskode til flere onlinetjenester? (f.eks netbank, email, facebook o.lign)	1 Ja 2 Nej		
B15	9. Tager du jævnligt sikkerhedskopi af data på din computer?	1 Ja 2 Nej	BlokB.b7 = 1,2,3,4	(Alle der har privat computer)
B16	Hvordan tager du sikkerhedskopi af data på din computer?	1 Kopi til ekstern hard-disk/USB-nøgle 2 Backup på nettet (cloud) 3 Brænder på cd/dvd 4 Kopi til anden computer 5 Andet	BlokB.b15 = 1	(Alle der har privat computer og tager sikkerhedskopi)
B17	10. Tager du jævnligt sikkerhedskopi af data på din smartphone eller tablet?	1 Ja 2 Nej	BlokB.b8 = 1,2,3,4	(Alle der har privat tablet eller smartphone)
B18	10A. Hvordan tager du sikkerhedskopi af data på din smartphone eller tablet?	1 Kopi til ekstern hard-disk/USB-nøgle 2 Backup på nettet (cloud) 3 Brænder på cd/dvd 4 Kopi til (anden) computer 5 Andet	BlokB.b17 = 1	(Alle der har privat computer og tager sikkerhedskopi)
BlokC	11. Ved du hvordan du skal beskytte dig mod følgende IT-sikkerhedstrusler?			

C1	11A.Virus og andre skadelige programmer?	1 Ja 2 Nej		
C2	11B.Phishing?	1 Ja 2 Nej 3 Ved ikke, hvad phishing er		
C3	11C.Mails med links eller vedhæftede filer?	1 Ja 2 Nej		
C4	11D Misbrug af din netbank?	1 Ja 2 Nej 3 Har ikke netbank		
C5	11E. Keylogger?	1 Ja 2 Nej 3 Ved ikke, hvad keylogger er		

4. Bilag 2: Danmarks Statistiks dokumentation af undersøgelsen

4.1. Varedeklaration

Opgave	IT-sikkerhed i private husstande
Kunde	DK CERT
Delopgaver udført af: Population Stikprøve Dataindsamling Opregning	 Danmarks Statistik Danmarks Statistik Danmarks Statistik Danmarks Statistik
Population	4.18 mill personer 16-74 år
Bruttostikprøve	1800 personer
Nettostikprøve	1.528 personer
Antal svar	981 personer
Svarprocenter: af bruttostikprøve af nettostikprøve	 54,5 pct. 64,2 pct.
Indsamlingsmetode	Web og telefon
Svar fordelt på indsamlingsmetode (telefon-web-post)	Web 473 svar / 48,2 pct. Telefon 508 svar / 51,8 pct.
Bortfaldskategorier	Ikke truffet 162 personer Nægtere 118 Øvrigt bortfald 41 Sprogvanskeligheder 19 Ikke kontakt på tlfnr. 59 Ikke fundet tlfnr. 148
Undersøgelsesperiode (web-telefon-post)	Web 1. jan 2014- 15. jan 2014 Telefon 4. jan 2014- 16.jan 2014
Rykkerudsendelse	1. rykker: Alle
Sprog og oversættelse af brev og skema	Nej
Anvendt tolkning på andre sprog	Nej
Pilotundersøgelse	Nej
Instruktion på undersøgelse	Ja – Danmarks Statistik
Opregning og vægtning af data	Ja

4.2. Generelt om population og stikprøve

Skal have bopæl i Danmark

Udover den eventuelle afgrænsning af populationen, som kan være lavet ud fra Danmarks Statistiks registre eller kundens egne registre, så afgrænses personer i populationen af den seneste befolkningsstatus. Den dannes hvert kvartal 30 dage efter kvartalsafslutning dvs. at 1. januar er klar primo februar osv.

For at tælles med i den danske befolkning, skal man have bopæl i Danmark og have tildelt et CPR-nummer.

24

Kvalitet af cpr

CPR's befolkningsstatus er ret præcis. Usikkerheden på den samlede befolkning er få promille. Kun ved undersøgelser, hvor personer har flyttet ind og ud af Danmark, kan der være en større usikkerhed.

Personer som flytter til udlandet

Personer, som flytter ud af Danmark, er ikke tvunget til at lade det registrerer nogen steder. Der er derfor en mindre gruppe personer, som stadig er registret som en del af den danske befolkning, på trods af at de ikke længere har adresse i Danmark.

