CIT-AWARE-09 - En undersøgelse af it-sikkerhed blandt borgerne i Danmark

Sharp, Robin

Publication date:
2010

Document Version
Publisher's PDF, also known as Version of record

CIT-AWARE-09
En undersøgelse af it-sikkerhed blandt borgerne i Danmark

Redigeret af:
Robin Sharp
Informatik og Matematisk Modellering
Danmarks Tekniske Universitet

Maj 2010

Kongens Lyngby 2010
IMM–Technical report–2010–07

Technical University of Denmark
Informatics and Mathematical Modelling
Building 321, DK-2800 Kgs. Lyngby, Denmark.
Phone +45 45253351, Fax +45 45882673
reception@imm.dtu.dk
www.imm.dtu.dk
IMM–TECHNICAL REPORT: ISSN 1601–2321

Resumé

Denne rapport præsenterer og giver an analyse af resultaterne fra en undersøgelse af it-sikkerhed blandt borgere i Danmark. Undersøgelsen blev gennemført i efteråret 2009 af CIT-AWARE konsortiet, som et led i det overordnede projekt "Borgernes IT-sikkerhed", der blev støttet af Statens Strategiske Forskningsråd.

Undersøgelsen blev udført som en anonym, webbaseret spørgeskemaundersøgelse, hvor der blev stillet spørgsmål inden for 8 tekniske områder: Generelt kendskab til it-sikkerhed, Datasikring, Adgangskoder, Virus og andet ondskabsfuldt programmel, E-mail, Download, E-banking og e-handel og Mobiltelefoner.

Undersøgelsens formål var at belyse hvad folk ved om it-sikkerhed og de praktiske foranstaltninger, der bruges for at opnå et højt sikkerhedsniveau, hvad folk har af holdninger til it-sikkerhed og hvordan folk opfører sig i praksis i situationer, hvor it-sikkerhed er af afgørende betydning. For at registrere den praktiske opførsel blev relevante spørgsmål stillet inden for rammerne af nogle interaktive scenarier, der efterligner situationer fra den almindelige brug af computeren. Denne tekniske tiltag blev kombineret med feedback til respondenterne med hensyn til, hvor godt de klarede sig i forhold til god sikkerhedsmæssig praksis. Det kunne konstateres, at denne fremgangsmåde havde en målbar oplærende effekt og således forøgede respondenternes præstation med hensyn til it-sikkerhed, en effekt som respondenterne selv fandt meget tilfredsstillende.

Rapporten består af to dele. Del I beskriver undersøgelsens form og de overordnede resultater og anbefalinger. Del II indeholder en mere detaljeret præsentation af de spørgsmål, der indgik i undersøgelsen, og detaljeret statistisk materiale om de svar, som blev indsamlet.

Bidragsydere

Denne rapport er blevet produceret af ***CIT-AWARE***-konsortiet:

Robin Sharp (Danmarks Tekniske Universitet)
Lisa Gjedde (Danmarks Pædagogiske Universitetsskole, Aarhus Universitet)
Helle Meldgaard (DK-CERT/UNI-C)
Preben Andersen (DK-CERT/UNI-C)

i samarbejde med virksomheden

Telia Stofa A/S

Rapporten er tilrettelagt og editeret af Robin Sharp.

Yderligere detaljer om ***CIT-AWARE***-projektet kan findes på webstedet:

`http://www.cit-aware.dk`

Tilkendegivelser

CIT-AWARE er et projekt inden for forskningsprogrammet *"Borgernes IT-sikkerhed"*, der støttes af Danmarks Strategiske Forskningsråd. Deltagerne i projektet vil gerne udtrykke deres taknemmelighed for denne støtte.

Indhold

I Undersøgelsen og dens resultater **1**

1 Indledende bemærkninger **3**

1.1 Respondenterne 4

1.2 Spørgeskemaets form 4

1.3 Udvikling af Spørgsmålene 7

2 Analyse af de indsamlede svar **9**

2.1 Viden om it-sikkerhed 9

2.2 Holdninger til it-sikkerhed 14

2.3 Opførsel i sikkerhedsmæssigt kritiske situationer 17

2.4 Læringsprocessens effekt 20

3 Konklusioner **23**

3.1 Iøjnefaldende resultater 23

3.2 Anbefalinger 26

II De samlede spørgsmål og svar **29**

4 Statistik **31**

4.1 Opstilling af spørgsmål og svar i dette dokument 31

Spørgsmålsgrupper **33**

0 Lidt om dig selv... **33**

1 Generelt kendskab til it-sikkerhed **38**

2 Datasikring **48**

3 Adgangskoder **52**

4 Virus og andet ondskabsfuldt **58**

5 e-mail **61**

6 Download **67**

7 e-banking og e-handel **70**

8 Mobiltelefoner **79**

Appendices **81**

A Samlede tekstsvar på spørgsmål **81**
A.1 Beskæftigelse . . . 81
A.2 Anden anvendelse af computeren . . . 88
A.3 Andre videnskilder . . . 89
A.4 Andre, der tager sig af it-sikkerhed i hjemmet . . . 92
A.5 Medier til sikkerhedskopier . . . 92
A.6 Gemning af sikkerhedskopier . . . 94
A.7 Hvordan huskes adgangskoderne . . . 95
A.8 Hvordan ser en god adgangskode ud? . . . 98
A.9 Opdatering af virusskanner . . . 99
A.10 Fjernelse af virus . . . 100
A.11 Hvordan bestemmes, om links følges . . . 100
A.12 Harmløse linknavne . . . 101
A.13 Hvordan bestemmes, om vedhæftede filer åbnes . . . 103
A.14 Harmløse filnavne . . . 104
A.15 Håndtering af fortrolige e-mails . . . 107

Litteratur **113**

Del I

Undersøgelsen og dens resultater

Kapitel 1

Indledende bemærkninger

Dette dokument opsummerer og kommenterer de statistiske oplysninger, der kan udtrækkes fra svarene på CIT-AWAREs webbaserede spørgeskema om it-sikkerhed blandt almindelige borgere. Spørgeskemaet var tilgængeligt for respondenter fra medio november indtil udgangen af december 2009.

Hovedvægten i denne analyse lægges på svarene for de enkelte spørgsmål. Herudover er der kigget på udvalgte relationer mellem svarene – for eksempel for at se, om forskellige svar i de mere detaljerede spørgsmål senere i spørgeskemaet hænger sammen med folks erfaring, beskæftigelse, alder, måde at bruge computeren på eller andre faktorer. Da der er utallige sådanne relationer, der i princippet kunne belyses, har det her været nødvendigt at foretage et valg. Den interesserede læser, der savner bestemte oplysninger, er velkommen til at henvende sig til forfatterne, hvorefter vi vil gøre hvad vi kan for at finde oplysningerne frem, hvis dette er muligt.

Nærværende rapport falder i to dele. Den første del beskriver i kapitel 1 selve undersøgelsen, giver i kapitel 2 en analyse af de opsamlede svar og slutter i kapitel 3 med de konklusioner, som vi har kunnet drage fra undersøgelsen. I den anden del af rapporten vises de spørgsmål, der indgik i undersøgelsen, og de samlede rå svar. Nogle spørgsmål kunne besvares med en “fritekst” og så vidt muligt er disse svar samlet på en systematiseret måde i Appendix A af anden del.

Overordnede data fra spørgeskemaværktøjet

Number of responses processed:	707
Total responses in survey:	707
Number of 100% complete responses:	419

Af dette kan man se, at 288 respondenter påbegyndte spørgeskemaet, men ikke fuldførte det. (For nogle ganske få ser det ud, som om de slet ikke besvarede så meget som et enkelt spørgsmål, da det kom til stykket.) Det er nok tingenes vilkår.

1.1 Respondenterne

Kontakt til respondenterne i den del af undersøgelsen, der rapporteres her, blev formidlet gennem Telia Stofa A/S i Horsens, der annonceret undersøgelsen i deres nyhedsbrev til deres Internetabonnenter. Af hensyn til lovgivningen skulle respondenterne give deres tilladelse til at blive kontaktet af forskergruppen bag undersøgelsen. De, der gav deres tilladelse, fik tilsendt en invitation i form af en e-mail med en personlig link, der gav adgang til selve undersøgelsen. Ca. halvdelen af de inviterede reflekterede på invitationen. Af de nærmere svar fremgår det, at respondenterne i alt væsentligt var voksne. Mindre end 0,5% var under 20 år. Til gengæld var der en pæn repræsentation af ældre borgere: 38% var ældre end 60.

Denne fremgangsmåde ved udvælgelse af respondenter giver en vis bias i forhold til tilfældig udvælgelse fra hele den danske befolkning, idet deltagere i undersøgelsen skal have en computer og en Internetforbindelse, og de skal udvise tilstrækkelig interesse for sagen til at reflektere på invitationen og til at afse tid til at besvare spørgeskemaet. Med disse forbehold viser svarene på de demografiske spørgsmål imidlertid, at respondenterne havde en aldersfordeling og en beskæftigelsesfordeling, der i alt væsentligt svarer til det forventelige i den voksne befolkning.

1.2 Spørgeskemaets form

Spørgeskemaet er udviklet ved hjælp af værktøjet LimeSurvey, et velrenommeret open source produkt til dette formål. Undersøgelsen blev afviklet som en anonym undersøgelse i den forstand, at de opsamlede svar ikke kunne føres tilbage til de enkelte respondenter. Respondenter kunne kun gå fremad igennem spørgeskemaet og ikke gå tilbage til tidligere besvarede spørgsmål for at se, ændre eller rette i tidligere svar.

Der blev benyttet en række forskellige spørgsmålstyper, herunder:

- Simple spørgsmål med mulighed for at vælge een ud af en række prædefinerede svarmuligheder.
  (F.eks. “Kender du udtrykket ‘en virusskanner´?”, med mulige svar *Ja-Nej*, “Har du en virusskanner i funktion på din computer?”, med mulige svar *Ja-Nej-Ved ikke* og “Hvad er din status på arbejdsmarkedet?” med mulige svar *Fuldtidsansat-Deltidsansat-Pensionist-Studerende/under uddannelse-Ikke i arbejde*.)
- Spørgsmål med mulighed for at vælge flere ud af en række prædefinerede svarmuligheder.
  (F.eks. “Hvilken uddannelse (eller uddannelser) har du gennemgået?”, med mulige svar *Folkeskolens 9. klasse-10. klasse-Gymnasiet-Kontoruddannelse-Bankuddannelse-Håndværker/faglært-Mellemlang videregående-Længere videregående-Andet*.)
- Spørgsmål, der kræver et tal som svar (F.eks. “I hvor mange år (ca.) har du brugt computere?”).
- Spørgsmål, der giver respondenten mulighed for at afgive et vilkårligt skriftligt svar (f.eks. med en forklaring, en angivelse af beskæftigelse osv.).

Det var godt! Så kan du nok spare dig selv for en hel del bøvl.

Det ville være ret farligt at klikke på linken her. Hvis du flyttede musen over linken, ville du se, at den henviser til et websted, hvor der er to meget mistænkelige forhold:

1. Webadressen har form af lutter tal (83.96.231.108). Normale websider kendes ved "navne" (som godt nok kan være lidt mystifistiske eller indeholde enkelte tal, men ikke bare tal!).
2. Websidens navn har endelsen ".exe". Dette viser, at der er tale om et program, snarere end en almindelig webside. Hvis du klikker på linken, udføres programmet (så vidt det er muligt) på din egen computer, hvor det kan gøre skade.

Figur 1.1: Et respons efter et svar, der indikerer en sikkerhedsmæssigt fornuftig strategi

Det var karakteristisk for undersøgelsen, at en del af de mere tekniske spørgsmål var stillet i forhold til interaktive scenarier, der lignede noget, som respondenten kunne opleve i den virkelige verden, såsom en ægte eller falsk webside, der blev vist frem på skærmen. Rationalet bag brugen af sådanne interaktive scenarier til at fremme læring i komplekse tekniske emner er blevet præsenteret i [3, 6, 2]. I det aktuelle spørgeskema var der tre former for interaktivt scenarie, der blev benyttet:

1. Fremvisning af en webside eller mail, således at linkdestinationer og andre sikkerhedsrelevant information kunne frembringes ved brug af “mouseover”, ligesom i en almindelig browser.
2. Fremvisning af en webside med mulighed for “mouseover” (som under pkt.1̃), men hvor respondenten bliver bedt om at indikere, hvor på siden, der var elementer, der gave tillid til sidens ægthed, og hvor der var elementer, der virkede mistænkelige.
3. Opstillinger, hvor respondenten interaktivt kunne flytte rundt på elementerne på siden for at placere lignende elementer i nærheden af hinanden.

Efter hvert spørgsmål (eller evt. gruppe af spørgsmål) af denne type fik respondenten et respons fra systemet, med feedback og vurdering af vedkommendes svar. For eksempel ved et svar, der indikerer fornuftig opførsel, blev der givet:

- Et positivt kvalitativt respons, typisk i form af et billede af en glad hund;
- En positiv, mere teknisk forklaring

som illustreret i Figur 1.1. Ved et svar, der derimod indikerer uvidenhed eller mindre fornuftig opførsel, blev der givet:

- Et negativt kvalitativt respons, typisk i form af et billede af en ulykkelig hund;

Uha, det ville være meget uheldigt at klikke på linken her.

Hvis du flyttede musen over linken, ville du se, at den henviser til et websted, hvor der er to meget mistænkelige forhold:

1. Webadressen har form af lutter tal (83.96.231.108). Normale websider kendes ved "navne" (som godt nok kan være list mystifistiske, eller indeholder enkelte tal, men ikke bare tal!).
2. Websidens navn har endelsen ".exe". Dette viser, at der er tale om et program, snarere end en almindelig webside. Hvis du klikker på linken, udføres programmet (så vidt det er muligt) på din egen computer, hvor det kan gøre skade.

Figur 1.2: Et respons efter et svar, der indikerer uvidenhed eller en sikkerhedsmæssigt mindre fornuftig strategi

- En mere teknisk forklaring på hvor man skal passe på.

som illustreret i Figur 1.2. Denne kombination af "interaktive spørgsmål" og umiddelbar feedback – både på en kvalitativ og på en mere detaljeret, teknisk form – til respondenterne udgør et meget væsentligt element i forsøget på at bibringe deltagere nye erkendelser i forhold til it-sikkerhed. Den pædagogiske teori, der ligger til grund for denne tilgang til læring, er præsenteret i [6].

Når en respondent var færdig med spørgeskemaets sidste spørgsmål, blev LimeSurveys *assessment* facilitet brugt til at give respondenten en *overordnet vurdering* af hans/hendes præstation, set fra et it-sikkerhedsmæssigt synspunkt. Denne vurdering var baseret på en pointgivning for de spørgsmål, hvor det var muligt at afgøre, om respondentens svar indikerede sikkerhedsmæssigt forsvarlig opførsel (som gav positive point), neutral opførsel (som gav nul point) eller mindre heldig opførsel (som gav negative point). Rent faktuelle spørgsmål om respondentens baggrund, beskæftigelse og viden om it-sikkerhed o.l. bidrog ikke til pointsummen. Den samlede vurdering kunne være, at respondenten:

- Udviste *ikke særlig sikker* opførsel. Ved denne vurdering fik respondenten meddelelsen:

  > *"Din måde at bruge computeren på er ikke særlig sikker. Du risikerer at få nogle ubehagelige overraskelser fra tid til anden. Måske burde du overveje at spørge nogen om råd med hensyn til IT-sikkerhed."*

- Udviste en *lidt blandet* opførsel med nogle gode og nogle dårlige sider. Ved denne vurdering fik respondenten meddelelsen:

  > *"Det ser ud som om du på nogle områder vælger de sikre løsninger, mens du på andre områder vælger mindre sikre løsninger, som kan bringe dig i fare. Det*

> *kan være svært at være 100% oppe på dupperne med det hele, men vi håber, at vi i forbindelse med denne undersøgelse har givet dig nogle gode råd om IT-sikkerhed, som du kan bruge fremover.*"

- Udviste en *rimelig sikker* opførsel, med kun enkelte svigt. Ved denne vurdering fik respondenten meddelelsen:

  > *"Din måde at bruge computeren på viser et rimelig godt kendskab til IT-sikkerhed. En gang imellem ser det ud, som om det svigter for dig. Men vi håber, at de råd, som vi har givet i forbindelse med dette spørgeskema, kan hjælpe dig til at være endnu mere sikker i fremtiden.*"

- Udviste *ret sikker* opførsel. Ved denne vurdering fik respondenten meddelelsen:

  > *"Din måde at bruge computeren på er ret fornuftig, set fra et IT-sikkerheds synspunkt. Bliv bare ved! Vi håber, du har fået nogle yderligere impulser fra at deltage i denne undersøgelse.*"

1.3 Udvikling af Spørgsmålene

De detaljerede spørgsmål bleve udviklet i en iterativ proces, hvorunder forskellige grupper af respondenter blev brugt som testpersoner. Et første udkast til spørgeskema blev udviklet i form af et interviewskema, som blev prøvet af på en række på 15 testpersoner. Samtidigt blev en række fokusgrupper benyttet for at indsamle oplysninger om, hvad almindelige it-brugere anser for de væsentligste problemer i forhold til it-sikkerhed. Spørgeskemaet blev derpå rettet til i lyset af erfaringerne fra de indledende interviews og fokusgruppeundersøgelsen, og billedmateriale til de enkelte spørgsmål blev udviklet. Andre testgrupper blev dernæst inddraget for at undersøge, om spørgsmålene og det tilhørende billedmateriale nu var fuldt forståelige. På basis af de forskellige gruppers kommentarer blev spørgeskemaet rettet til og dens endelige version udviklet. Den indeholdte en indledende række demografiske spørgsmål, samt spørgsmål inden for 8 tekniske områder:

1. Generelt kendskab til it-sikkerhed
2. Datasikring
3. Adgangskoder
4. Virus og andet ondskabsfuldt programmel
5. E-mail
6. Download
7. E-banking og e-handel
8. Mobiltelefoner

Kapitel 2

Analyse af de indsamlede svar

Overordnet set afslører de indsamlede svar en række forhold, som giver anledning til eftertanke. I overensstemmelse med det overordnede formål med undersøgelsen deler vi disse forhold op, alt efter om de relaterer til:

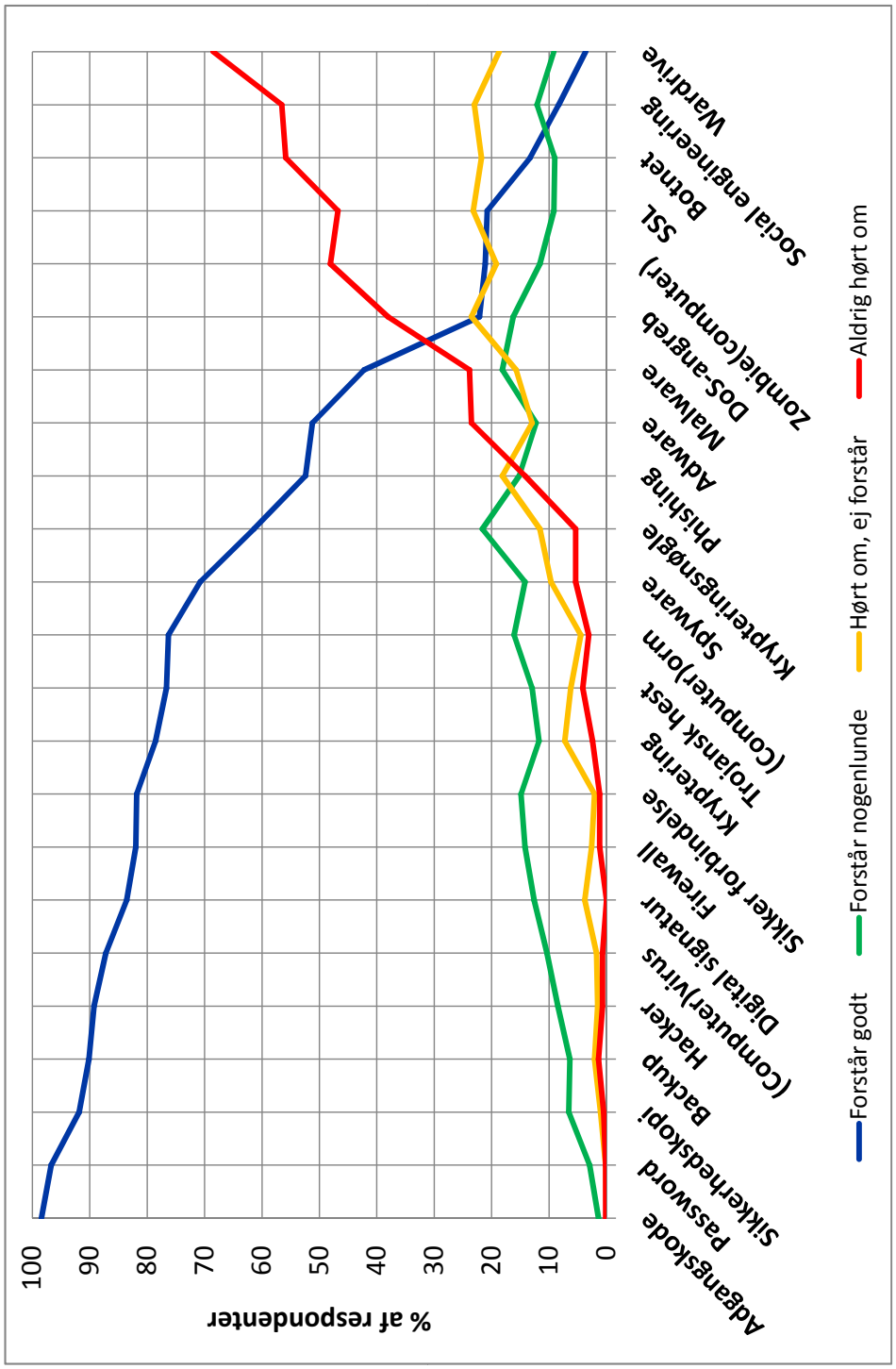
1. Hvad folk ved om it-sikkerhed og de praktiske foranstaltninger, der bruges for at give et højt sikkerhedsniveau.
2. Hvad folk har af holdninger til it-sikkerhed.
3. Hvordan folk opfører sig i situationer, hvor it-sikkerhed er af afgørende betydning.

Ved udvikling af undersøgelsen havde vi den hypotese, at brugen af interaktive scenarier i nogle af spørgsmålene ville stimulere respondenternes *implicitte viden* om it-sikkerhed, således at respondenterne faktisk ville forbedre deres præstation med hensyn til it-sikkerhed ved at gennemføre spørgeskemaet. I den sidste del af kapitlet ser vi nærmere på, om denne hypotese kan bekræftes eller ej.

2.1 Viden om it-sikkerhed

Kendskab til tekniske ord En hel del af de tekniske ord, som flittigt benyttes i avisartikler, i radioen og på TV, er ukendt af et bredere publikum. (Dette er checket på forskellig vis i flere forskellige spørgsmål.) Denne observation er især bekymrende, fordi ord, der ofte benyttes i aktuelle forholdsregler for it-sikkerhed (såsom SSL) eller som refererer til aktuelle farer i forbindelse med internettet (såsom Phishing og Botnet) er iblandt de termer, som ikke er godt forstået. Figur 2.1 opsummerer svarene på Spørgsmål Q1.14, der handler netop om disse forhold.

Interessant nok ser det ud til at være underordnet, om engelske eller danske gloser benyttes: Stort set lige mange svarede, at de havde en god forståelse af begreberne Password og Adgangskode, og tilsvarende Backup og Sikkerhedskopi.



Figur 2.1: Svarene på spørgsmål Q1.14, ordnet efter graden af forståelse af begreberne

Begrebsforvirring En mulig konsekvens af manglende forståelse af hyppigt forekommende tekniske ord er, at det let giver anledning til en del begrebsforvirring. For eksempel var der omkring 2/3 af respondenterne, der mente at en virusskanner ville fange et ikke-ønskeligt *indhold* i en e-mail, såsom:

- En anmodning om at blive tilsendt personlige oplysninger,
- Et uønsket seksuelt tilbud,
- Et uønsket tilbud om varer eller tjenester.

Om noget ville sådanne e-mails snarere blive fanget af et *spamfilter* end en virusskanner.

Ydermere mente næsten 2/3, at virusskanneren også ville fange indirekte henvisninger til farlige websider, såsom:

- En link til en webside, hvor der er en anmodning om personlige oplysninger,
- En link til en webside, hvor opslag på siden vil resulterer i, at et skadeligt program installeres.

Dette ligger uden for rækkeviden af de fleste virusskannere idag.

Informationskilder Den hyppigste kilde til information om it-sikkerhed (Q1.9) er selve internettet, mens andet skriftligt materiale, såsom aviser og pjecer om it-sikkerhed, er forholdsvis lidt benyttet.

Blandt de respondenter, der svarer, at de (bl.a.) henter information fra "Andet" medium, er der blandt begyndere og folk, der ikke har været på kursus, en stor tendens til at få information fra venner og bekendte, mens de mere avancerede brugere bruger fagtidsskrifter, lærebøger og lignende kilder.

Korrelationer mellem baggrund og informationskilde For at se, om der var nogen sammenhæng mellem folks baggrund og hvor de får deres information om it-sikkerhed fra, undersøgte vi, om respondenternes foretrukne informationskilde(r) varierede med respondentens alder, (selvopfattede) erfaringsniveau eller uddannelse. Resultaterne kan opsummeres som følger:

	Alder			
Kilde	<20	20-39	40-59	>60
Aviser	IA	37%	50%	51%
Radio/TV	IA	30%	44%	39%
Pjecer	IA	8%	25%	35%
Internet	IA	77%	73%	57%
Andet	IA	20%	30%	27%

	Niveau			
Kilde	Uvidende	Begynder	Øvet	Ekspert
Aviser	22%	28%	55%	46%
Radio/TV	44%	22%	46%	35%
Pjecer	11%	18%	31%	22%
Internet	33%	44%	73%	90%
Andet	11%	27%	28%	37%

	Uddannelse							
Kilde	U1	U2	U3	U4	U5	U6	U7	U8
Aviser	37%	37%	49%	45%	60%	43%	57%	63%
Radio/TV	39%	42%	44%	41%	47%	36%	52%	39%
Pjecer	20%	28%	24%	34%	40%	28%	28%	28%
Internet	65%	70%	74%	56%	80%	67%	71%	75%
Andet	20%	28%	28%	23%	20%	28%	33%	31%

Her og senere i denne rapport svarer koderne for uddannelsesmæssig baggrund til de koder, der er brugt i spørgsmål Q0.7, nemlig:

U1	Folkeskolens 9. klasse	U5	Bankuddannelse
U2	10. klasse	U6	Håndværker / faglært
U3	Gymnasiet	U7	Mellemlang videregående
U4	Kontoruddannelse	U8	Længere videregående

En nærmere statistisk undersøgelse viser, at alder og erfaring har en statistisk signifikant indflydelse på valg af informationskilde, mens uddannelse har meget lidt betydning. En χ^2-test af de oprindelige data (hvor kontingenstabellerne ikke er reducerede til at vise procentsatser inden for de enkelte kategorier) giver en sandsynlighed af 0.86 for, at valget af informationskilder er uafhængigt af uddannelse. Derimod viser en tilsvarende χ^2-test, at sandsynligheden for, at valget er uafhængigt af alder, kun er 0.000066, mens sandsynligheden for, at valget er uafhængigt af erfaring er 5.6x10^{-15}. Ved inspektion af kontingenstabellerne kan man se, at jo ældre man bliver, des mere sandsynligt er det, at man tyer til skriftlige kilder såsom aviser og pjecer. De yngre og de mere erfarne it-brugere bruger internettet.

Brug af almene sikkerhedsmekanismer En række spørgsmål drejede sig om, om folk i praksis benytter alment tilgængelige sikkerhedsmekanismer. Her tænkes på, om respondenterne bruger:

- Regelmæssig backup (Q2.3), som her omfatter backup mindst en gang om måneden eller "efter behov";
- En virusskanner (Q4.4);
- En sikker forbindelse til mailserveren (Q5.14);
- En de mere sikre metoder til at få adgang til en netbank (Q7.9) – det vil sige at have sine netbanknøgler på et token eller kort, eller at bruge engangskoder.

Andre aspekter af god praksis, såsom håndtering af e-mail og valg af adgangskoder, diskuteres senere i denne rapport.

Det kunne indledningsvis konstateres, at mens brug af en virusskanner og regelmæssig backup er relativt udbredt, står det værre til med hensyn til brug af sikre forbindelser til mailserveren og brug af de mere sikre metoder til at få adgang til en netbank. Også her er det interessant at se, om folks alder eller erfaring har betydning for, om de benytter disse mekanismer på deres computer. Resultaterne kan opsummeres som følger:

	Alder			
Brug af beskyttelse	<20	20-39	40-59	>60
Regelmæssig backup (Q2.3)	IA	81%	80%	76%
Virusskanner (Q4.4)	IA	92%	98%	93%
Sikker forbindelse til mailserver (Q5.14)	IA	28%	30%	15%
Netbanknøgler på token/engangskoder (Q7.9)	IA	28%	30%	30%

	Niveau			
Brug af beskyttelse	Uvidende	Begynder	Øvet	Ekspert
Regelmæssig backup (Q2.3)	IA	72%	75%	100%
Virusskanner (Q4.4)	IA	98%	96%	88%
Sikker forbindelse til mailserver (Q5.14)	IA	16%	23%	28%
Netbanknøgler på token/engangskoder (Q7.9)	IA	26%	31%	30%

Note: Procentsatserne i ovenstående to tabeller er udregnet på en anden måde end i resten af tabellerne i denne rapport (se kapitel 4) for at give et bedre billede af, hvor stor en procentdel af den relevante gruppe af respondenter, der benyttede pågældende sikkerhedsmekanisme. Således inden for hver gruppe:

- Procentdelen af respondenter, der benytter regelmæssig backup, er udregnet i forhold til antallet af respondenter, der svarede på Q2.1 og Q2.5, om hvorvidt der i det hele taget blev taget backup.
- Procentdelen, der benyttede virusskanner, er beregnet i forhold til antallet af respondenter, der svarede på Q4.4.
- Procentdelen, der benyttede en sikker forbindelse til mailserveren, er beregnet i forhold til antallet af respondenter, der svarede på Q5.11, om hvorvidt man vidste, at det var muligt at aflytte adgangskoden.
- Procentdelen, der benyttede de mere sikre metoder til at tilgå netbanken, er beregnet i forhold til antallet, der svarede på Q7.2, at de faktisk benyttede en netbank.

En nærmere statistisk analyse af disse resultater viser, at hverken alder eller erfaring har nogen markant betydning for folks praksis inden for disse fire områder. En χ^2-test af de oprindelige data (hvor kontingenstabellerne ikke er reducerede til at vise procentsatser inden for de enkelte kategorier) giver en sandsynlighed af 0.31 for, at god praksis er uafhængig af alder og en sandsynlighed af 0.56 for, at den er uafhængig af erfaring. Det vil sige, at der ikke kan ses nogen statistisk signifikant forskel på respondenternes praksis, afhængigt af alder eller erfaring. Selv om vi ikke viser de relevante kontingenstabeller her, kunne vi heller ikke finde en statistisk signifikant forskel, der var afhængig af uddannelse eller (mere specifikt) antallet af it-sikkerhedskurser, som respondenterne havde gennemførte.

For de to sidste aspekter af god praksis – brug af en sikker forbindelse til mailserveren og brug af sikre metoder til at tilgå netbanken – er disse resultater særlig interessante, fordi de muligheder,

som forbrugerne har på disse områder, er afhængige af hvilken tjenesteleverandør, de benytter. Om man i det hele taget kan bruge en sikker forbindelse til mailserveren afhænger af hvilken ISP og mailtjeneste, man vælger. Og om man kan bruge en af de mere sikre metoder til netbanking afhænger af, hvilken bank man bruger. Den relativt lave hyppighed, hvormed de mere sikre løsninger anvendes, indikerer, at it-brugere enten er uopmærksomme på de sikkerhedsmæssige forskelle på forskellige leverandørers produkter, eller ikke vægter disse forskelle højt, når de skal vælge mailtjeneste eller bank.

Sikkerhed på mobiltelefoner Da brug af mobiltelefoner til andet end blot at telefonere er et relativt nyt fænomen, er det interessant at se, om der er særlige grupper, der allerede nu er bevidste om de risici, der kan være forbundet med brug af mobiltelefoner. Vi undersøgte derfor specifikt, om der skulle være nogen korrelation mellem folks alder og (selvvurderede) erfaringsniveau og deres brug af sikkerhedsmekanismer på mobiltelefonen (Q8.9). Resultaterne kan opsummeres som følger:

	Alder			
Brug af beskyttelse	<20	20-39	40-59	>60
Ja	IA	14%	29%	27%
Nej	IA	63%	44%	51%
Ved ikke	IA	24%	27%	21%

	Niveau			
Brug af beskyttelse	Uvidende	Begynder	Øvet	Ekspert
Ja	IA	26%	27%	27%
Nej	IA	48%	48%	58%
Ved ikke	IA	26%	25%	15%

Heller ikke her kunne en nærmere statistisk analyse påvise en statistisk signifikant afhængighed af hverken alder eller erfaring. En χ^2-test af de oprindelige data (hvor kontingenstabellerne ikke er reducerede til at vise procentsatser inden for de enkelte kategorier) giver en sandsynlighed af 0.08 for, at brug af beskyttelse på mobiltelefonen er uafhængig af alder og en sandsynlighed af 0.51 for, at den er uafhængig af erfaring.

2.2 Holdninger til it-sikkerhed

Tillid til netbanking og e-handel Respondenterne var meget tillidsfulde i forhold til netbanking og e-handel, som de vurderer til at være rimeligt sikre. Kun ca. 8,5% benyttede ikke en netbank, og kun 7% brugte hverken e-handel eller e-banking. Af dem, der benyttede en netbank, mente hele 99%, at det enten var sikkert eller nogenlunde sikkert – selv om 84% af alle respondenter havde set historier i medierne om problemer med netbankernes sikkerhed og 20% af netbankbrugerne havde følt, der kunne være en risiko for, at nogle prøvede at tømme deres bankkonto via internettet.

Af de (få) respondenter, der ikke brugte en netbank, var den hyppigste årsag til dette (68% af svarene) imidlertid, at de anså det for at være for usikkert, mens den næsthyppigste årsag (27% af svarene) var, at de foretrak at fortsætte med den gamle metode.

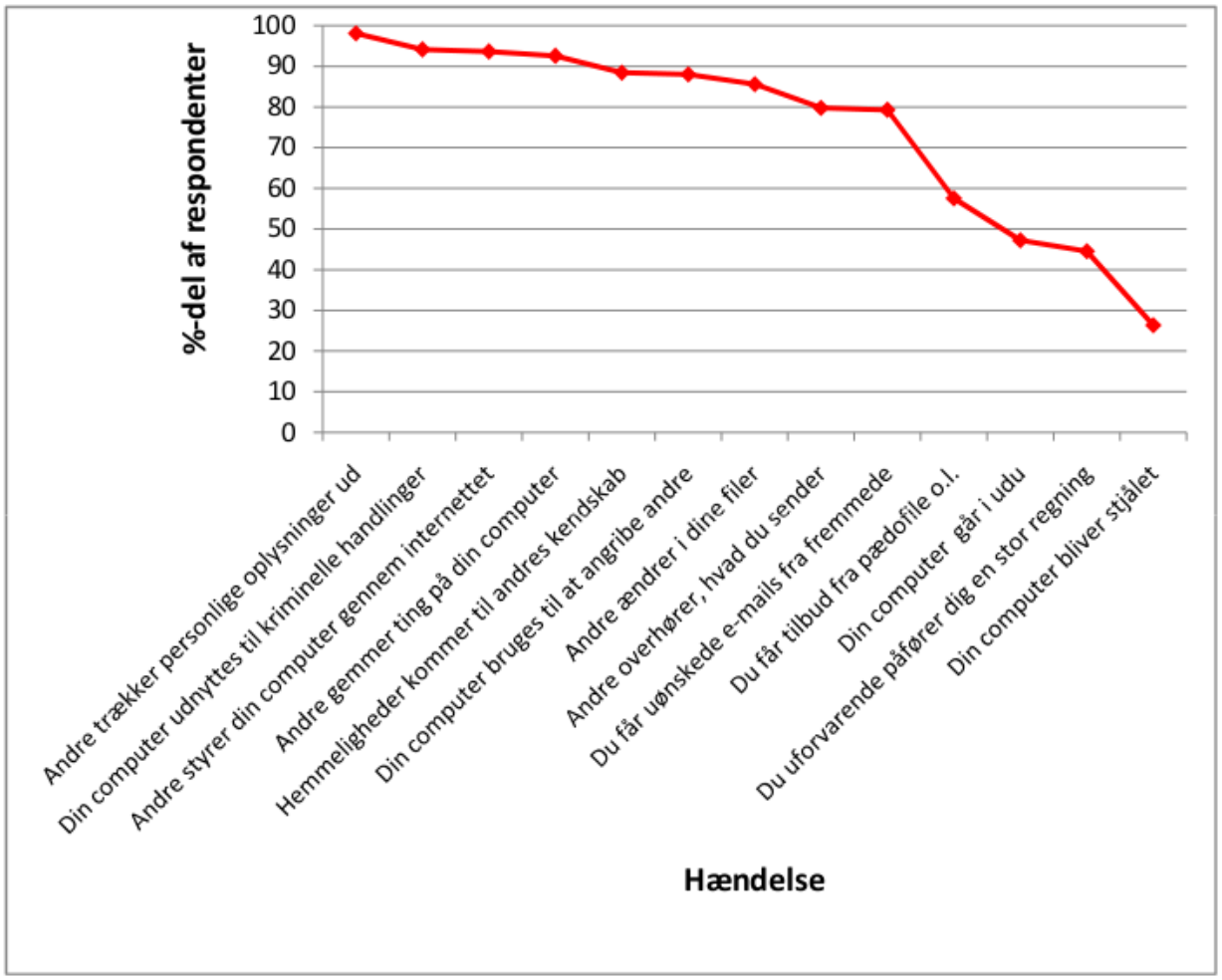
Disse observationer svarer meget godt til det generelle billede – kendt fra andre undersøgelser – af danske it-brugere som en folkefærd, der ser meget på de positive aspekter ved brugen af internettet, mens eventuelle farer nedtones eller ignoreres.

Opfattelser af hvad it-sikkerhed handler om Respondenterne er ikke helt konsekvente, når de vurderer, hvad der er væsentligt og hvad der er mindre væsentligt at beskytte sig imod. Et markant eksempel på dette er, at 68% af respondenter ikke mente, at det, at ens computer kunne blive stjålet, havde noget med it-sikkerhed at gøre. I virkeligheden medfører tyveri af ens computer en væsentlig fare for, at uvedkommende personer kan få fat i fortrolige eller personlige oplysninger, medmindre disse er særligt beskyttet på en eller anden måde. Figur 2.2 opsummerer opfattelserne af de 16 mulige farer, som der blev spurgt om i spørgsmål Q1.11; i figuren er svarene ordnede efter, hvor stor en brøkdel af respondenterne mente, at beskyttelse mod pågældende fare have noget med it-sikkerhed at gøre.