Udenlandske studerende

Uddannelsessøgende skal have et CPR-nummer for at blive optaget på en dansk uddannelse. De skal dog også være optaget på studiet før de kan få opholdstilladelse, og der kan derfor være et mindre antal personer, som ikke tælles med.

Forskerbeskyttelse

Omkring 700.000 personer i den danske befolkning har forskerbeskyttelse, hvilket betyder, at de ikke deltager i interviewundersøgelser fra Danmarks Statistik.

Du kan læse mere om forskerbeskyttelse her

http://www.dst.dk/TilSalg/Interview/Kunde/Forskerbeskyttelse.aspx

Sikring af repræsentivitet i undersøgelser

Danmarks Statistik danner populationer med udgangspunkt i Befolkningsregisteret (CPR) samt øvrige registeroplysninger. I denne proces anvender vi et unikt person-ID for alle personer (en anonym CPR-nøgle). Vi tester og fejlsøger data for at sikre at hver person kun optræder én gang i vores population.

Efter at vi har lavet stikprøvedesignet, danner vi stikprøven ved hjælp af SAS Proc SurveySelect. Her anvender vi SRS-metode (Simple Random Sample). Denne metode giver samme

tilfældige udvalgschance (uden tilbagelægning) for alle deltagere. Metoden danner en ny tilfældig seedning hver gang og dermed en sikring af, at det ikke er de samme personer, som bliver udvalgt fra populationen gentagene gange.

Du kan læse mere om PROC SURVEYSELECT funktionen her

SAS-koden

Kodeeksempel:

```
proc surveyselect
  data=pop_select sampsize=1020
  method=srs out=stikip
  OUTSIZE STATS;
run;
```


Udvalgssandsynligheden

Vi kan også udvælge en stratificeret stikprøve, hvor der er forskellige udvalgssandsynligheder. Derfor gemmer vi altid udvalgssandsynligheden og stikprøvevægten for alle deltagere i undersøgelsen.

Test og kvalitetssikring

Efter dannelse af stikprøven, så tester og fejlsøger vi for dubletter. Vi laver tabeloversigter på hhv. population og stikprøve for at se om sammensætningen er nogenlunde ensartet på en række baggrundsvariable (køn, alder, herkomst, uddannelse, indkomst mv.) Herudover tester vi også for om der er udvalgt flere på samme bopæl, og om bopælen er en særlig adresse (med mange personer eller ugyldig adresse).

Vi validerer herefter stikprøven op mod en aktuel CPR-befolkning (få dage gammel) for at sikre os, at vi har korrekte oplysninger på alle deltagere, samt frasortering af beskyttede, døde og udvandrede personer.

Ved at anvende denne metode og tilhørende fejlsøgningsproces sikrer vi os at vores stikprøver er repræsentative for den population de er udtrukket fra.

4.3. Danmarks Statistiks begreber

Populationen

Vores definition af population er efter match med seneste kvartals-befolkningsstatus.

Bruttostikprøve

Den udvalgte bruttostikprøve fra populationen er uden hensyn til forskerbeskyttelse og seneste flyttede/døde.

Nettostikprøve

Nettostikprøve indeholder personer, der kan kontaktes efter seneste cpr-opdatering. Forskerbeskyttede og adressebeskyttede personer er ikke med. Ligeledes er personer, som står med 'Rådhusadresser' dvs. hjemløse og personer uden fast adresse mv. heller ikke er medregnet. (vejkode 99).

4.4. Undersøgelsesforløbet

Telefonsøgning

Vi laver et dataudtræk med interviewpersonen og op til tre øvrige personer i husstanden over 18 år. Vi anvender den seneste adressekode fra CPR. Har der været en flytning inden for de seneste måneder, så medtager vi også den tidligere adressekode. Data sendes til DM Partner, der står for selve telefonnummerberigelsen.

Vi modtager op til fem telefonnummerer på hver interviewperson. Vi har i samarbejde med DM Partner lavet følgende prioritering af de numre vi finder:

A-match (KVH og navnesammenfald)

A2-match på tidligere adresse (KVH_old og navnesammenfald)

A3-match på person 2-4 (altså IKKE hovedperson) (KVH og navnesammenfald)

B-match (Samme KVHX - fastnet)

C1-match (Lavfrekvent navn (f.eks. Peter Rattleff) eller min et mellemnavn og samme postnummer)

C2-match (Meget lavfrekvent navn (f.eks. Ôhcgul Rattleff) eller min 2 mellemnavne og samme postnummer)

C3-match (Samme KVHX - mobilnr)

C4-match (KVH alene match)

REST-match (Ingen match)

Brev til interviewperson

Vi sender altid et brev til interviewpersonen inden vi starter interview. Har vi fundet et telefonnummer, så skriver vi normalt det i brevet. Hvis personen ønsker at blive kontaktet på et andet nummer, er dette muligt ved at henvende sig til Danmarks Statistik. Ligeledes opfordrer vi i brevet til at indsende et telefonnummer på mail, hvis vi ikke har fundet noget nummer på interviewpersonen.