Rangordning af mulige farer Bedt om at rangordne en række på 16 mulige farer, alt efter hvilke det ville være vigtigst at beskytte sig imod (Q1.13b), var det vigtigste helt klart at beskytte sig imod, at *andre kan trække personlige oplysninger ud af ens computer*. Denne fare blev placeret i første rang med ca. dobbelt så mange "stemmer" som dens nærmeste konkurrent, som var beskyttelse imod, at *man kan tabe alt det, man har gemt på computeren*. I anden rang var det hyppigste valg beskyttelse imod, at *folk kan udnytte ens computer til kriminelle handlinger*, som dog kun fik ca. 40% flere stemmer end den nærmeste konkurrent, som var beskyttelse imod, at *andre kan komme til at styre ens computer gennem internettet*. I 3., 4. og 5. rang var der ingen klar vinder, idet flere potentielle farer fik omkring samme antal stemmer.

Det var interessant at se, at en af de farer, som blev betragtet som ret væsentlig af nogle af fokusgrupperne – at andre kan få fat i ens personlige data, når ens computer kasseres – ikke blev anset for en stor trussel af den meget større gruppe af respondenter, der deltog i den endelige spørgeskemaundersøgelse. Dette afspejler måske, at dette emne kom op i medierne lige før fokusgruppemøderne blev afholdt. Sådanne virkninger af midlertidig medieinteresse ses ofte og er en af de vigtige kilder til den kendte diskrepans mellem objektive vurderinger af risiko og menneskers (subjektive) opfattelse af risiko [4].

Valg af beskyttelsestrategi Respondenterne har ofte naive strategier for at beskytte sig. Et eksempel: Adspurgt om, hvordan de håndterer e-mails, som gerne skal holdes fortroligt (Q5.16), svarede ca. 12%, at de stolede på deres computers adgangskontrol til at sikre, at det kun var dem selv, der kunne tilgå de fortrolige mails. Denne strategi ignorerer det forhold, at andre via et angreb gennem nettet måske kunne trække personlige oplysninger ud af computeren, eller kunne få fat i fortrolige oplysninger fra en kasseret eller stjålet computer.



Figur 2.2: Procentdel af respondenter, der mente at beskyttelse mod de nævnte hændelser havde noget med it-sikkerhed at gøre

2.3 Opførsel i sikkerhedsmæssigt kritiske situationer

Diskrepans mellem viden og faktisk opførsel Respondenterne bruger ikke altid deres basale viden om it-sikkerhed, når de skal agere på nettet. For eksempel sagde mere end 80% af dem, der svarede på spørgsmål Q3.6, at en god adgangskode bestod af mindst 8 blandede store og små bogstaver og tal, hvad der må siges at være tegn på et rimelig højt vidensniveau. (Det ville have været endnu bedre, hvis de også havde taget med, at en god adgangskode skal indeholde tegn, som hverken er bogstaver eller tal, og at adgangskoden heller ikke må bestå af letkendelige ord; kun ca. 40% havde medtaget disse yderligere krav.) Men 42% af samme gruppe respondenter erkendte, at under halvdelen af deres adgangskoder var gode (Q3.7).

Det kan naturligvis argumenteres, at der kan være situationer, hvor en adgangskode kun beskytter mindre vigtige (eller endda helt uvæsentlige) oplysninger. Ikke desto mindre er det svært at tro, at det er tilfældet for en meget stor brøkdel af de anvendelser, hvor en adgangskode er påkrævet. En nærmere undersøgelse af dette spørgsmål kræver dog, at respondenterne oplyser, til hvilke formål de bruger de svage adgangskoder. Dette har vi af etiske grunde afstået fra at spørge om.

Korrelationer mellem baggrund og brug af gode adgangskoder For at se, om der var nogen sammenhæng mellem folks baggrund og deres brug af gode adgangskoder, undersøgte vi om den brøkdel af den enkelte respondents adgangskoder, som respondenten selv mente var gode (Q3.7), varierede med respondentens alder, (selvopfattede) erfaringsniveau eller uddannelse. Resultaterne kan opsummeres som følger:

	Alder			
Brøkdel	<20	20-39	40-59	>60
Ingen	IA	5%	3%	6%
Under 10%	IA	16%	13%	19%
10-50%	IA	20%	22%	25%
50-99%	IA	44%	43%	35%
Alle	IA	15%	19%	15%

	Niveau			
Brøkdel	Uvidende	Begynder	Øvet	Ekspert
Ingen	33%	8%	4%	3%
Under 10%	17%	21%	16%	7%
10-50%	50%	33%	23%	16%
50-99%	0%	21%	41%	45%
Alle	0%	17%	15%	28%

	Uddannelse							
Brøkdel	U1	U2	U3	U4	U5	U6	U7	U8
Ingen	6%	5%	6%	7%	0%	6%	2%	4%
Under 10%	15%	15%	13%	10%	25%	15%	16%	15%
10-50%	21%	23%	19%	17%	12%	27%	19%	26%
50-99%	38%	38%	43%	45%	25%	40%	50%	40%
Alle	19%	18%	19%	21%	38%	12%	13%	15%

En nærmere statistisk analyse af disse data viser, at hverken alder eller uddannelse har nogen markant betydning for brøkdelen af gode adgangskoder. En χ^2-test af de oprindelige data (hvor kontingenstabellerne ikke er reducerede til at vise procentsatser inden for de enkelte kategorier) giver en sandsynlighed af 0.70 for, at brøkdelen af gode adgangskoder er uafhængig af alder og en sandsynlighed af 0.95 for, at brøkdelen er uafhængig af uddannelse. Erfaringsniveauet har derimod betydning: en χ^2-test giver en sandsynlighed af kun 0.05 for, at brøkdelen af gode adgangskoder er uafhængig af erfaring. Inspektion af tabellerne viser, at " eksperterne" ville (måske ikke særligt overraskende) være mærkbart mere tilbøjelige til at vælge gode adgangskoder end de mindre erfarne brugere.

Korrelationer mellem baggrund og brug af forskellige adgangskoder For tilsvarende at se, om der var nogen sammenhæng mellem folks baggrund og deres brug af *forskellige* adgangskoder, undersøgte vi om den brøkdel af den enkelte respondents adgangskoder, som var forskellige (Q3.2), varierede med respondentens alder, (selvopfattede) erfaringsniveau eller uddannelse. Resultaterne kan opsummeres som følger:

	Alder			
Brøkdel	$<$20	20-39	40-59	$>$60
Ingen	IA	1%	2%	4%
Under 25%	IA	29%	30%	35%
Ca. 50%	IA	46%	32%	30%
Over 75%	IA	17%	21%	17%
Alle	IA	7%	16%	14%

	Niveau			
Brøkdel	Uvidende	Begynder	Øvet	Ekspert
Ingen	14%	10%	2%	0%
Under 25%	14%	38%	32%	27%
Ca. 50%	29%	22%	35%	34%
Over 75%	43%	11%	17%	30%
Alle	0%	19%	14%	9%

	Uddannelse							
Brøkdel	U1	U2	U3	U4	U5	U6	U7	U8
Ingen	2%	2%	0%	2%	0%	4%	3%	0%
Under 25%	33%	32%	27%	47%	62%	33%	27%	26%
Ca. 50%	37%	29%	40%	31%	15%	29%	34%	45%
Over 75%	15%	17%	20%	8%	15%	22%	19%	22%
Alle	13%	19%	12%	12%	8%	13%	17%	7%

Ligesom i spørgsmålet om brug af gode adgangskoder, havde erfaringsniveauet en mærkbar betydning for hvor stor en brøkdel af adgangskoderne var forskellige. En χ^2-test af de oprindelige data (hvor kontingenstabellerne ikke er reducerede til at vise procentsatser inden for de enkelte kategorier) giver en sandsynlighed af kun 0.003 for, at brøkdelen af forskellige adgangskoder er uafhængig af erfaring. Sandsynligheden for, at brøkdelen af forskellige adgangskoder er uafhængig af alder, er derimod 0.14 og sandsynligheden for, at brøkdelen er uafhængig af uddannelse, er 0.08; disse sandsynligheder er relativt små, men ikke statistisk signifikante indikationer (til 5% niveauet) af afhængighed.

Reglerne for accept af e-mail Den hyppigste regel, som folk bruger til at bestemme, om de vil acceptere e-mail – og navnlig, om de vil acceptere eventuelle indlejrede links eller vedhæftede filer – er, at de kigger på, om mailen kommer fra en, som de kender. Dette er en fornuftig regel, men kan ikke virke alene, idet mange brugere (ca. 44%) erkender, at de modtager e-mails, der kommer fra falske afsendere (Q5.4).

Vurdering af phishingsider Respondenterne kan let forvirres, når de står over for en webside eller lignende, hvor der er lavet phishingforsøg. Respondenterne fik for eksempel fremvist en række websider, hvoraf nogle var kopier af ægte sider, mens andre var falske sider, hvor der manglede et eller flere af de velkendte indikatorer, der typisk ville kendetegne en sikker side, i den forstand, at man kunne have tillid til, at oplysninger, der blev tastet ind på siden, ville gå til sidens øjensynlige udgiver uden at blive afsløret for uvedkommende:

1. Sidens webadresse (URL) starter med `https`:
2. Der findes en hængelås nederst i browservinduet eller oppe ved siden af adressefeltet.
3. Sideudgiverens webadresse står ved siden af hængelåsen.
4. Når man flytter musen over hængelåsen, kommer der en oplysning frem om, hvem der står inde for sidens ægthed.

I grove træk viser respondenternes svar, at folk var gode til at genkende de falske sider, hvis *alle* indikatorer manglede, mens de var meget i tvivl om ægtheden, hvis kun enkelte indikatorer ikke var til stede. Dette resultat er i bred overensstemmelse med resultaterne fra andre undersøgelser af it-brugeres reaktioner over for phishingsider, som for eksempel Dhamija, Tygar and Hearsts meget kendte undersøgelse [1] af, hvorfor en omhyggeligt konstrueret phishingside let kan narre selv ret erfarne brugere. It-brugere finder det i almindelighed svært at holde styr på alle de forskellige indikatorer, der skal bruges for at afgøre sagen.

Interessant nok blev respondenternes vurderinger mere pålidelige, som de kom igennem rækken af eksempler. Vi vender tilbage til dette aspekt ved spørgeskemaet i afsnit 2.4 nedenfor.

Betydning af viden for folks præstation Det er interessant at undersøge, om viden betyder noget for folks præstation, hvad it-sikkerhed angår. Dette kan vi få et fingerpeg om ved at kigge på svarene på spørgsmålene, der handlede om genkendelse af falske websider, hvor vi nu ser på, om svarene var afhængige af folks (selvopfattede) erfaringsniveau eller antallet af it-sikkerhedskurser, som de havde været igennem. Resultaterne kan opsummeres som følger:

	Niveau			
"Sikre svar"	Uvidende	Begynder	Øvet	Ekspert
Q7.8a	IA	21%	52%	60%
Q7.8b	IA	44%	54%	74%
Q7.8c	IA	42%	55%	70%
Q7.8d	IA	63%	85%	89%
Q7.8e	IA	45%	74%	91%
Q7.8f	IA	84%	97%	100%

	Antal sikkerhedskurser		
"Sikre svar"	Ingen	Eet	Flere
Q7.8a	49%	57%	38%
Q7.8b	55%	62%	50%
Q7.8c	56%	59%	50%
Q7.8d	83%	82%	75%
Q7.8e	74%	68%	75%
Q7.8f	96%	98%	100%

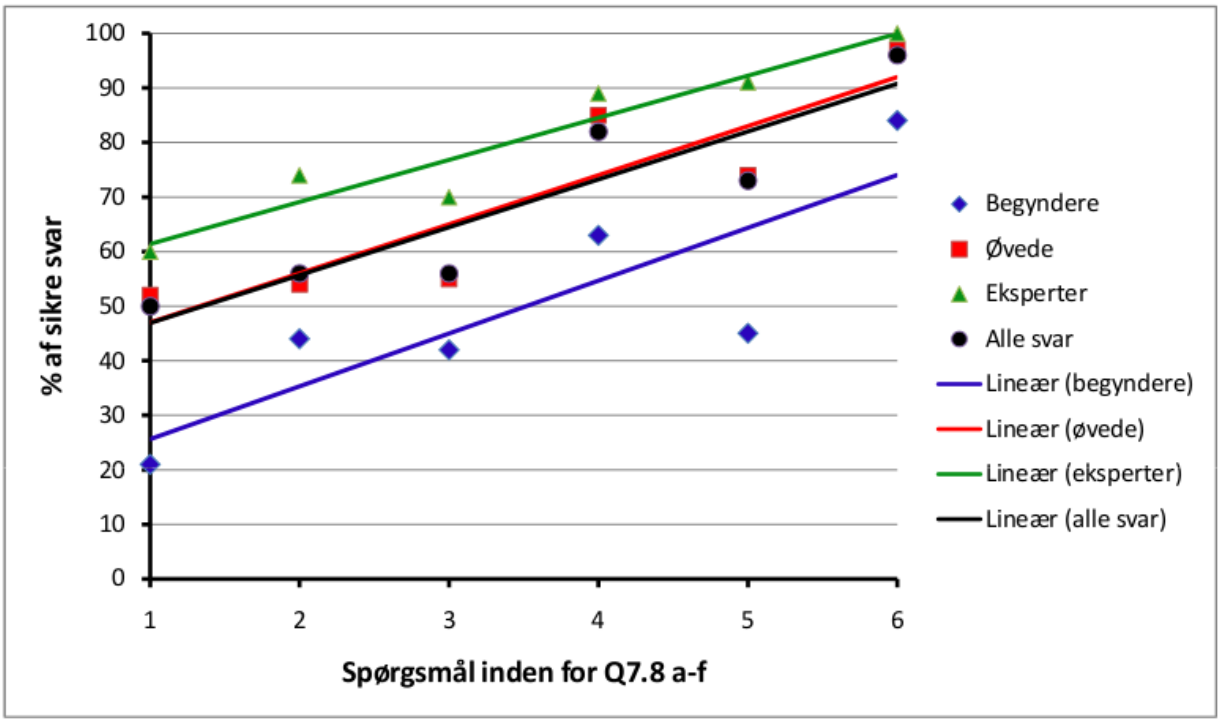
En nærmere analyse af disse viser, at antallet af gennemførte it-sikkerhedskurser kun har beskeden betydning for folks præstation på disse spørgsmål (der er ingen statistisk signifikant forskel mellem at have gennemført 0, 1 eller flere kurser). Erfaringsniveauet har derimod en signifikant betydning. Vi vender tilbage til dette nedenfor, hvor vi analyserer læringseffekten af de interaktive spørgsmål.

2.4 Læringsprocessens effekt

Betydning af it-sikkerhedskurser for folks præstation Blandt folk, der havde været på et eller flere it-sikkerhedskurser var der en meget lavere frekvens af "ved ikke" svar. Fornuften i de valgte strategier for at undgå sikkerhedsproblemer var dog ikke nødvendigvis bedre end for folk, der slet ikke havde været på kursus. Dette tyder på, at it-sikkerhedskurser i al almindelighed træner paratviden, men ikke hvordan denne viden bedst deployeres i praktiske situationer. Da vi ikke har haft mulighed for at checke de mange forskellige kurser, som respondenterne har nævnt, igennem, er det da muligt at der er store forskelle kurserne imellem. Dette spørgsmål

burde undersøges nærmere.

Læringseffekt af de interaktive spørgsmål Antallet af sikkerhedsmæssigt forsvarlige svar øges, som man kommer igennem de interaktive spørgsmål (inden for det enkelte emne) i vores spørgeskema. Klare eksempler på dette kan ses i tabellerne over antallet af "sikre svar" for spørgsmålene Q7.8a–f i forrige afsnit. Plot af procentdelen af sikre svar, som spørgsmålsrækken gennemløbes, kan ses i Figur 2.3 for de tre erfaringsniveauer *Begynder–Øvet–Ekspert* og for de samlede svar fra alle respondenter. Gruppen af *Uvidende* er udeladt, idet respondentgruppen var så lille, at den statistiske usikkerhed blev anset for for dominerende.



Figur 2.3: Udvikling i brøkdel af sikre svar

De rette linier er lineære regressionslinier for de fire sæt punkter. De beregnede Pearson korrelationskoefficienter (r^2), de tilsvarende F-værdier og sandsynligheden $P(F)$ for at denne r^2-værdi opstår ved et tilfælde – i modsætning til at det sker på grund af en ægte lineær sammenhæng mellem de to variable – og regressionsliniernes intercept a og hældning m for de fire sæt data kan ses i Tabel 2.1.

Alle de beregnede lineære regressionslinier har opadgående hældninger, hvad der må formodes at afspejle den oplærende virkning af at gennemgå en serie af relaterede spørgsmål med feedback efter hvert svar. Der er ingen statistisk signifikant forskel på hældningerne. På den anden side er der en statistisk signifikant (til 5%-niveauet) forskel på intercept-værdierne, der formodentlig kan tilskrives den intuitivt indlysende observation, at begyndere udviser en mindre sikker

	Begynder	Øvet	Ekspert	Alle svar
r^2	0.72	0.80	0.92	0.83
F	10.1	15.9	44.4	22.2
$P(F)$	0.027	0.012	0.002	0.008
Intercept, a	15.9$\pm$11.9	38.0$\pm$8.8	53.7$\pm$4.5	38.1$\pm$7.6
Hældning, m	9.68$\pm$3.05	9.00$\pm$2.25	7.71$\pm$1.16	8.77$\pm$1.95

Tabel 2.1: Statistiske parametre for regressionslinierne i figur 2.3

opførsel end eksperterne. Tilsvarende analyser af relationen mellem antallet af sikre svar og respondenternes alder eller andre baggrundsfaktorer viser den samme oplærende virkning. Samlet tyder alt dette på, at læringsprocessen er effektiv.

Kapitel 3

Konklusioner

I dette kapitel forsøger vi at samle de vigtigste konklusioner, som kan drages fra undersøgelsen. Disse konklusioner falder i to dele: Først opsummeres de mest markante resultater, som de fremgår af de grundlæggende svar, der er præsenteret i Del II af denne rapport, eller som de fremgår af den analyse, der blev præsenteret i kapitel 2. Derefter slutter vi Del I af rapporten af ved at give nogle anbefalinger til, hvordan fremtidige kampagner for it-sikkerhed blandt almindelige borgere med fordel kunne tilrettelægges for bedst at udnytte de resultater, der er kommet frem gennem undersøgelsen CIT-AWARE-09.

3.1 Iøjnefaldende resultater

Forståelse af tekniske ord En hel del af de tekniske ord, der ofte benyttes ved omtale af it-sikkerhed i radioen, på TV, i aviser og på websider, ser ud til at være ukendt af et bredere publikum. Dette er meget problematisk, fordi det betyder, at der er en væsentlig barriere for forståelse af de budskaber, der præsenteres. Blandt de relativt ukendte ord (Q1.14) tælles betegnelserne for væsentlige angrebsformer, såsom Phishing, DoS-angreb og Botnet, såvel som for den hyppigt anvendte beskyttelsemekanisme SSL. Hvis den almindelige borger ikke forstår, hvad de forskellige angrebsformer går ud på, er det meget svært for vedkommende at vælge passende modtræk. Tilsvarende, hvis borgerne ikke forstår hvad de enkelte beskyttelsesmekanismer gør godt for, vil de have svært ved at vælge de rigtige mekanismer til brug på deres computer. Hvis man vil have et budskab om it-sikkerhed kommunikeret til borgerne, er det nødvendigt at forklare de tekniske ord i budskabet en del bedre end man gør idag.

Denne mangel på forståelse af vigtige begreber smitter af på forskellige andre områder, som vi har undersøgt. For det første kunne vi konstatere en del begrebsforvirring. Et markant eksempel herpå var forvirring omkring, hvad en virusskanner kan beskytte imod. Selv om de fleste havde en rimelig klar idé om, hvordan en virusskanner virker så at sige rent mekanisk (Q4.3), og en stor brøkdel af dem havde en virusskanner installeret på deres computer (Q4.4), var der meget større usikkerhed vedrørende, hvad virusskanneren kan finde af skadelige ting (Q5.10),

så forventningerne til en virusskanners formåen var i mange tilfælde temmelig overdrevne. Her har leverandører af antivirusprodukter rettet mod almindelige it-brugere et behøv for bedre at forklare i klart sprog, hvad deres produkter rent faktisk kan.

Tilsvarende kunne det ses, at ret få respondenter brugte en sikker forbindelse til deres mailserver, hvad der ellers kunne sikre deres e-mail mod aflytning og således bidrage til at opretholde fortrolighed omkring private data. Her kan der være flere faktorer, der spiller en rolle. Dels, som vi har set, er begreber som SSL relativt lidt kendte, hvad der kan betyde, at mange almindelige brugere ville være usikre på, om det er noget, de skal bruge eller ej. Dels er ISP'er og andre leverandører af mailtjenester ofte meget tilbageholdende med at tilbyde adgang via en sikker forbindelse eller med at forklare, hvad en sådan forbindelse kan hjælpe it-brugeren til at opnå. Også her vil en forklarende oplysningskampagne kunne bidrage til at forøge borgernes it-sikkerhed.

Vurdering af farer Respondenterne udviste i det store og hele den for Danmark meget typiske tillidsfulde opførsel i forhold til internettet, og havde øjensynligt meget få betænkeligheder i forhold til brug af internettet til kommunikation, e-handel og e-banking. Men de var også rimelig overbeviste om, at der findes nogle farer, og der var overraskende bred enighed om, at den største fare var, at andre kunne trække personlige oplysninger ud af computeren (Q1.13b). Dette var langt fra den type ubehagelig hændelse, som de fleste respondenter eller folk i deres bekendtskabskreds rent faktisk selv havde oplevet [1], men var åbenbart den, som folk anså for den mest bekymrende.

Diskrepans mellem viden og praksis Der var en betydelig forskel inden for visse områder mellem respondenternes viden om, hvordan de skulle bære sig ad for at opnå et højt niveau af it-sikkerhed, og hvad de i praksis gjorde. Et markant eksempel var med hensyn til valg af adgangskoder, hvor en høj procentdel – op imod 80% – af respondenterne øjensynligt vidste, hvordan en god adgangskode skulle konstrueres, men hvor de i langt fra alle tilfælde valgte at benytte sådanne gode adgangskoder. Diskrepansen mellem viden og praksis var større for respondenter med mindre erfaring i brug af computere end for dem med større erfaring. Samtidig havde de mindre erfarne respondenter en større tendens til at genbruge samme adgangskode til forskellige formål (Q3.2) og til at bruge usikre metoder til at huske koderne (Q3.3), hvad der gør disse brugere mere eksponeret for angreb. En god oplysningskampagne rettet især mod nybegyndere ville gøre det vanskeligere for ondsindede personer at gætte sig til adgangskoderne og ville således højne niveauet for it-sikkerhed blandt borgerne.

Vurdering af phishingsider Undersøgelsen viste, at it-brugere let kunne forvirres af websider (og faktisk også af e-mails), der var blevet forfalsket med henblik på phishing efter personlige eller andre fortrolige oplysninger. Denne virkning er især markbar for websider, idet en bruger skal se efter mindst fire indikatorer på siden for at afgøre, om siden er en ægte side – eksempelvis

[1] De hyppigst oplevede hændelser var at modtage uønskede e-mails fra fremmede, at få uønskede "popup"-vinduer, og at opleve at computeren "gik i udu" (Q1.12a og Q1.12b).

fra en bank: Sidens webadresse skal starte med `https:`, der skal stå en lille hængelås nederst i browservinduet eller ved siden af adressefeltet, udgiverens webadresse skal stå ved siden af hængelåsen, og en oplysning om hvem der står inde for sidens ægthed skal komme frem, når man flytter musen over hængelåsen. Mere avancerede brugere vil måske ydermere vide, at man kan få flere oplysninger om sidens indehaver, hvis man klikker på hængelåsen. Det er en stor kognitiv udfordring at holde styr på alle disse *indikatorer*.

I CIT-AWARE-09 var respondenterne gennemgående gode til at genkende sider som falske, hvis alle indikatorer manglede. Men de tog fejl i mange tilfælde, hvor kun nogle (for eksempel een eller to) af de obligatoriske indikatorer manglede. Dette er i bred overensstemmelse med tidligere publicerede undersøgelser af, hvordan folk reagerer over for phishingsider, såsom de forsøg der blev beskrevet af Dhamija et al. i 2006 [1]. I bund og grund er problemet et problem af kognitiv overbelastning, når hjernen skal sammenholde viden om flere nødvendige indikatorer. Selv om der er gået mere end 4 år siden Tygar og hans kollegaer udførte deres forsøg, er der ikke sket nogen nævneværdige ændringer i den principielle opbygning af de brugergrænseflader, der bruges af banker, forsikringsselskaber, myndigheder osv., hvorfor it-brugere stadig oplever de samme vanskeligheder som dengang. Men resultaterne fra vor egen undersøgelse viser, at it-brugere kan trænes til at være bedre til at genkende phishingsider ved at gennemgå et forløb, hvor de efter hvert forsøg på at vurdere en sides ægthed får en umiddelbar tilbagemelding om, hvor vidt deres vurdering var korrekt eller ej.

Læringsprocessens effekt En væsentlig karakteristik ved undersøgelsen CIT-AWARE-09 har været, at respondenternes praksis i sikkerhedsmæssigt kritiske situationer blev undersøgt ved at stille respondenten over for et interaktivt scenarie, der lignede en situation som kunne opleves ved almindelig brug af computeren, og hvor respondenten skulle når frem til sit svar ved at eksperimentere inden for rammerne af dette scenarie. Eksempler på denne fremgangsmåde fandtes bl.a. i spørgsmålsgrupperne om:

- Adgangskoder (Spm. Q3.14a til Q3.14d);
- Download (Spm. Q6.1a til Q6.1e);
- E-banking og e-handel (Spm. Q7.8a til Q7.8g).

I alle tilfælde fik respondenten en umiddelbar tilbagemelding om, hvor vidt hans (eller hendes) svar var sikkerhedsmæssigt forsvarligt. Respondenterne sætter meget stor pris på denne karakteristik ved undersøgelsen, idet de føler at de selv lærer noget, samtidigt med at de giver nyttig information til os gennem deres deltagelse.

Om respondenterne virkelig lærer noget ved at gennemføre sådanne forløb forsøgte vi at undersøge ved at se på det længste sammenhængende forløb, nemlig de 6 spørgsmål Q7.8a til og med Q7.8f, der alle handler om phishing (Q7.8g handler også om phishing, men prøver at snyde brugerne på en anden måde, så det er ikke sammenligneligt med 7.8a–7.8f). Her kunne det tydeligt ses, at respondenternes præstationer blev bedre, som de kom igennem spørgsmålsrækken (jvfr. figur 2.3). En nærmere statistisk analyse viste, at effekten var uafhængig af respondentens

alder, uddannelse og antallet af gennemførte it-sikkerhedskurser. Den eneste af de faktorer, som vi undersøgte, der betød noget, var, at respondenter der (efter eget udsagn) havde meget erfaring klarede sig hele vejen igennem bedre end dem med mindre erfaring. Der er derfor gode grunde til at tro, at læringseffekten er reel.

3.2 Anbefalinger

På grundlag af undersøgelsen – og især de resultater, der er trukket frem i afsnit 3.1 – slutter vi her med en række anbefalinger, som kan øge niveauet for it-sikkerhed blandt almindelige borgere:

1. **Læringsforløb:** For at fremme sikker adfærd anbefaler vi, at der udvikles læringsforløb baseret på interaktive scenarier, hvor brugeren har mulighed for at træne sikker adfærd og gives umiddelbar feedback på sit valg af svar. Da undersøgelsen indikerer at det ikke er nok at tilegne sig paratviden, er det væsentligt at tilbyde læringsformer, der understøtter tilegnelse af kompetencer, som er handlingsorienterede og relaterer til praktisk forekommende situationer i den daglige brug af computeren.

2. **Motiverende eksempler:** Da det af undersøgelsen helt klart fremgår, at det som respondenterne opfattede som den største fare var, at andre kunne trække personlige oplysninger ud af computeren, anbefales det, at man udnytter denne opfattelse, så den bliver en motiverende faktor i kampagner.

   Opførselspsykologiske studier og teorier, såsom Rogers *Protection Motivation Theory* [5], peger på, at en holdningsskift, der får en person til udvikle en "god" reaktion på en farlig situation afhænger af personens motivation for at blive beskyttet, og at denne afhænger af resultaterne af fire kognitive processer:

   (a) Perception af truslens alvor;

   (b) Perception af sandsynligheden for, at truslen materialiseres;

   (c) Perception af reaktionens effektivitet i forhold til håndtering af truslen;

   (d) Perception af personens egen evne til at frembringe reaktionen.

   I lyset af sådanne studier er det klart, at det er vigtigt at tage udgangspunkt i de trusler, som folk opfatter som de mest alvorlige.

3. **Begrebsforklaringer:** På trods af mange kampagner er der stadig stor usikkerhed om væsentlige begrebers betydning og sikkerhedsmæssige funktion. Vi anser det for meget vigtigt, at brugere af it-tekniske begreber gør sig stor umage for at forklare begreberne og deres signifikans på en måde, som almindelige borgere kan forstå. I lyset af de meget positive tilbagemeldinger, som vi har haft fra deltagere i vor undersøgelse, vil vi anbefale at forklaringerne ikke blot formuleres med ord, men også udnytter animationer og andre visuelle former for præsentation.

4. **Simple huskeregler:** Undersøgelsen har afdækket en mærkbar diskrepans mellem respondenternes viden om sikre adgangskoder og deres praktiske brug af adgangskoder, som i mange tilfælde ikke var særlig stærke. En indlysende forklaring på denne diskrepans er, at det kan være svært at huske et større antal stærke adgangskoder. Det fremgår af respondenternes svar, at "gennemsnitsrespondenten" har brug for en adgangskode i omkring 10 forskellige situationer (nogle respondenter i mere end 20 situationer). For at imødekomme dette store behøv, vælger de ofte meget simple regler for at konstruere adgangskoderne og simple, usikre strategier for at huske dem.

   For at råde bod på dette problem anbefaler vi, at der ved fremtidige kampagner og læringsforløb lægges vægt på at promovere enkle metoder til at konstruere stærke adgangskoder på en måde, så de let kan huskes men er svære for en udefra kommende at finde eller gætte sig til.

5. **Informationskilder:** Da det fremgår af undersøgelsen, at ældre it-brugere foretrækker at finde information via skriftlige kilder, såsom aviser og pjecer, anbefaler vi, at fremtidige kampagner fortsat henvender sig til denne gruppe på skriftlig form. For de yngre målgrupper anbefaler vi derimod, at der udvikles mere netbaserede materiale, som (i lyset af erfaringer fra undersøgelsen) bør indeholde interaktive elementer og give umiddelbar feedback for at maksimere læringseffekten af kampagnen.

Vi gør opmærksom på, at der inden for rammerne af projektets budget kun har været mulighed for at gennemføre en enkelt undersøgelse af borgernes it-sikkerhed. Et longitudinalt studie, der omfattede en række undersøgelser udført med jævn mellemrum, ville gør det muligt dels at undersøge langtidseffekten af de læringsteknikker, der er indbygget i vor undersøgelsesmetode, dels at følge med i befolkningens eventuelle ændrede bekymringer og evner til at beskytte sig, som trusselsbilledet ændrer sig med tiden. Sådan et longitudinalt studie ville være meget ønskeligt.

Del II

De samlede spørgsmål og svar

Kapitel 4

Statistik

4.1 Opstilling af spørgsmål og svar i dette dokument

I resten af dette dokument præsenteres de spørgsmål, som respondenterne blev stillet over for, i de samme 9 spørgsmålsgrupper, i samme rækkefølge og med samme nummerering som i selve spørgeskemaet. For hvert spørgsmål angives:

1. Selve spørgsmålet, der blev stillet.
2. Eventuelle betingelser for, at spørgsmålet blev stillet (for eksempel, at der er afgivet et bestemt svar på et eller flere foregående spørgsmål).
3. Statistik for de afgivne svar (i visse tilfælde med henvisning til et appendiks med yderligere oplysninger).
4. Eventuelle kommentarer til eller forklaring på den situation eller scenarie, som spørgsmålet henviser til.

I selve spørgeskemaet er en hel del af spørgsmålene tilknyttet scenarier, som respondenten skal forholde sig til. Da disse i reglen er lavet som dynamiske websider med mulighed for respondenten til at deltage aktivt i udforskning af scenariet, kan de ikke umiddelbart gengives i papirudgaven af nærværende rapport. En webudgave er under udarbejdelse. Ligeledes indeholder selve spørgeskemaet en række forklaringer til respondenten og vurderinger af respondentens indsats, især i forhold til disse scenarier. Da disse forklaringer ikke i sig selv giver anledning til yderligere respons fra respondenterne, er de heller ikke gengivet her.

For at berolige eventuelle nervøse læsere: Når man kigger på de nummererede spørgsmål, kan det se ud som om, der her og der er hul i rækken. Dette er ikke fordi, der er faldet noget ud, men skyldes snarere en egenskab ved det værktøj (LimeSurvey), som vi har brugt til konstruktion af spørgeskemaet. Det regner nemlig svar og lignende kommentarer og forklaringer, som man giver respondenterne, teknisk set som “spørgsmål”. Og disse svar o.l. er netop udeladt fra denne samling af statistik.

Endelig en bemærkning til procentsatserne i de statistiske tabeller: I alle spørgsmål beregnes den procentdel af respondenter, der svarede på en bestemt måde, som en procentdel af *det antal respondenter, der blev præsenteret for spørgsmålet*. Denne måde at gøre ting på anses for at være den mest retvisende, når de enkelte spørgsmål besvares af varierende antal respondenter. I nærværende spørgeskema vil dette ske i spørgsmål, hvor en eller flere respondenter:

1. Ikke når så langt som til pågældende spørgsmål;
   eller
2. Springer spørgsmålet over, fordi det ikke er obligatorisk;
   eller
3. Ikke bliver præsenteret for spørgsmålet, da dette kun bliver stillet under visse betingelser.

Lad os for eksempel antage, at 30% af respondenterne har svaret ‘Ja´ på et spørgsmål A, mens 70% har enten svaret ‘Nej´ eller slet ikke svaret. Antag nu, at et andet spørgsmål, B, kun stilles for en respondent, hvis denne har svaret ‘Ja´ på spørgsmål A. Så et det mest informativt at beregne den procentdel af respondenterne, der svarer på en bestemt måde på spørgsmål B, som procentdelen af de 30% af respondenterne, der faktisk blev stillet spørgsmål B – og ikke som procentdelen af det samlede antal respondenter. Ligeledes er det antal, der ikke besvarede spørgsmålet, beregnet i forhold til det antal, der faktisk fik spørgsmålet stillet.

Gruppe 0

Lidt om dig selv...

Denne gruppe spørgsmål bruges til at indsamle demografiske oplysninger og til at undersøge, hvad respondenten bruger computere og andet it-udstyr til.

Q0.2 Hvilken by bor du i?

	Antal	Procent
Besvaret	692	97.87
Ikke besvaret	15	2.13

Q0.3 I hvilken by er du født?

	Antal	Procent
Besvaret	669	94.61
Ikke besvaret	38	5.39

Q0.4 Hvor gammel er du?

Svar	Antal	Procent
Under 20 (1)	3	0.44
20-39 (2)	104	15.32
40-59 (3)	303	44.62
Ældre end 60 (4)	268	39.47
Ikke besvaret	1	0.15

Q0.5 Har du hjemmeboende børn?

Svar	Antal	Procent
Ja (J1)	165	24.37
Nej (J2)	508	75.04
Ikke besvaret	4	0.59

Q0.7 Hvilken uddannelse (eller uddannelser) har du gennemgået? (Der må gerne sættes mere end et kryds.)

Svar	Antal	Procent
Folkeskolens 9. klasse (U1)	142	20.08
10. klasse (U2)	134	18.95
Gymnasiet (U3)	108	15.28
Kontoruddannelse (U4)	64	9.05
Bankuddannelse (U5)	15	2.12
Håndværker / faglært (U6)	183	25.88
Mellemlang videregående (U7)	223	31.54
Længere videregående (U8)	116	16.41
Andet	102	14.43

Q0.8 Hvad er din status på arbejdsmarkedet?

Svar	Antal	Procent
Jeg er fultidsansat (A1)	338	47.81
Jeg er deltidsansat (A2)	46	6.51
Jeg er pensionist (A3)	226	31.97
Jeg er studerende/under uddannelse (A4)	16	2.26
Jeg er ikke i arbejde (A5)	66	9.34

Q0.9 Hvad arbejder du som?
Besvares kun hvis svar på Q0.8 inkluderer A1 eller A2

	Antal	Procent
Besvaret	376	98.95
Ikke besvaret	4	1.05

Nærmere detaljer ses i Appendix A.1.

Q0.10 Arbejder du hjemme eller ude?
Besvares kun hvis svar på Q0.8 inkluderer A1 eller A2

Svar	Antal	Procent
Hjemme (H1)	8	2.12
Ude (H2)	286	75.66
Begge dele (H3)	84	22.22
Ikke besvaret	0	0.00

Q0.11 Hvad er det for en slags virksomhed du arbejder i?
Besvares kun hvis svar på Q0.8 inkluderer A1 eller A2

Svar	Antal	Procent
Offentlig (VT1)	152	21.50
Privat (VT2)	204	28.85
Selvstændig (VT3)	35	4.95

Q0.12 Ca. hvor mange medarbejdere er der, der hvor du arbejder?
Besvares kun hvis svar på Q0.8 inkluderer A1 eller A2

Svar	Antal	Procent
Under 20 (M1)	95	25.33
20-49 (M2)	59	15.73
50-100 (M3)	60	16.00
Flere end 100 (M4)	157	41.87
Ved ikke (M5)	4	1.07
Ikke besvaret	0	0.00

Q0.13 Bruger du en computer hjemme?