Web og telefonundersøgelser

Ofte har vi en kombination af web- og telefonundersøgelse evt. også postskema. I brevet til interviewpersonen sender vi login og password, så personen selv kan udfylde skemaet på internettet. De har normalt 8-14 dage fra udsendelse til at udfylde på nettet, før vi begynder at kontakte pr. telefon.

4.5. Svar

Svar

Vi tæller kun gennemførte interviews med i svarprocenten.

Svarprocent

Vi udregner normalt svarprocenten ud fra nettostikprøven. Der kan dog tages højde for eventuelle *ikke relevante*.

Dataindsamlingsmetode

Det vil fremgå med hvilken metode data er indsamlet med. Telefon, web eller postskema.

4.6. Bortfaldskategorier

Ikke truffet

Vi har fundet telefonnummer, og har måske haft kontakt (eller optaget/ikke svar), men vi har ikke kunne gennemføre interview.

Nægter

Vi har haft kontakt til interviewpersonen, der har meddelt at han/hun ikke ønsker at deltage. Denne kategori inkluderer også delvist gennemførte interviews.

Øvrigt bortfald

Det er personer, som har sygdom/handicap eller er døde, samt personer som er væk fra hjemmet i interviewperioden. Vi har normalt haft kontakt til en anden end interviewpersonen i husstanden.

Sprogvanskeligheder

Interviewpersonen har ikke været i stand til at gennemføre et interview på dansk. På mange af vores undersøgelser forsøger vi herefter at tolke på en række sprog, hvor det er muligt.

Ikke kontakt på telefonnummer

Vi har normalt forsøgt at ringe mindst fire gange til interviewpersonen. Vi laver desuden ekstra telefonnummersøgning på navnet og adressen, normalt sker dette efter mindst fire forgæves opkald. Denne kategori omfatter også personer, hvor vi får 'nummer i uorden'/'tre klang', samt personer der er flyttet fra adressen uden mulighed for telefonisk kontakt.

Ikke fundet nummer

Vores telefonsøgning har ikke fundet et telefonnummer til interviewpersonen.

Ikke relevant

Interviewpersonen har oplyst at de ikke er relevante for undersøgelsen.

4.7. Særligt for denne undersøgelse

Her viser det sig, at der er forskelle i svarprocenterne på næsten alle variable, der indgår i modellen.

Tabel 3.

svar – Stik- Populati-on

	1. Svar	2. Stik	3. Pop	**1. Svar**	**2. Stik**	**3. Pop**
	———— Antal ————			———— Pct. ————		
I alt	981	1.528	4.177.975	100	100	100
Køn						
1. Mænd	438	726	2.093.647	45	48	50
2. Kvinder	543	802	2.084.328	55	53	50
Alder pr. '01JAN2014'						
16-29 år	193	355	989.842	20	23	24
30-39 år	139	217	687.060	14	14	16
40-49 år	181	287	809.757	19	19	19
50-64 år	300	424	1.077.073	31	28	26
65-74 år	168	245	614.243	17	16	15
Geografi						
Bornholm	9	12	29.984	1	1	1
Byen København	115	203	574.306	12	13	14
Fyn	90	148	360.260	9	10	9
Københavns omegn	83	135	385.207	9	9	9
Nordjylland	113	171	431.062	12	11	10
Nordsjælland	73	119	324.738	7	8	8
Sydjylland	142	203	523.628	15	13	13
Vest- og Sydsjælland	86	143	427.785	9	9	10
Vestjylland	84	117	309.598	9	8	7
Østjylland	131	208	635.498	13	14	15
Østsjælland	55	69	175.909	6	5	4
Uddannelse						
1. Grundskole	272	503	1.403.439	28	33	34
2. Ungdoms udd.	389	582	1.677.053	40	38	40