Svar	Antal	Procent
Ja (Y)	661	93.48
Nej (N)	0	0.00
Ikke besvaret	0	0.00

Q0.14 Den computer, som du bruger hjemme, er den:
Besvares kun hvis svar på Q0.13 var 'Ja´

Svar	Antal	Procent
En stationær computer? (PC1)	289	43.79
En bærbar computer? (PC2)	147	22.27
Jeg bruger begge dele (PC3)	223	33.79
Ikke besvaret	1	0.15

Q0.15 Bruger du computeren hjemme til et eller flere af følgende formål? (Der må gerne sættes flere kryds.)
Besvares kun hvis svar på Q0.13 var 'Ja´

Svar	Antal	Procent
til e-mail (Br1)	656	99.24
til at søge oplysninger (Br2)	645	97.58
til e-handel/indkøb (Br3)	519	78.52
til netbank el.lign. (Br4)	594	89.86
til at tegne med (Br5)	84	12.71
til tekstbehandling (Br6)	549	83.05
til chat el.lign. (Br7)	166	25.11
til at opsøge sociale sider (Br8)	182	27.53
til at se film eller TV (Br9)	151	22.84
til computerspil (Br10)	245	37.06
til at holde styr på kalenderen (Br11)	193	29.20
til billed/videobehandling (Br12)	450	68.08
Andet	79	11.95

Nærmere detaljer om "Andet" ses i Appendix A.2.

Q0.16 Er computeren forbundet med et netværk?
Besvares kun hvis svar på Q0.13 var 'Ja´

Svar	Antal	Procent
Ja (JNV1)	388	59.06
Nej (JNV2)	241	36.68
Ved ikke (JNV3)	28	4.26
Ikke besvaret	0	0.00

Q0.18 Henter du nogensinde programmer fra internettet – det kan være nytteprogrammer, nye webbrowsere, spil eller hvad det nu skulle være – til din hjemmecomputer?
Besvares kun hvis svar på Q0.13 var 'Ja´

Svar	Antal	Procent
Ja (Y)	550	83.84
Nej (N)	105	16.01
Ikke besvaret	1	0.15

Q0.19 Henter du musik, billeder eller video'er fra internettet til din hjemmecomputer?
Besvares kun hvis svar på Q0.13 var 'Ja´

Svar	Antal	Procent
Ja (Y)	359	54.81
Nej (N)	296	45.19
Ikke besvaret	0	0.00

Q0.20 Bruger du en "smartphone" eller PDA?

Svar	Antal	Procent
Ja (Y)	104	15.88
Nej (N)	551	84.12
Ikke besvaret	0	0.00

Q0.21 Bruger du din smartphone/PDA til et eller flere af følgende formål?
Besvares kun hvis svar på Q0.20 var 'Ja´

Svar	Antal	Procent
til at sende eller modtage e-mail (PD1)	71	68.27
til at søge oplysninger (PD2)	56	53.85
til e-handel/indkøb (PD3)	7	6.73
til at se film eller TV (PD4)	14	13.46
til computerspil (PD5)	12	11.54
til at holde styr på kalenderen (PD6)	84	80.77
Andet	19	18.27

Q0.22 Næsten alle sådanne apparater kan kobles sammen med computere og andet udstyr gennem forskellige slags forbindelse. Hvilke(n) af følgende almindelige typer af forbindelse bruger du?

Besvares kun hvis svar på Q0.20 var 'Ja´

Svar	Antal	Procent
med kabel, fx. USB kabel (F1)	90	86.54
ved brug af Bluetooth (F2)	55	52.88
ved brug af infrarød forbindelse (F3)	7	6.73
ved brug af trådløs ("WiFi") forbindelse (F4)	63	60.58
via telefon (F5)	12	11.54
ingen (F6)	1	0.96
ved ikke (F7)	3	2.88
Andet	0	0.00

Gruppe 1

Generelt kendskab til it-sikkerhed

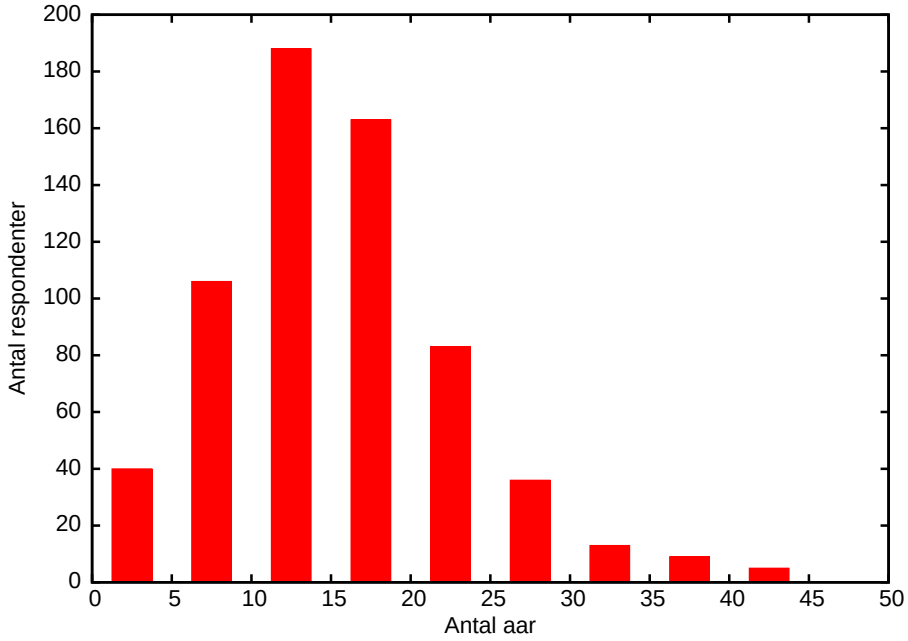
Denne gruppe spørgsmål bruges til at indsamle basale viden om respondentens eventuelle baggrundsviden om og grundlæggende holdninger til it-sikkerhed. Gruppen introduceres til respondenten med teksten:

> *Hvad ved du om it-sikkerhed i al almindelighed? Hvad er det egentlig for en størrelse og hvad handler det om? Hvad tror du, der kan ske, hvis it-sikkerheden fejler? Forstår du de ord, som folk i fjernsynet og i pressen bruger, når de taler om it-sikkerhed – eller er det sort tale det hele?*
>
> *I dette indledende modul stiller vi nogle spørgsmål om dit forhold til disse emner...*

De enkelte spørgsmål og de indsamlede svar er som følger:

Q1.1 I hvor mange år (ca.) har du brugt computere?

Antal år	Antal
0–5	40
5–10	106
10–15	188
15–20	163
20–25	83
25–30	36
30–35	13
35–40	9
40–45	5
$>$45	0



Q1.2 På hvilket niveau vill du placere dig selv med hensyn til kendskab til computere og deres brug?

Svar	Antal	Procent
Uvidende (N1)	9	1.40
Begynder (N2)	78	12.13
Øvet (N3)	474	73.72
Ekspert (N4)	82	12.75
Ikke besvaret	0	0.00

Q1.3 Har du nogensinde været på et kursus el.lign. om brug af computere?

Svar	Antal	Procent
Ja (J1)	362	56.47
Nej (J2)	171	26.68
Ja, flere (J4)	107	16.69
Ikke besvaret	1	0.16

Q1.4 Hvem stod for kurset/kurserne?
Besvares kun hvis svar på Q1.3 var J1 eller J4

	Antal	Procent
Besvaret	450	95.95
Ikke besvaret	19	4.05

Q1.5 Har du nogensinde været på et kursus el.lign. om brug af internettet?

Svar	Antal	Procent
Ja (J1)	188	29.42
Nej (J2)	437	68.39
Ja, flere (J4)	14	2.19
Ikke besvaret	0	0.00

Q1.6 Hvem stod for kurset/kurserne?
Besvares kun hvis svar på Q1.5 var J1 eller J4

	Antal	Procent
Besvaret	193	96.02
Ikke besvaret	8	3.98

Q1.7 Har du nogensinde været på et kursus el.lign. om it-sikkerhed?

Svar	Antal	Procent
Ja (J1)	87	13.66
Nej (J2)	540	84.77
Ja, flere (J4)	10	1.57
Ikke besvaret	0	0.00

Q1.8 Hvem stod for kurset/kurserne?
Besvares kun hvis svar på Q1.7 var J1 eller J4

	Antal	Procent
Besvaret	92	94.85
Ikke besvaret	5	5.15

Q1.9 Har du fået oplysninger om it-sikkerhed fra et eller flere af følgende medier?

Svar	Antal	Procent
Aviser (M1)	324	45.83
Radio/fjernsyn (M2)	270	38.19
Pjecer, fx. NetSikkerNu! (M3)	178	25.18
Internettet (M4)	457	64.64
Ved ikke (M5)	52	7.36
Andet	183	25.88

Nærmere detaljer om “Andet” ses i Appendix A.3.

Q1.10 Hvem tager sig af it-sikkerhed på din computer i hjemmet?

Svar	Antal	Procent
Mig selv (T1)	588	83.17
Min ægtefælle (T2)	18	2.55
Børn/børnebørn (T3)	41	5.80
Andet familiemedlem (T4)	27	3.82
Andet	33	4.67

Nærmere detaljer om "Andet" ses i Appendix A.4.

Q1.11a Man kan tabe alt det, man har gemt på computeren: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	377	59.65
Nej (2)	236	37.34
Ved ikke (3)	19	3.01
Ikke besvaret	0	0.00

Q1.11b Andre kan trække personlige oplysninger ud af din computer: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	618	98.10
Nej (2)	3	0.48
Ved ikke (3)	9	1.43
Ikke besvaret	0	0.00

Q1.11c Andre kan gemme ting, du ikke ved noget om, på din computer: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	582	92.53
Nej (2)	22	3.50
Ved ikke (3)	25	3.97
Ikke besvaret	0	0.00

Q1.11d Folk kan udnytte din computer til kriminelle handlinger: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	588	94.08
Nej (2)	15	2.40
Ved ikke (3)	22	3.52
Ikke besvaret	0	0.00

Q1.11e Andre kan komme til at styre din computer gennem internettet: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	585	93.60
Nej (2)	15	2.40
Ved ikke (3)	25	4.00
Ikke besvaret	0	0.00

Q1.11f Dine hemmeligheder kan komme til andres kendskab: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	552	88.46
Nej (2)	50	8.01
Ved ikke (3)	22	3.53
Ikke besvaret	0	0.00

Q1.11g Man kan få uønskede e-mails fra fremmede: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	493	79.13
Nej (2)	116	18.62
Ved ikke (3)	14	2.25
Ikke besvaret	0	0.00

Q1.11h Man kan blive udsat for tilbud fra pædofile eller andre sexkriminelle: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	357	57.49
Nej (2)	213	34.30
Ved ikke (3)	51	8.21
Ikke besvaret	0	0.00

Q1.11i Folk kan ændre i dine filer, uden at du ved det: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	531	85.51
Nej (2)	42	6.76
Ved ikke (3)	47	7.57
Ikke besvaret	1	0.16

Q1.11j Din computer kan blive stjålet: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	163	26.29
Nej (2)	425	68.55
Ved ikke (3)	32	5.16
Ikke besvaret	0	0.00

Q1.11k Din computer kan "gå i udu" eller bryde helt sammen: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	292	47.10
Nej (2)	297	47.90
Ved ikke (3)	31	5.00
Ikke besvaret	0	0.00

Q1.11l Andre kan overhøre, hvad du sender via internettet: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	494	79.68
Nej (2)	70	11.29
Ved ikke (3)	55	8.87
Ikke besvaret	1	0.16

Q1.11m Folk kan bruge din computer til at angribe andre: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	545	88.05
Nej (2)	31	5.01
Ved ikke (3)	43	6.95
Ikke besvaret	0	0.00

Q1.11n Man kan uforvarende komme til at påføre sig en stor regning: Handler it-sikkerhed om at beskytte sig imod dette?

Svar	Antal	Procent
Ja (1)	274	44.41
Nej (2)	291	47.16
Ved ikke (3)	52	8.43
Ikke besvaret	0	0.00

Q1.12a Er der nogle af de farer, der blev omtalt i Spørgsmål Q1.11, som du selv har oplevet?

Svar	Antal	Procent
Man kan tabe alt det, man har gemt på computeren (F1)	121	17.11
Andre kan trække personlige oplysninger ud af din computer (F2)	16	2.26
Andre kan gemme ting, du ikke ved noget om, på din computer (F3)	67	9.48
Folk kan udnytte din computer til kriminelle handlinger (F4)	15	2.12
Andre kan komme til at styre din computer gennem internettet (F5)	25	3.54
Dine hemmeligheder kan komme til andres kendskab (F6)	16	2.26
Man kan få uønskede e-mails fra fremmede (F7)	406	57.43
Man kan blive udsat for tilbud fra sexkriminelle (F8)	28	3.96
Folk kan ændre i dine filer, uden at du ved det (F9)	19	2.69
Din computer kan blive stjålet (F10)	22	3.11
Din computer kan "gå i udu" (F11)	235	33.24
Andre kan overhøre, hvad du sender via internettet (F12)	9	1.27
Folk kan bruge din computer til at angribe andre (F13)	21	2.97
Man kan uforvarende komme til at påføre sig en stor regning (F14)	22	3.11
Man kan få uønskede "popup"-vinduer (F15)	351	49.65
Når din computer kasseres, kan andre få fat i dine personlige data (F16)	32	4.53
Nej – jeg har ikke oplevet nogen af disse farer. (F17)	130	18.39

Q1.12b Er der nogle af de farer, der blev omtalt i Spørgsmål 1.11, som en, som du kender, har oplevet?

Svar	Antal	Procent
Man kan tabe alt det, man har gemt på computeren (F1)	208	29.42
Andre kan trække personlige oplysninger ud af din computer (F2)	44	6.22
Andre kan gemme ting, du ikke ved noget om, på din computer (F3)	74	10.47
Folk kan udnytte din computer til kriminelle handlinger (F4)	33	4.67
Andre kan komme til at styre din computer gennem internettet (F5)	41	5.80
Dine hemmeligheder kan komme til andres kendskab (F6)	45	6.36
Man kan få uønskede e-mails fra fremmede (F7)	322	45.54
Man kan blive udsat for tilbud fra sexkriminelle (F8)	49	6.93
Folk kan ændre i dine filer, uden at du ved det (F9)	37	5.23
Din computer kan blive stjålet (F10)	82	11.60
Din computer kan “gå i udu” (F11)	268	37.91
Andre kan overhøre, hvad du sender via internettet (F12)	16	2.26
Folk kan bruge din computer til at angribe andre (F13)	48	6.79
Man kan uforvarende komme til at påføre sig en stor regning (F14)	45	6.36
Man kan få uønskede “popup”-vinduer (F15)	295	41.73
Når din computer kasseres, kan andre få fat i dine personlige data (F16)	54	7.64
Nej – jeg kender ikke nogen, der har oplevet nogen af disse farer (F17)	159	22.49

Q1.13b Hvilke af disse farer mener du, det er vigtigst at beskytte sig imod? (Giv en rangfølge for de op til 5 vigtigste, hvor Rang 1 er den vigtigste.)

Faretype	Rang				
	1	2	3	4	5
Man kan tabe alt det, man har gemt på computeren (R1)	132	34	27	23	34
Andre kan trække personlige oplysninger ud af din computer (R2)	246	69	31	34	37
Andre kan gemme ting, du ikke ved noget om, på din computer (R3)	22	64	56	48	48
Folk kan udnytte din computer til kriminelle handlinger (R4)	90	140	55	55	45
Andre kan komme til at styre din computer gennem internettet (R5)	36	102	81	65	35
Dine hemmeligheder kan komme til andres kendskab (R6)	9	30	49	38	34
Man kan få uønskede e-mails fra fremmede (R7)	7	21	28	22	13
Man kan blive udsat for tilbud fra sexkriminelle (R8)	2	7	11	5	12
Folk kan ændre i dine filer, uden at du ved det (R9)	5	24	71	65	50
Din computer kan blive stjålet (R10)	4	12	18	11	9
Din computer kan "gå i udu" (R11)	10	16	34	33	27
Andre kan overhøre, hvad du sender via internettet (R12)	0	10	16	28	25
Folk kan bruge din computer til at angribe andre (R13)	4	26	57	74	71
Man kan uforvarende komme til at påføre sig en stor regning (R14)	3	10	21	25	35
Man kan få uønskede "popup"-vinduer (R15)	3	3	8	14	22
Når din computer kasseres, kan andre få fat i dine personlige data (R16)	7	10	12	30	61

Q1.14 Nu følger der en række (måske temmelig tekniske) ord, som man fra tid til anden kan se brugt i forbindelse med omtale af it-sikkerhed i aviserne, i radioen eller på TV. Kan du sige, i hvor høj grad du selv mener, at du forstår, hvad disse ord betyder?

Begreb	Forstår godt	Forstår nogenl.	Hørt om, ej forstår	Ej hørt om
Digital signatur	485	73	22	0
Password	561	17	1	1
Firewall	475	83	15	7
Krypteringsnøgle	356	126	67	31
Malware	245	105	92	138
(Computer)virus	505	61	10	4
(Computer)orm	442	94	26	18
Phishing	304	88	105	83
Social engineering	48	71	134	327
Botnet	77	53	126	324
Spyware	410	83	56	31
Adware	297	71	75	137
Hacker	517	50	9	4
Adgangskode	571	8	0	1
Trojansk hest	444	76	36	24
DoS-angreb	129	94	136	221
Zombie(Computer)	122	68	112	278
Wardrive	21	54	108	397
SSL	121	53	134	271
Backup	523	37	12	8
Kryptering	456	68	42	14
Sikkerhedskopi	533	38	6	3
Sikker forbindelse	475	86	12	7

Gruppe 2

Datasikring

Denne gruppe spørgsmål bruges til at indsamle viden om respondentens forhold til sikring afa vigtige data. Gruppen introduceres til respondenten med teksten:

> *Indeholder din computer vigtige data, som det ville være ret besværligt – måske umuligt – at genskabe? Har du dokumenter og breve, som du ikke har på papir? Du har måske også fortrolige oplysninger, som giver adgang til din Internetbank eller lignende. Og hvad ville du gøre, hvis dine favoritprogrammer pludselig gik tabt? De følgende spørgsmål handler om, hvad du gør for at sikre disse vigtige data...*

De enkelte spørgsmål og de indsamlede svar er som følger:

Q2.1 Tager du selv kopier af vigtige dokumenter og filer, som ikke må gå tabt?

Svar	Antal	Procent
Ja (JN1)	390	70.24
Nej (JN2)	69	12.75
Delvis (JN3)	92	17.01
Ikke besvaret	0	0.00

Q2.2 På hvilket medium eller medier tager du kopierne?
Besvares kun hvis svar på Q2.1 var JN1 eller JN3

Svar	Antal	Procent
På CD/DVD (M1)	227	48.09
På en ekstern disk (M2)	237	50.21
På en anden computer (M3)	71	15.04
På bånd (M4)	2	0.42
På USB nøgle/memory stick (M5)	225	47.67
Andet	54	11.44

Nærmere detaljer om “Andet” ses i Appendix A.5.

Q2.3 Hvor ofte tager du kopier?
Besvares kun hvis svar på Q2.1 var JN1 eller JN3

Svar	Antal	Procent
Hver dag (K1)	31	8.16
Hver uge (K2)	46	12.11
Hver måned (K3)	58	15.26
Efter behov (K4)	244	64.47
Ikke besvaret	0	0.00

Bemærkning: Inden det næste spørgsmål blev respondenterne præsenteret for en serie animerede tegninger, der illustrerede forskellige muligheder for, hvor man kunne opbevare sine sikkerhedskopier: I lommen, lige ved PC'en, i pengeskabet, i et særskilt rum og uden for huset.

Q2.4x Hvor opbevarer du så DINE kopier?
Besvares kun hvis svar på Q2.1 var JN1 eller JN3

Svar	Antal	Procent
I lommen? (P1)	4	1.08
Lige ved PC'en? (P2)	134	36.02
I pengeskabet? (P3)	28	7.53
I et særskilt rum? (P4)	124	33.33
Uden for huset? (P5)	31	8.83
Andet	51	13.71
Ikke besvaret	0	0.00

Nærmere detaljer om "Andet" ses i Appendix A.6. Blandt svarene her var der nogle få, der indikerede, at respondenten ikke ville oplyse gemmestedet – selv når spørgeskemaet (som her) var anonymt.

Q2.5 Er der andre, der sørger for at tage kopier af dine vigtige dokumenter og filer, som ikke må gå tabt?

Svar	Antal	Procent
Ja (A1)	32	5.95
Nej (A2)	453	84.57
Delvis (A3)	42	7.81
Ved ikke (A4)	8	1.49
Ikke besvaret	1	0.19

Q2.6 På hvilket medium eller medier tager de kopierne?
Besvares kun hvis svar på Q2.5 var A1 eller A3

Svar	Antal	Procent
På CD/DVD (M1)	29	39.19
På en ekstern disk (M2)	27	36.49
På en anden computer (M3)	16	21.62
På bånd (M4)	7	9.46
På USB nøgle/memory stick (M5)	26	35.14
Ved ikke (M6)	3	4.05
Andet	14	18.92

Nærmere detaljer om "Andet" ses i Appendix A.5.

Q2.7 Hvor ofte tager de kopier?
Besvares kun hvis svar på Q2.5 var A1 eller A3

Svar	Antal	Procent
Hver dag (P1)	23	31.51
Hver uge (P2)	6	8.22
Hver måned (P3)	13	17.81
Ved ikke (P4)	31	42.47
Ikke besvaret	0	0.00

Q2.8 Hvor opbevares kopierne?
Besvares kun hvis svar på Q2.5 var A1 eller A3

Svar	Antal	Procent
I lommen? (AP1)	0	0.00
Lige ved PC'en? (AP2)	13	18.06
I pengeskabet? (AP3)	5	6.94
I et særskilt rum? (AP4)	14	19.44
Uden for huset? (AP5)	16	22.22
Ved ikke (AP6)	13	18.06
Andet	11	15.28
Ikke besvaret	0	0.00

Nærmere detaljer om "Andet" ses i Appendix A.6.

Q2.9 Kan det ske, at du har så travlt, at du bare skynder dig for at komme videre, uden at kopier tages?

Svar	Antal	Procent
Ja (J1)	351	65.49
Nej (J2)	185	34.51
Ikke besvaret	0	0.00

Q2.10 Hvor ofte sker dette?

Besvares kun hvis svar på Q2.9 var 'Ja´

Svar	Antal	Procent
Hver dag? (OF1)	56	15.95
Omkring en gang om ugen? (OF2)	54	15.38
Omkring en gang hver måned? (OF3)	69	19.66
Ret sjældent? (OF4)	170	48.43
Aldrig? (OF5)	2	0.57
Ikke besvaret	0	0.00

Gruppe 3

Adgangskoder

Denne gruppe spørgsmål bruges til at undersøge respondentens viden om forsvarlig brug af adgangskoder. Gruppen introduceres til respondenten med teksten:

> *Alle kender situationen: Man skal ind på sin yndlingswebside, men hvad var det nu for et password, man skulle bruge? Var det* `"lillekattekilling"` *eller var det* `"XP6%srq&gAb"` *? Der er rigtig mange situationer, hvor man skal indtaste en hemmelig adgangskode (et "password"), inden man kan få lov til at lave bestemte ting på en computer. Det kan være for at komme ind på en internetbank, for at læse ens mail, for at få adgang til bestemte websider eller blot for at låse computeren op ved dagens begyndelse. De følgende spørgsmål handler om disse adgangskoder og hvordan du bruger dem...*

De enkelte spørgsmål og de indsamlede svar er som følger:

Q3.1 I cirka hvor mange forskellige situationer skal du bruge en adgangskode i dit arbejde med computere, alt taget i betragtning?

Svar	Antal	Procent
1 (P1)	15	2.82
2–5 (P2)	180	33.90
6–10 (P3)	169	31.83
11–20 (P4)	99	18.64
Flere end 20 (P5)	68	12.81
Ikke besvaret	0	0.00

Q3.2 Ca. hvor mange af dine adgangskoder er forskellige?

Svar	Antal	Procent
Ingen – de er helt ens (K1)	14	2.64
Ganske få – under en fjerdedel af dem (K2)	166	31.64
Omkring halvdelen (K3)	176	33.15
De fleste – mere end tre fjerdedele (K4)	99	18.64
De er allesammen forskellige (K5)	74	13.94
Ikke besvaret	0	0.00

Q3.3 Hvordan husker du dem?

Svar	Antal	Procent
Jeg skriver dem ned på en huskeseddel, som jeg går rundt med (PW1)	13	2.57
Jeg skriver dem ned på en huskeseddel, som jeg har ved siden af computeren (PW2)	31	6.13
Jeg skriver dem ind i en særlig fil på computeren (PW3)	36	7.11
Jeg skriver nogle huskeregler ned, som jeg kan bruge til at minde mig selv om adgangskoden (PW4)	51	10.08
Jeg opdigter en sætning, som jeg let kan huske, og bruger første tegn i hvert ord som adgangskode (PW5)	28	5.53
Jeg vælger bare noget, som er let at huske, for eksempel navnet på et familiemedlem eller en familiefødselsdag (PW6)	89	17.59
Jeg kan ikke beskrive, hvordan jeg gør (PW7)	114	22.53
Andet	119	23.52
Ikke besvaret	25	4.94

Nærmere detaljer om "Andet" ses i Appendix A.7. Også her var der nogle få svar, der indikerede, at respondenten mente, at selv metoden til at huske en adgangskode var så hemmelig, at den ikke burde oplyses.

Q3.4 Har du hørt udtrykket "en god adgangskode" ?

Svar	Antal	Procent
Ja (J1)	416	78.79
Nej (J2)	111	21.02
Ikke besvaret	1	0.19

Q3.5 Kan du forklare hvordan en sådan god eller stærk adgangskode ser ud?
Besvares kun hvis svar på Q3.4 var 'Ja´

Svar	Antal	Procent
Ja (J1)	370	88.94
Nej (J2)	45	10.82
Ikke besvaret	1	0.24

Q3.6 Hvordan ville du beskrive en god adgangskode? (Der må gerne sættes mere end et kryds.)
Besvares kun hvis svar på Q3.4 og Q3.5 var 'Ja´

Svar	Antal	Procent
Den skal indeholde store og små bogstaver (GAK1)	310	83.78
Den skal også indeholde tal (GAK2)	316	85.40
Den skal også indeholde tegn, der hverken er bogstaver eller tal, såsom komma, semikolon, *, &, #, osv. (GAK3)	131	35.41
Den skal være på mindst 4 tegn (GAK4)	0	0.00
Den skal være på mindst 6 tegn (GAK5)	43	11.62
Den skal være på mindst 8 tegn (GAK6)	298	80.54
Den skal ikke bestå af letkendelige ord (f.eks. ord, der findes i en almindelig ordbog) (GAK7)	145	39.19
Jeg kan ikke beskrive den (GAK8)	2	0.54
Andet	15	4.05

Nærmere detaljer om "Andet" ses i Appendix A.8. Også her var der nogle få svar, der indikerede, at respondenten mente, at beskrivelsen af en god adgangskode var så hemmelig, at den ikke burde oplyses.

Q3.7 Ca. hvor stor en brøkdel af dine adgangskoder er "gode adgangskoder"?
Besvares kun hvis svar på Q3.4 og Q3.5 var 'Ja´

Svar	Antal	Procent
Ingen (S1)	16	4.32
Under 10% (S2)	57	15.41
Mellem 10 og 50% (S3)	82	22.43
Mellem 50 og 99% (S4)	150	40.81
Alle mine adgangskoder er gode (S5)	63	17.03
Ikke besvaret	0	0.00

Q3.8 Når man siger, at adgangskoden skal være hemmelig, hvad lægger du i dette?

Svar	Antal	Procent
Den må ikke deles med fremmede (H1)	53	10.10
Den må ikke deles med kollegaer (H2)	1	0.19
Den må ikke deles med nogen (H3)	407	77.52
Den må ikke skrives ned (H4)	54	10.29
Jeg er ikke sikker på, hvad det betyder (H5)	3	0.57
Andet	6	1.14
Ikke besvaret	1	0.19

Q3.9 Deler du nogensinde en eller flere af dine adgangskoder med andre?

Svar	Antal	Procent
Ja (J1)	115	31.17
Nej (J2)	254	68.83
Ikke besvaret	0	0.00

Q3.10 Her følger nogle eksempler på aktiviteter, hvor en adgangskode ofte er påkrævet. Deler du nogensinde dine adgangskoder til disse aktiviteter med andre – og hvis du deler din kode, hvem deler du den så med? Hvis du deler adgangskoden til pågældende aktivitet, klik i den lille firkant og skriv en kommentar i boksen, om hvem du deler adgangskoden med.

Besvares kun hvis svar på Q3.9 var 'Ja´

Svar	Antal	Procent
Til at åbne computeren	64	55.65
Til at bruge netbank	56	48.70
Til at få adgang til Told/Skat	32	27.82
Til at komme ind på et chatforum	5	4.34
Til at komme ind på en webside, der tilhører en klub eller forening	24	20.87
Til at komme ind på en webside tl din faglige organisation	7	6.09
Til at komme ind på en side med spil	16	13.91
Til at få adgang til en mailkonto	46	40.00
Andet	10	8.69

Q3.11 Når din computer er tændt og du ikke benytter den et stykke tid, viser den så et pauseskærmsbillede (en "screensaver"), som dækker for alle "vinduer"?

Svar	Antal	Procent
Ja (J1)	378	72.41
Nej (J2)	129	24.71
Ved ikke (J3)	15	2.87
Ikke besvaret	0	0.00

Q3.12 Skal du bruge en adgangskode for at låse pauseskærmen op, så du kan fortsætte med dit arbejde?

Besvares kun hvis svar på Q3.11 var 'Ja´

Svar	Antal	Procent
Ja (J1)	142	37.57
Nej (J2)	232	61.38
Ved ikke (J3)	4	1.06
Ikke besvaret	0	0.00

Q3.13 Som vi tidligere har spurgt om, skal man for en del websider indtaste en adgangskode for at komme ind på siden. Hvis der er nogen, der "lytter med på linien", kan de opsnappe din hemmelige adgangskode (blandt meget andet). Vidste du, at man kan se, om man er beskyttet imod den slags aflytning?

Svar	Antal	Procent
Ja (J1)	150	40.87
Nej (J2)	216	58.86
Ikke besvaret	1	0.27

Bemærkning: I de næste 4 spørgsmål (Q3.14a til Q3.14d) bedes respondenterne om at vurdere, om man kan stole på, at oplysninger, der tastes ind på siden, ikke kan aflyttes. Der er både falske og (kopier af) ægte sider iblandt. For de ægte sider benyttes alle fire af de velkendte indikatorer, der typisk ville kendetegne en sikker side:

1. Sidens webadresse (URL) starter med https:
2. Der findes en hængelås nederst i browservinduet eller oppe ved siden af adressefeltet.
3. Sideudgiverens webadresse står ved siden af hængelåsen.
4. Når man flytter musen over hængelåsen, kommer der en oplysning frem om, hvem der står inde for sidens ægthed.

For de falske sider mangler en eller flere af disse indikatorer.

Q3.14a Er de informationer, som du taster ind på denne webside, beskyttede imod aflytning?
Besvares kun hvis svar på Q3.13 var 'Ja´

Svar	Antal	Procent
Ja (JNV1)	63	42.28
Nej (JNV2)	72	48.32
Ved ikke (JNV3)	14	9.40
Ikke besvaret	0	0.00

Kommentarer: Siden er en falsk side, øjensynligt fra Adobe, hvor indikatorerne 2, 3 og 4 mangler.

Q3.14b Er de informationer, som du taster ind på denne webside, beskyttede imod aflytning?
Besvares kun hvis svar på Q3.13 var 'Ja´

Svar	Antal	Procent
Ja (JNV1)	67	44.97
Nej (JNV2)	66	44.30
Ved ikke (JNV3)	16	10.74
Ikke besvaret	0	0.00

Kommentarer: Denne er en falsk side, igen øjensynligt fra Adobe, hvor indikator 1 mangler.

Q3.14c Er de informationer, som du taster ind på denne webside, beskyttede imod aflytning?
Besvares kun hvis svar på Q3.13 var 'Ja´

Svar	Antal	Procent
Ja (JNV1)	104	69.80
Nej (JNV2)	27	18.12
Ved ikke (JNV3)	18	12.08
Ikke besvaret	0	0.00

Kommentarer: Denne er (en kopi af) en ægte side fra Adobe, hvor alle indikatorerne er på plads.

Q3.14d Er de informationer, som du taster ind på denne webside, beskyttede imod aflytning?
Besvares kun hvis svar på Q3.13 var 'Ja´

Svar	Antal	Procent
Ja (JNV1)	128	86.49
Nej (JNV2)	16	10.81
Ved ikke (JNV3)	4	2.70
Ikke besvaret	0	0.00

Kommentarer: Denne er en falsk side, denne gang øjensynligt fra Skat's TastSelv-service, men hvor indikatoren 4 mangler.

Q3.15 Hvad er det, du kigger efter, for at finde ud af om en side beskytter de informationer, som du taster ind?
Besvares kun hvis svar på Q3.13 var 'Ja´

Svar	Antal	Procent
Om sidens tekst "lyder rigtigt"? (PR1)	16	10.67
Om der er hængelås i browservinduet? (PR2)	101	67.33
Om hængelåsen står det rigtige sted i vinduet? (PR3)	43	28.67
Om webadressen starter med https? (PR4)	84	56.00
Om man får information om, hvem der står inde for, at siden er ægte, når man flytter musen over hængelåsen? (PR5)	50	33.33
Om man kan finde information om, hvor siden kommer fra, når man klikker på hængelåsen? (PR6)	35	23.33
Kan ikke forklare, hvordan jeg gør (PR7)	6	4.00
Andet	11	7.33

Gruppe 4

Virus og andet ondskabsfuldt

Denne gruppe spørgsmål bruges til at indsamle oplysninger om respondentens viden om virus og andre skadelige programmer og om hvordan man bekæmper dem. Gruppen introduceres til respondenten med teksten:

> *Av! Jeg skulle bare lige hente det program fra nettet og så gik skærmen helt i sort og nu står der noget med russiske bogstaver på den. Og lamperne på boksen med internetforbindelsen blinker som vanvittige. Hvad kan der være sket? Kan det være et virus? Nå, din computer er måske aldrig blevet hjemsøgt af virus, men hvor meget kender du til virus og hvordan man beskytter sig imod dem? Det handler spørgsmålene i dette modul om...*

De enkelte spørgsmål og de indsamlede svar er som følger:

Q4.1 Kender du udtrykket “en virusskanner” (eller “et antivirus program”)?

Svar	Antal	Procent
Ja (J1)	490	98.20
Nej (J2)	9	1.80
Ikke besvaret	0	0.00

Q4.2 Forstår du, hvad sådan en virusskanner laver?
Besvares kun hvis svar på Q4.1 var ‘Ja´

Svar	Antal	Procent
Ja (J1)	438	89.39
Nej (J2)	52	10.61
Ikke besvaret	0	0.00

Q4.3 Hvad laver sådan en virusskanner, efter din opfattelse?
Besvares kun hvis svar på Q4.1 og Q4.2 var 'Ja´

Svar	Antal	Procent
Den kigger mine filer igennem, for at se om den kan finde et virus (VS1)	54	12.36
Den kigger harddisken igennem, for at se om den kan finde et virus (VS2)	50	11.44
Den checker alle indkommende mails og websider, for at se om de bærer rundt på et virus (VS3)	67	15.33
Den checker harddisken og alle mails og websider, for at se om den kan finde et virus (VS7)	199	45.54
Den checker alle dele af computeren, for at se om der er sket skade, der skyldes et virus (VS4)	55	12.59
Den måler computerens temperatur, for at se om den er inficeret af et virus (VS5)	3	0.69
Jeg kan ikke beskriver, hvad den laver (VS6)	4	0.92
Andet	4	0.92
Ikke besvaret	1	0.23

Q4.4 Har du en virusskanner i funktion på din computer?

Svar	Antal	Procent
Ja (J1)	464	94.89
Nej (J2)	19	3.89
Ved ikke (J3)	6	1.23
Ikke besvaret	0	0.00

Q4.5 En virusskanner skal normalt holdes ajour med de nyeste former for angreb, der kan true it-sikkerhed. Hvem er det, der sørger for, at dette sker på din computer hjemme?

Svar	Antal	Procent
Mig selv (VSU1)	376	78.75
Min ægtefælle (VSU2)	7	1.46
Børn/børnebørn (VSU3)	5	1.04
Andet familiemedlem (VSU4)	11	2.29
Jeg ved ikke, hvem det er (VSU5)	6	1.25
Andet	73	15.21
Ikke besvaret	0	0.00

Nørmere detaljer om "Andet" findes i Appendix A.9.

Q4.6 Hvis din computer fik et virus, hvad ville du gøre for at få computeren til at virke normalt igen?

Svar	Antal	Procent
Slukke computeren og genstarte systemet (V1)	3	0.60
Bruge virusfjerneren i antivirusprogrammet (V2)	386	77.82
Reinstallere operativsystemet og alle programmer (V3)	52	10.48
Smide harddisken ud og købe en helt ny (V4)	1	0.20
Smide computeren ud og købe en helt ny (V5)	3	0.60
Jeg ved ikke, hvad jeg ville gøre (V6)	25	5.04
Andet	26	5.24
Ikke besvaret	0	0.00

Nærmere detaljer om “Andet” ses i Appendix A.10.

Gruppe 5

e-mail

Denne gruppe spørgsmål bruges til at undersøge respondentens viden om e-mail og de farer, der måtte være forbundet dermed. Gruppen introduceres for respondenten med teksten:

> *Bruger du e-mail? Det gør de fleste danskere ihvertfald, fra små børn til oldeforældre. Man kan give folk små beskeder, skrive lange breve, sende kæresten et sødt digt, fortælle farfar hvordan man glæder sig til at komme på besøg – og meget andet. Og dog. I indbakken med e-mail er der ofte ubehagelige overraskelser. Hvorfor får jeg så mange e-mails fra Nigeria, når jeg ikke kender nogen derfra? Og syge tilbud om alt muligt? Og nogle gange, hvis jeg åbner disse mails, sker der de mærkeligste ting. Jeg er ved at være rigtig træt af det. Hvad kan der ske med din computer, når du bruger e-mail? Og hvordan kan man beskytte sig imod uheld? Det handler spørgsmålene i dette modul om...*

De enkelte spørgsmål og de indsamlede svar er som følger:

Q5.1 Kan du forklare i grove træk, hvordan e-mail virker? altså, hvad der sker fra det øjeblik, du sender en e-mail, indtil det øjeblik, hvor modtageren åbner mail'en på sin computer?

Svar	Antal	Procent
Mail'en overføres direkte fra din computer til modtagerens computer (EM1)	99	20.29
Mail'en overføres til en central computer, hvorfra modtageren henter og åbner den (EM2)	328	67.21
Mail'en gemmes på din computer, hvorfra modtageren henter den (EM3)	2	0.41
Modtageren får en meddelelse om, at der er en mail til ham, som han kan hente (EM4)	35	7.17
Jeg ved ikke, hvordan det virker (EM5)	21	4.30
Andet	3	0.61
Ikke besvaret	0	0.00

Q5.2 Når du modtager en e-mail, hvordan finder du ud af, hvem den kommer fra? Du må gerne skrive en kommentar i boksen, hvis du vil give yderligere forklaring.