3. Korte Videregående udd.	60	80	179.152	6	5	4
4. Mellemlange Videregående udd.	142	204	529.926	15	13	13
5. Lange Videregående udd.	118	159	388.405	12	10	9
Arbejdsfunktion						
0. Militært arbejde	2	4	24.612	0	0	1
1. Ledelse+arbejde, færdigheder højeste niveau	216	309	782.666	22	20	19
2. Arbejde, færdigheder mellemniveau+kontor	133	185	502.848	14	12	12
3. Salgs-, service- og omsorgsarbejde	124	183	553.984	13	12	13
4. Landbrug, gartner, skovbrug	15	20	36.241	2	1	1
5. Håndværkspræget arbejde	53	79	233.685	5	5	6
6. Proces, maskinoperatør, transport, anlæg	28	42	139.773	3	3	3
7. Andet arbejde	57	96	279.139	6	6	7
9. Ingen oplysning	353	610	1.625.027	36	40	39
Socioøkonomisk status						
1. Studerende	90	141	427.777	9	9	10
2. Lønmodtager grundniveau	297	451	1.367.287	30	30	33
3. Lønmodtager mellemniveau+	276	387	969.564	28	25	23
4. Selvstændig	48	70	167.983	5	5	4
5. Uden for erhverv	270	479	1.245.364	28	31	30
BRUTTO						
1. Ingen indkomst	33	80	182.634	3	5	4
2. -200	329	575	1.576.233	34	38	38
3. 200-350	300	430	1.251.184	31	28	30
4. 350-500	209	291	778.934	21	19	19
5. 500-750	85	115	282.368	9	8	7
6. 750+	25	37	106.622	3	2	3
Herkomst						
Dansk oprindelse	909	1.351	3.681.407	93	88	88
Indvandrere/Efterkommere	72	177	496.568	7	12	12

5. Kilder

BEC, 11-11-2013: Nye tal og tendenser i mobilbanken, http://www.bec.dk/bec/presse/nyheder/tal-og-tendenser-i-mobilbanken.aspx?PID=4143&M=NewsV2&Action=1

Betalingsrådet, november 2013: Rapport om nye betalingsløsninger, http://nationalbanken.dk/C1256B730054214F/sysOakFil/Betalingsraadets_rapport_nye_betalingsloesninger_nov2013/$File/Betalingsraadet_Rapport_om_nye_betalingsloesninger.pdf

CSO Online, 07-09-2012: Mobile malware shifting to SMS fraud, http://www.csoonline.com/article/715700/mobile-malware-shifting-to-sms-fraud

Danmarks Statistik, november 2013: It-anvendelse i befolkningen 2013, http://www.dst.dk/pubpdf/18685/itanv

Danske Bank, 4-12-2013: Telefoninterview med Jesper Nielsen, Danske Bank.

Danske Bank, 11-12-2013: Telefoninterview med Peter Kjærgaard Nielsen, Danske Bank.

DIBS, 1-12-2013: Dansk E-handel 2013 - E-handlen boomer fortsat, http://www.dibs.dk/news/dibs-e-handel-2013

DIBS, 3-12-2013: Telefoninterview med Lars Juul Dalsted, DIBS.

DKCERT, 2011: Smartphones – ulven er ankommet, https://www.cert.dk/pdf/indsigtsmartphones.pdf

EPN, 29-11-2013: Danskerne shopper løs med mobilen, http://epn.dk/brancher/detail/ECE6293187/danskerne-shopper-loes-med-mobilen/

FireEye, 26-11-2013: Dissecting Android KorBanker, http://www.fireeye.com/blog/technical/targeted-attack/2013/11/dissecting-android-korbanker.html

Kriminalitet i en digitaliseret verden, 2013: Samlet rapport, Peter Kruize, Det Juridiske Fakultet, Københavns Universitet, http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Kriminalitet%20i%20en%20digitaliseret%20verden%20samlet%20rapport.pdf

Microsoft Security Intelligence Report, http://www.microsoft.com/security/sir/default.aspx

Nets, 22-8-2013: Nets indgår aftaler om udviklingen af fremtidens mobilbetaling, http://www.nets.eu/dk-da/Om/nyheder-og-presse/Pages/Nets-indg%C3%A5r-aftaler-om-udviklingen-af-fremtidens-mobilbetaling.aspx

Nets, 26-11-2013: Mail med besvarelse af spørgsmål stillet af DKCERT om Mobilpenge og andre løsninger til mobilbetaling.

NSS 11-12-2013: NSS Labs: View From the Precipice - Mobile Financial Malware, https://www.nsslabs.com/reports/view-precipice-mobile-financial-malware

PCI DSS: PCI Security Standards Council, https://www.pcisecuritystandards.org/