Svar	Antal	Procent
Jeg kigger på listen over indkommende mails (MM1)	262	53.91
Jeg kigger på "Fra"-linien i starten af mailen (MM2)	203	41.77
Jeg kigger på den afsluttende hilsen i mailen (MM3)	2	0.41
Jeg kigger på den digitale signatur på mailen (MM4)	14	2.88
Jeg ved ikke (eller har ikke tænkt over), hvordan jeg gør det (MM5)	5	1.03
Ikke besvaret	0	0.00

Q5.3 Vil det sige, du skal åbne mailen for at se, hvem den er fra?

Svar	Antal	Procent
Ja (JNV1)	18	3.72
Nej (JNV2)	462	95.87
Ved ikke (JNV3)	2	0.41
Ikke besvaret	0	0.00

Q5.4 Modtager du nogensinde mails, der ser ud til at komme fra folk, som du kender, men som rent faktisk ikke gør det?

Svar	Antal	Procent
Ja (JNV1)	213	44.01
Nej (JNV2)	250	51.65
Ved ikke (JNV3)	21	4.34
Ikke besvaret	0	0.00

Q5.5 Når du åbner en mail, kan meddelelsen indeholde en række henvisninger (såkaldte "links") til websider, som afsenderen gerne vil henlede din opmærksomhed på. Mange mennesker har haft den oplevelse, at de modtager mails, hvori der står links, som fører hen til websider, der indeholder porno, tvivlsomme tilbud, sider med hasardspil eller andet, som de helst vil være frie for. Hvordan bestemmer du, om links i en e-mail skal følges – altså, om du skal klikke på linken eller ej?

Svar	Antal	Procent
Jeg kigger på, om mailen kommer fra venner/familie (ML1)	127	17.96
Jeg kigger på, om mailen kommer fra en afsender, jeg kender (ML2)	395	55.87
Jeg kigger på meddelelsens emne og indhold (ML3)	219	30.98
Jeg kigger på, om navnet angivet ved linken ser harmløst ud (ML4)	70	9.90
Jeg har ingen særlige regler (ML5)	5	0.71
Andet	28	3.96

Nærmere detaljer on "Andet" ses i Appendix A.11.

Q5.6 Kan du forklare, hvordan et "harmløst linknavn" ser ud?
Besvares kun hvis svar på Q5.5 var ML4

Besvaret	56	80.00
Ikke besvaret	14	20.00

Nærmere detaljer ses i Appendix A.12.

Q5.7 Når du modtager en mail, kan den også indeholde en række vedhæftede dokumenter (såkaldte "attachments"), som for eksempel kan bestå af tekstfiler, billeder, videoer, lydfiler og meget andet. Også her har mange mennesker haft den oplevelse, at vedhæftede dokumenter kan indeholde materiale, som de helst vil være frie for. Hvordan bestemmer du, om du skal se på sådanne vedhæftede dokumenter – eller måske endda gemme dem på din computer til senere brug?

Svar	Antal	Procent
Jeg kigger på, om mailen kommer fra venner/familie (MV1)	172	24.33
Jeg kigger på, om mailen kommer fra en afsender, jeg kender (MV2)	341	48.23
Jeg kigger på meddelelsens emne og indhold (MV3)	311	43.99
Jeg kigger på, om dokumentets navn ser harmløst ud (MV4)	118	16.69
Jeg har ingen særlige regler (MV5)	4	0.57
Andet	33	4.67

Nærmere detaljer om "Andet" ses i Appendix A.13.

Q5.8 Kan du forklare, hvordan et "harmløst dokumentnavn" ser ud?
Besvares kun hvis svar på Q5.7 var MV4

Besvaret	96	81.36
Ikke besvaret	22	18.64

Nærmere detaljer ses i Appendix A.14.

Q5.9 De fleste har hørt om, at siderne tilgået via links og vedhæftede dokumenter i e-mails kan indeholde pornografisk materiale, selv om de måske ikke selv har modtaget sådanne mails. Men af og til hører man også om andre former for ubehageligt materiale, som også kan fås gennem e-mails. Hvilke af følgende kan der være tale om?

	Ja	Nej	Ved ikke	IB
Et vedhæftet dokument kan indeholde et program, der kan få din computer til at bryde sammen	436	13	21	5
Et vedhæftet dokument kan indeholde et program, der sender dine personlige oplysninger til uvedkommende	426	14	29	6
Et vedhæftet dokument kan indeholde et program, der kan skade andre folks computere	340	50	79	6
Et vedhæftet dokument kan indeholde et program, der kan slette filer på din computer	431	15	23	6
Sådanne skadelige virkninger kan kun finde sted, hvis du åbner det vedhæftede dokument	367	70	32	6
Sådanne skadelige virkninger kan også finde sted, selv om du ikke åbner det vedhæftede dokument	105	279	85	6
En mail med forfalsket afsender kan bede dig om at sende fortrolige oplysninger (fx. CPR-nr., bankoplysninger)	454	1	14	6
En mail kan henvise til en webside, hvor man bliver bedt om at oplyse fortrolige oplysninger	457	0	12	6
En mail kan henvise til en webside, der uden din medvirken installerer et skadeligt program på din computer	425	14	30	6
En mail kan indeholde uønskede seksuelle tilbud	444	2	23	6
En mail kan indeholde uønskede tilbud om varer eller tjenester	457	1	11	6

Q5.10 Det anbefales ofte, at man bruger en virusskanner for at beskytte imod mange af de skadelige virkninger, der kan komme med e-mails. Hvis vi kigger igen på listen fra forrige spørgsmål, kan du fortælle os, i hvor høj grad en virusskanner ville fange de ikke-ønskelige mails?

	Altid	Nogle gange	Aldrig	Ved ikke	IB
Et vedhæftet dokument kan indeholde et program, der kan få din computer til at bryde sammen	178	228	22	30	7
Et vedhæftet dokument kan indeholde et program, der sender dine personlige oplysninger til uvedkommende	176	213	29	40	7
Et vedhæftet dokument kan indeholde et program, der kan skade andre folks computere	159	199	37	63	7
Et vedhæftet dokument kan indeholde et program, der kan slette filer på din computer	188	215	18	37	7
En mail med forfalsket afsender kan bede dig om at sende fortrolige oplysninger (fx. CPR-nr., bankoplysninger)	106	154	158	40	7
En mail kan henvise til en webside, hvor man bliver bedt om at oplyse fortrolige oplysninger	102	162	161	33	7
En mail kan henvise til en webside, der uden din medvirken installerer et skadeligt program på din computer	135	165	120	38	7
En mail kan indeholde uønskede seksuelle tilbud	90	164	163	41	7
En mail kan indeholde uønskede tilbud om varer eller tjenester	91	167	168	32	7

Q5.11 På mange computere skal man afgive en password/adgangskode for at kunne sende mail eller hente egen mail. Vi har tidligere talt om, at sådanne adgangskoder skal holdes hemmeligt. Når man skal bruge e-mail, sendes adgangskoden gennem internettet til den computer, der håndterer din mail (den såkaldte "mailserver").

Når adgangskoden sendes gennem internettet, tror du, at nogen kan "lytte med på linien" og så få fat i din hemmelige kode?

Svar	Antal	Procent
Ja (JNV1)	242	52.84
Nej (JNV2)	147	32.10
Ved ikke (JNV3)	6	14.85
Ikke besvaret	0	0.00

Q5.12 Kan man beskytte sig mod, at andre opsnapper ens adgangskode ved en sådan aflytning?
Besvares kun hvis svar på Q5.11 var 'Ja´

Svar	Antal	Procent
Ja (JNV1)	193	79.75
Nej (JNV2)	20	8.26
Ved ikke (JNV3)	29	11.98
Ikke besvaret	0	0.00

Q5.13 Hvordan kan man sikre sig imod aflytning af adgangskoden?
Besvares kun hvis svar på Q5.11 og Q5.12 var 'Ja´

Svar	Antal	Procent
Man kan bruge en sikker forbindelse til mailserveren. (AFL1)	154	79.79
Man kan bruge SSL/TLS til at beskytte forbindelsen til mailserveren. (AFL2)	76	39.38
Man kan bruge en VPN forbindelse til mailserveren. (AFL3)	38	19.69
Man kan bruge en SSH tunnel til mailserveren. (AFL4)	21	10.88
Man kan bruge webmail, hvor mailserverens webadresse starter med "https:" (AFL6)	64	33.16
Jeg ved ikke, hvordan man gør. (AFL5)	24	12.44
Andet	6	3.11

Q5.14 Bruger systemet til håndtering af mail på din computer en af disse sikre muligheder?
Besvares kun hvis svar på Q5.11 og Q5.12 var 'Ja´ og svar på Q5.13 ikke var AFL5

Svar	Antal	Procent
Ja (J1)	107	63.31
Nej (J2)	35	20.71
Ved ikke (J3)	26	15.98
Ikke besvaret	0	0.00

Q5.15 Modtager du nogensinde mails med indhold, der skal holdes fortroligt?

Svar	Antal	Procent
Ja (J1)	266	58.33
Nej (J2)	179	39.25
Ved ikke (J3)	11	2.41
Ikke besvaret	0	0.00

Q5.16 Hvordan sikrer du, at de fortrolige mails ikke kommer til andres kendskab?
Besvares kun hvis svar på Q5.15 var 'Ja´

Besvaret	202	75.94
Ikke besvaret	64	24.06

Nærmere detaljer ses i Appendix A.15.

Gruppe 6

Download

Denne gruppe af spørgsmål handler om download og dens mulige konsekvenser. Gruppen introduceres for respondenten med teksten:

> *Min ven Jesper siger, at han får al den nyeste musik fra internettet. Og Julie har en virkelig fed plakat, som hun har hentet fra en webside i Kina. Og forleden hørte jeg, at man kan få rigtig flotte spil fra en site i Brasilien. Det eneste, der bekymrer mig, er, at jeg hørte naboen sige, at hans computer begyndte at opføre sig helt underligt, da han hentede et program fra et sted i Ungarn... Ja, der er mange fristelser derude. Og muligvis mange farer. De følgende spørgsmål handler om dit kendskab til disse ting...*

De enkelte spørgsmål og de indsamlede svar er som følger.

Indledningsvis spørges om respondenterne ville downloade de produkter, som er omtalt i 5 forskellige mails eller websider, som er af varierende lødighed:

Q6.1a Ville du downloade det postkort, der er link til i denne mail? (her er det tanken, at du "leger som om" mailen blev sendt til dig og ikke til `"hanne1234@get2net.dk"`)

Svar	Antal	Procent
Ja (JNM1)	29	6.59
Nej (JNM2)	401	91.14
Ved ikke (JNM3)	10	2.27
Ikke besvaret	0	0.00

Kommentarer: Hvis musen flyttes over linket, afsløres, at det henviser til URL `http://83.96.231.106/~test/Greetings.exe`, hvilket indeholder to suspekte elementer: (1) Hostnavnet angives på numerisk form og (2) linket henviser til en .exe-fil. En sikker strategi ville derfor være ikke at downloade "postkortet".

Q6.1b Ville du downloade den nyeste version af Flash player fra denne webside hos `www.spacemynews.com` for at se Reuters' video om bombeangrebet?

Svar	Antal	Procent
Ja (JNM1)	57	12.98
Nej (JNM2)	371	84.51
Ved ikke (JNM3)	10	2.28
Ikke besvaret	1	0.23

Kommentarer: Hvis musen flyttes over linket, afsløres, at det henviser til URL `http://www.spacemynews.com/save.exe`, altså at linkets mål er en .exe-fil. (Faktisk er der her tale om en kendt malware site.) Også her ville en sikker strategi være ikke at downloade den tilbudte nye Flash player.

Q6.1c Ville du downloade Twingly's screensaver fra denne side hos `www.reallyslick.com`?

Svar	Antal	Procent
Ja (TW1)	114	26.03
Nej (TW2)	299	68.26
Ved ikke (TW3)	25	5.71
Ikke besvaret	0	0.00

Kommentarer: Der er flere links på siden. De links, der øjensynligt kan bruges til at downloade screensaveren henviser til URL `http://static.twingly.com/Twingly-Screensaver.zip`, dvs. et zip-arkiv, hvis indhold man ikke umiddelbart kan se. En sikker strategi ville være ikke at downloade screensaveren, medmindre man har forhåndskendskab til Twingly's produkter.

Q6.1d Ville du downloade disse screensavers fra denne side hos `www.reallyslick.com`?

Svar	Antal	Procent
Ja (RS1)	66	15.07
Nej (RS2)	341	77.85
Ved ikke (RS3)	31	7.08
Ikke besvaret	0	0.00

Kommentarer: Der er flere links på siden. De links, der øjensynligt kan bruges til at downloade de (i øvrigt meget smukke) screensavere, henviser til URL `http://www.reallyslick.com/download/xxxxx.scr`, hvor xxxxx er afhængigt af netop hvilken screensaver, der er tale om. Alle links henviser altså til .scr-filer, hvad der er helt normalt for screensavere. Da der imidlertid er tale om en type eksekverbar fil, ville en sikker strategi være ikke at downloade screensaverne, medmindre man har forhåndskendskab til ReallySlick's produkter.

Q6.1e Ville du så downloade disse screensavers fra denne side hos `www.reallyslick.com`?

Svar	Antal	Procent
Ja (JNM1)	20	4.57
Nej (JNM2)	402	91.78
Ved ikke (JNM3)	16	3.65
Ikke besvaret	0	0.00

Kommentarer: Overfladisk set ligner siden den fra Q6.1d. Men i modsætning til Q6.1d henviser kun nogle af linksene til en URL af formen `http://www.reallyslick.com/download/xxxxx.scr`. De øvrige henviser til en .exe-fil fra et websted i Kina. Her ville det være klogt at se på denne side med stor mistænksomhed og derfor ikke downloade noget fra den.

Q6.2 Hvis du downloader et skadeligt program, hvilke af følgende muligheder tror du, der kan komme på tale?

Hændelse	Ja	Nej	Ved ikke	IB
Programmet kan få din computer til at bryde sammen	402	18	18	0
Programmet kan sende dine personlige oplysninger til uvedkommende	423	3	12	0
Programmet kan skade andre folks computere	329	50	59	0
Programmet kan slette filer på din computer	416	7	15	0
Programmet kan hente og gemme filer på din computer	411	7	20	0
Programmet kan gøre det muligt for andre at styre din computer udefra	413	5	20	0

Q6.3 Tror du, man uforvarende kan komme til at downloade noget, når man blot tilgår en webside uden at klikke på nogen links på siden?

Svar	Antal	Procent
Ja (JNV1)	279	63.70
Nej (JNV2)	118	26.94
Ved ikke (JNV3)	41	9.36
Ikke besvaret	0	0.00

Q6.4 Hvis man nærer tvivl til en webside, hvor der tilbydes download af billeder, programmer eller andre produkter, kan man rapportere det et sted?

Svar	Antal	Procent
Ja (JNV1)	245	56.06
Nej (JNV2)	18	4.12
Ved ikke (JNV3)	174	39.82
Ikke besvaret	0	0.00

Gruppe 7

e-banking og e-handel

Denne gruppe spørgsmål bruges til at undersøge respondentens holdning til brugen af e-banking og e-handel og hans eller hendes viden om, hvad man eventuelt kan gøre for at beskytte sig imod de farer, der måtte være forbundet dermed. Gruppen introduceres for respondenten med teksten:

> *At handle ind via nettet kan være meget sjovt – og billigt. Og tænk, hvor meget tid man sparer ved at betale sine regninger via en netbank. Men man hører jo også historier om folk, der bliver snydt, hvor varerne aldrig kommer eller pengene forsvinder fra bankkontoen.*
>
> *Hvad er dine egne oplevelser – og ved du nok om, hvordan man kan undgå at blive snydt eller bedraget? Det handler spørgsmålene i dette modul om...*

De enkelte spørgsmål og de indsamlede svar er som følger:

Q7.1 Bruger du nogensinde internettet til e-handel og/eller e-banking?

Svar	Antal	Procent
Ja (J1)	406	93.33
Nej (J2)	29	6.67
Ikke besvaret	0	0.00

Q7.2 Anvender du en netbank?

Svar	Antal	Procent
Ja (J1)	397	91.26
Nej (J2)	37	8.51
Ikke besvaret	1	0.23

Q7.3 Føler du, at det er sikkert at anvende netbank?
Besvares kun hvis svar på Q7.2 var 'Ja´

Svar	Antal	Procent
Ja (JNV1)	329	82.87
Nej (JNV2)	1	0.25
Nogenlunde (JNV3)	66	16.62
Ved ikke (JNV4)	1	0.25
Ikke besvaret	0	0.00

Q7.4 Har du set historier i medierne om problemer med netbankernes sikkerhed?

Svar	Antal	Procent
Ja (J1)	364	83.87
Nej (J2)	70	16.13
Ikke besvaret	0	0.00

Q7.5 Kender du begrebet "phishing"?

Svar	Antal	Procent
Ja (J1)	283	65.21
Nej (J2)	151	34.79
Ikke besvaret	0	0.00

Q7.6 Kan du i korte træk forklare, hvad phishing går ud på?
Besvares kun hvis svar på Q7.5 var 'Ja´

Svar	Antal	Procent
Det er, når fremmede prøver at fiske efter dine hemmeligheder (PHIS0)	51	18.02
Det er, når folk prøver at franarre dig personlige data, som de kan udnytte til at påstå, at de er dig (PHIS1)	124	43.82
Det er, når en ondskabsfuld person angriber din computer, så den giver en ilde lugt fra sig (PHIS2)	0	0.00
Det er, når folk prøver at stjæle de adgangskoder, som du bruger til netbanken (PHIS3)	91	32.16
Det er, når nogle svindlere prøver at få dig til at investere en masse penge i et værdiløst projekt (PHIS4)	2	0.71
Jeg kan ikke forklare, hvad det går ud på (PHIS5)	13	4.59
Andet	0	0.00
Ikke besvaret	2	0.71

Q7.7 Har du følt, der kunne være en risiko for, at nogle prøvede at tømme din bankkonto via internettet?
Besvares kun hvis svar på Q7.2 var 'Ja´

Svar	Antal	Procent
Ja (J1)	79	19.90
Nej (J2)	318	80.10
Ikke besvaret	0	0.00

Bemærkning: I de næste 7 spørgsmål (Q7.8a til Q7.8g) bedes respondenterne om at vurdere, om en række websider er sikre, i den forstand at man kan have tillid til, at oplysninger, der tastes ind på siden, går til sidens øjensynlige udgiver uden at blive afsløret for uvedkommende på nogen måde. Der er både falske og (kopier af) ægte sider iblandt. For de ægte sider benyttes alle fire af de velkendte indikatorer, der typisk ville kendetegne en sikker side:

1. Sidens webadresse (URL) starter med https:
2. Der findes en hængelås nederst i browservinduet eller oppe ved siden af adressefeltet.
3. Sideudgiverens webadresse står ved siden af hængelåsen.
4. Når man flytter musen over hængelåsen, kommer der en oplysning frem om, hvem der står inde for sidens ægthed.

For de falske sider mangler en eller flere af disse indikatorer. Svarene på disse spørgsmål bør sammenholdes med svarene på Q3.14(a-d) og Q3.15.

Q7.8a Ville du stole på, at oplysninger, som du taster ind på denne webside, holdes sikre?
Besvares kun hvis svar på Q7.2 var 'Ja´

Svar	Antal	Procent
Ja (JNM1)	137	34.51
Nej (JNM2)	198	49.87
Ved ikke (JNM3)	59	14.86
Ikke besvaret	3	0.00

Kommentarer: Siden er an falsk side, øjensynligt fra Nordea, hvor indikatorerne 1 og 4 mangler.

Q7.8b Ville du stole på, at de oplysninger, som du taster ind på denne webside, holdes sikre?
Besvares kun hvis svar på Q7.2 var 'Ja´

Svar	Antal	Procent
Ja (JNP1)	219	55.87
Nej (JNP2)	135	34.44
Ved ikke (JNP3)	37	9.44
Ikke besvaret	1	0.26

Kommentarer: Siden er en kopi af en ægte side fra Nordea, hvor alle 4 indikatorer er til stede.

Q7.8c Ville du stole på, at de oplysninger, som du taster ind på denne webside, holdes sikre?
Besvares kun hvis svar på Q7.2 var 'Ja´

Svar	Antal	Procent
Ja (JNM1)	105	26.99
Nej (JNM2)	218	56.04
Ved ikke (JNM3)	66	16.97
Ikke besvaret	0	0.00

Kommentarer: Siden er en falsk side, øjensynligt fra PayPal, hvor indikatorerne 2, 3 og 4 mangler.

Q7.8d Ville du stole på, at de oplysninger, som du taster ind på denne webside, holdes sikre?
Besvares kun hvis svar på Q7.2 var 'Ja´

Svar	Antal	Procent
Ja (JNM1)	38	9.79
Nej (JNM2)	320	82.47
Ved ikke (JNM3)	30	7.73
Ikke besvaret	0	0.00

Kommentarer: Siden er en falsk side, øjensynligt fra PayPal, hvor samtlige indikatorer mangler.

Q7.8e Ville du stole på, at de oplysninger, som du taster ind på denne webside, holdes sikre?
Besvares kun hvis svar på Q7.2 var 'Ja´

Svar	Antal	Procent
Ja (JNP1)	282	73.06
Nej (JNP2)	69	17.88
Ved ikke (JNP3)	35	9.07
Ikke besvaret	0	0.00

Kommentarer: Siden er en kopi af en ægte side fra PayPal, hvor alle 4 indikatorer er til stede.

Q7.8f Ville du stole på, at de oplysninger, som du taster ind på denne webside, holdes sikre?
Besvares kun hvis svar på Q7.2 var 'Ja´

Svar	Antal	Procent
Ja (JNM1)	9	2.34
Nej (JNM2)	368	96.35
Ved ikke (JNM3)	5	1.30
Ikke besvaret	0	0.00

Kommentarer: Siden er en falsk side, øjensynligt fra Nordea, hvor samtlige indikatorer mangler – og hvor brugeren samtidig spørges om sin loginkode, som i flere velkendte phishingforsøg.

Q7.8g Ville du stole på, at de oplysninger, som du taster ind på denne webside, holdes sikre?
Besvares kun hvis svar på Q7.2 var 'Ja´

Svar	Antal	Procent
Ja (JNM1)	206	53.79
Nej (JNM2)	166	43.34
Ved ikke (JNM3)	11	2.87
Ikke besvaret	0	0.00

Kommentarer: Siden er en side, øjensynligt fra Nordea, hvor alle indikatorer er til stede – men hvor brugeren samtidig spørges om sin loginkode, som i flere velkendte phishing-forsøg.

Q7.9 Når du logger på netbanken, hvilken af følgende muligheder bruger du?
Besvares kun hvis svar på Q7.2 var 'Ja´

Svar	Antal	Procent
Jeg bruger en adgangskode og nøgler, der ligger i en fil på computeren. (NB1)	214	56.73
Jeg bruger en adgangskode kombineret med nøgler, der ligger uden for computeren, for eksempel på et token eller nøglekort. (NB2)	105	27.70
Jeg bruger engangskoder. (NB3)	13	3.43
Jeg ved ikke helt, hvad disse muligheder går ud på. (NB4)	28	7.39
Andet	18	4.75
Ikke besvaret	0	0.00

Q7.10 Når du nu ikke bruger netbanking, hvad er den vigtigste grund til dette?
Besvares kun hvis svar på Q7.2 var 'Nej´

Svar	Antal	Procent
Jeg synes, det er for usikkert. (NOB1)	21	56.76
Jeg er bange for at taste forkert og sende pengene et helt forkert sted hen. (NOB2)	2	5.41
Jeg forstår ikke, hvordan man gør. (NOB3)	0	0.00
Jeg foretrækker at fortsætte med den gamle metode. (NOB4)	10	27.03
Jeg blev frarådet at gøre det af en, som jeg stoler på. (NOB5)	0	0.00
Andet	4	10.81
Ikke besvaret	0	0.00

Q7.11 Køber du varer på internettet?

Svar	Antal	Procent
Ja (J1)	369	87.86
Nej (J2)	51	12.41
Ikke besvaret	0	0.00

Q7.12 Handler du i danske netbutikker?
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Ja (J1)	359	97.29
Nej (J2)	10	2.71
Ikke besvaret	0	0.00

Q7.13 Handler du i udenlandske netbutikker?
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Ja (J1)	212	57.45
Nej (J2)	157	42.55
Ikke besvaret	0	0.00

Q7.14 Hvordan betaler du, når du handler på internettet? Du må gerne bruge boksen til at tilføje en nærmere forklaring på, hvornår du gør det ene og hvornår det andet.
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Jeg betaler med et betalingskort, f.eks. Dankort.	225	31.77
Jeg betaler med et kreditkort, f.eks. Visa, Mastercard e.l.	260	36.60
Jeg betaler pr. efterkrav.	31	4.40
Jeg beder om en faktura, som jeg så betaler.	46	6.52
Jeg bruger bankoverførsel fra min bankkonto.	83	11.77
Andet	6	0.85

Q7.15 Er du opmærksom på, hvordan forretningen beskytter oplysninger om dit kort, når du handler på nettet?
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Ja (Y)	271	73.44
Nej (N)	98	26.56
Ikke besvaret	0	0.00

Q7.16 Undersøger du forretningens politik omkring brug af personoplysninger, når du handler på nettet?
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Ja (Y)	247	66.94
Nej (N)	122	33.06
Ikke besvaret	0	0.00

Q7.17 Har du nogensinde opgivet pinkoden til dit kredit- eller betalingskort, når du har handlet på nettet?
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Ja (Y)	10	2.71
Nej (N)	359	97.29
Ikke besvaret	0	0.00

Q7.18 Har du nogensinde været ude for, at dit kredit- eller betalingskort er blevet misbrugt i forbindelse med e-handel?
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Ja (J1)	17	4.62
Nej (J2)	350	95.11
Ved ikke (J3)	1	0.14
Ikke besvaret	0	0.00

Q7.19 Har du nogensinde været ude for, at dine personlige oplysninger er blevet misbrugt, efter at du har handlet på nettet – f.eks. at du har modtaget uønskede e-mail eller tilbud fra tredjeparter?
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Ja (J1)	37	10.05
Nej (J2)	300	81.52
Ved ikke (J3)	31	8.42
Ikke besvaret	0	0.00

Q7.20 At anvende betalingskort til at betale i netforretninger er, efter din mening:
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Sikkert (SUS1)	119	32.34
Temmelig sikkert (SUS2)	233	63.32
Usikkert (SUS3)	16	4.35
Ikke besvaret	0	0.00

Q7.21 Når du anvender betalingskort ved køb på nettet, er du sikret af særlige regler?
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Ja (J1)	299	81.25
Nej (J2)	14	3.80
Ved ikke (J3)	55	14.95
Ikke besvaret	0	0.00

Q7.22 Vil du kunne få refunderet beløbet fra banken, hvis der blev hævet penge på din konto, uden at du har givet lov?
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Ja, altid (JNM1)	200	54.35
Nej, aldrig (JNM2)	3	0.82
Under visse betingelser (JNM3)	152	41.30
Ved ikke (JNM4)	13	3.53
Ikke besvaret	0	0.00

Q7.23 Har du hørt om, at der findes en mærkningsordning for tryg og etisk forsvarlig færden og handel på internettet, som hedder "e-mærket"?
Besvares kun hvis svar på Q7.11 var 'Ja´

Svar	Antal	Procent
Ja (J1)	279	73.37
Nej (J2)	75	20.38
Ved ikke (J3)	23	6.25
Ikke besvaret	0	0.00

Q7.24 Handler du i netbutikker, der ikke har et "e-mærke"?
Besvares kun hvis svar på Q7.11 og Q7.23 var 'Ja´

Svar	Antal	Procent
Ja (J1)	103	38.15
Nej (J2)	114	42.22
Ved ikke (J3)	53	19.63
Ikke besvaret	0	0.00

Gruppe 8

Mobiltelefoner

Denne sidste gruppe spørgsmål bruges til at undersøge respondentens viden om sikkerhed på mobiltelefoner og hvordan man kan beskytte sig. Gruppen introduceres for respondenten med teksten:

> *Mobiltelefoner er hvermandseje – og efterhånden kan de bruges til rigtig mange ting. Ikke blot til at ringe til folk, men også til spil, til at holde styr på private oplysninger såsom adresselister og meget andet. Og så kan man komme på nettet fra sin mobiltelefon, så man kan søge oplysninger og downloade billeder og andre sjove ting. Eller man kan bruge Bluetooth til at komme i kontakt med hjælpeudstyr – eller eventuelt andre telefoner uden at ringe op.*
>
> *Giver disse muligheder nogle risici? Og kan man gøre noget ved dem? Det handler spørgsmålene i dette modul om...*

De enkelte spørgsmål og de indsamlede svar er som følger:

Q8.1 Har du en mobiltelefon?

Svar	Antal	Procent
Ja (Y)	406	96.90
Nej (N)	13	3.10
Ikke besvaret	0	0.00

Q8.2 Accepterer du at modtage data på din telefon via Bluetooth?
Besvares kun hvis svar på Q8.1 var 'Ja´

Svar	Antal	Procent
Ja (J1)	99	23.63
Nej (J2)	291	69.45
Ved ikke (J3)	29	6.92
Ikke besvaret	0	0.00

Q8.3 Tror du, at man kan få virus på sin mobiltelefon?
Besvares kun hvis svar på Q8.1 var 'Ja´

Svar	Antal	Procent
Ja (JNV1)	355	84.73
Nej (JNV2)	22	5.25
Ved ikke (JNV3)	42	10.02
Ikke besvaret	0	0.00

Q8.5 Tror du, man kan overføre virus fra din PC til mobilen?
Besvares kun hvis svar på Q8.1 var 'Ja´

Svar	Antal	Procent
Ja (JNV1)	273	65.16
Nej (JNV2)	48	11.46
Ved ikke (JNV3)	98	23.39
Ikke besvaret	0	0.00

Q8.7 Tror du, man kan overføre virus fra mobilen til din PC?
Besvares kun hvis svar på Q8.1 var 'Ja´

Svar	Antal	Procent
Ja (JNV1)	272	64.92
Nej (JNV2)	51	12.17
Ved ikke (JNV3)	96	22.91
Ikke besvaret	0	0.00

Q8.9 Har du nogen sikkerhedsmekanismer på din mobiltelefon?
Besvares kun hvis svar på Q8.1 var 'Ja´

Svar	Antal	Procent
Ja (J1)	111	26.49
Nej (J2)	207	49.40
Ved ikke (J3)	101	24.11
Ikke besvaret	0	0.00

Appendix A

Samlede tekstsvar på spørgsmål

Dette appendix indeholder de samlede, detaljerede svar fra en række spørgsmål, hvor respondenterne blev bedt om at skrive en kort tekst eller forklaring, eller hvor spørgsmålet gav mulighed for de angive et svar "Andet", hvor man i et fritekstfelt kunne specificere dette nærmere.

Da der i flere af spørgsmålene kom enslydende svar fra en række respondenter, er svarene for hvert spørgsmål samlet med en angivelse af, hvor mange respondenter afgav samme svar. Ved optællingen ignoreres åbenlyse tastefejl og mindre stavevarianter, således at for eksempel "administrator" og "administator" ville betragtes som samme svar. Tilsvarende ignoreres forskellige former for ellipsis og små grammatiske varianter i svarene, således at for eksempel "Jeg gør det selv", "Gør det selv" og "gøre det selv" ville betragtes som samme svar.

A.1 Beskæftigelse

Samlede detaljerede svar på Q0.9.

Beskæftigelse	Antal
A/V tekniker	1
Account manager	2
Adm. chef	1
Administrativ og bogholderi	1
Administrator for en fond	1
Advokatsekretær	1
Afdelingschef	2
Afdelingsleder	1
Anæstesisygeplejerske	2
Assurandør	1
Automekaniker	1

Fortsættes på næste side

Beskæftigelse	Antal
Bager	1
Bedemand	1
Beton pumpe	1
Bibel-arbejder	1
Bioanalytiker	1
Biolog	1
Blikkenslager	1
Blomsterhandler	1
Bogholder	1
Bogtrykker	1
Butiksassistent	1
Butiksslagter	1
Bygningssnedker	1
Cafeteriamedhjælper	1
Chauffør	6
Chef for Søværnets Sergent- og Grundskole	1
Chefkonsulent	1
Client coordinator	1
CNC operatør	2
Coach og konsulent	1
Dagplejer	1
Direktionssekretær	1
Direktør	1
Direktør/massør	1
Disponent	1
e-business konsulent	1
Ejendomsserviceteknikker	1
Ekspedient ved VVS grossist	1
Ekspeditionssektær - offentlig ansat	1
Eksportchauffør	1
Elektriker	3
Fabriksarbejder	4
Fagforening	1
Faglært	1
Faglært på depot	1
Faglig konsulent	1
Farmakonom	1
Fibertekniker	1

Fortsættes på næste side

Beskæftigelse	Antal
Fiskeindustriarbejder	1
Flytekniker	2
Flyveleder	2
Folkeskolelærer	4
Forsendelse og modtagelse/ad hoc	1
Forsker	2
Forskningslektor	1
Friskolekonsulent	1
Fuldmægtig	2
Fuldtid: Kontor - Deltid: Brandmand	1
Funktionær	3
Fysioterapeut	1
Fængselsbetjent	1
Fødevarekontrolant	1
Førtidspensionist	1
Geolog	1
Grafiker	1
Grafisk designer	1
Greenkeeperassistent	1
Havnearbejder	1
Husassistent	1
Håndværker	2
Indehaver af reklamebureau	1
Indkøber	1
Industri/produktion	1
Ingeniør	7
Inspektør	2
Integrations Tester	1
Isenkram/lager på tømmerhandel	1
IT almuligmand	1
IT og Administration	1
IT-chef	1
IT-driftschef	2
IT-konsulent	4
It-medarbejder	1
IT-specialist	1
IT-supporter	3
IT-udvikler	1

Fortsættes på næste side

Beskæftigelse	Antal
Jobrådgiver	1
Jordbrugstekniker	1
Jurist	3
Kartonagearbejder	1
Kok	1
Kommunalt ansat	1
Kommunikationsmedarbejder	1
Kommunal assistent (HK)	1
Konstruktør	1
Konstruktør - Tilbudsberegning	1
Konsulent	6
Konsulent chef IT	1
Kontorleder	1
Kontoransat	1
Kontorassistent	5
Koordinator	1
Kriminalassistent	1
Kundechef	1
Kundekonsulent	2
Laborant	2
Læge	3
Lægesekretær	1
Lærer	14
Lager og terminalarbejder	1
Lager og logistik	1
Lagerarbejder	4
Lagerassistent/pedel	1
Lagerekspedient	1
Lagermand	1
Lagermedarbejder	1
Lager-truckfører	1
Lastvognsmekaniker	1
Ledende bioanalytiker	1
Leder	3
Lektor	3
Lektor/ingeniør	1
Levnedsmiddeltekniker	1
Logistikassistent	1

Fortsættes på næste side

Beskæftigelse	Antal
Logistikchef	1
Lokomotivfører	3
Maler	1
Marketingkoordinator	1
Marketingmedarbejder	1
Maskinarbejder	3
Maskinmester	1
Maskinteknikker	1
Materielassistent	1
Materielkonsulent	1
Mellemleder i en kommune	1
Metal arbejder	2
Miljøtekniker	1
Montør	2
Murer/kloakmester	1
Musiker	1
Officer	1
Opstiller/reparetør	1
Overlæge	1
Oversætter	1
Pedel	1
Planlægger	1
Portør	1
Postbud	2
Postomdeler	2
Praktiserende fysioterapeut	1
Praktiserende læge	1
Procesoperatør	1
Production virksomhed	1
Produktion	1
Produktionsass	1
Produktionsmedarbejder	2
Programmør	2
Project coordinator	1
Projektleder	1
Psykolog	1
Psykolog/psykisk arbejdsmiljø/fagforening	1
Pædagogmedhjælper	1

Fortsættes på næste side

Beskæftigelse	Antal
Pædagog	9
Pædagog og afdelingsleder	1
Pædagog og voksenunderviser	1
Pædagogisk assistent	1
R&D Manager	1
Rejsekonsulent	1
Renggør	1
Rengøringsassistent	2
Revisor	3
Sagsbehandler	2
Salgsassistent	2
Salgsingeniør	2
Salgskonsulent	1
Salgskoordinator	1
Saxofonist/Musikskolelærer og ensemblechef	1
Sceneinstruktør	1
Sekretær	3
Selvstændig	4
Selvstændig arkitekt	1
Selvstændig landmand	1
Selvstændig praktiserende Fysioterapeut	1
Selvstændig rengøring og vinduespudser	1
Selvstændig/freelancer	1
Senior Application Engineer	1
Servicearbejder	1
Servicekonsulent	1
Serviceleder	1
Servicemesarbejder	3
Servicetekniker	2
Shippingmand	1
Skibsass.	3
Skoleinspektør	1
Smed	1
Socialformidler	1
Social og sundhedsassistent på hospital	1
Social og sundhedsassistent på plejehjem	1
Socialpædagog	2
Socialrådgiver	2

Fortsættes på næste side

Beskæftigelse	Antal
Softwareudvikler	2
Soldat	1
Specialarbejder	12
Specialarbejder på renseanlæg samt brandmand	1
Specialkonsulent	1
Ssh	1
Statsautoriseret revisor	1
Supervisor	1
Supervisor Vedligehold	1
Support	1
Sygeplejerske	5
System Administrator	1
Systemudvikler	1
Systemadministrator	1
Systemkonsulent	1
Systemsdrift	1
Sælger	1
Tandplejer	1
Tekniker	2
Tekniker/leder	1
Teknisk assistent	2
Teknisk chef	1
Telefonsupporter	1
Telemarketing + telefonomstilling	1
Tjener	2
Tjenestemand	1
Tolk	1
TV/Digital-TV og Inet til slutbruger	1
Tømrer	2
Uddannelseskoordinator	1
Udviklingskonsulent	2
Ufaglært	1
Underviser	2
Underviser på Handelsgymnasiet, lektor/cand.merc.	1
Uuddannet hjemmehjælper	1
Vejleder	1
Veligeholdelsestekniker	1
Vicevært	2

Fortsættes på næste side

Beskæftigelse	Antal
Virksomhedskonsulent	1
Værkstedsleder	1
Økonomi controller	1
Økonomichef	3

A.2 Anden anvendelse af computeren

Samlede svar fra Q0.15 vedrørende anden anvendelse af computeren end de anvendelser, der eksplicit er nævnt i spørgsmålet.

Anden anvendelse	Antal
Administration	1
Afspille musik	1
Alt	2
Arbejde	2
Audiobehandling	1
Beregninger	1
Bogføring for firma	1
Broderi	1
Budget	1
C++	1
Database	5
Dataopsamling	2
Deltagelse i forskellige fora	1
Design af broderier	1
E-boks o.l.	1
E-læring	2
Facebook	2
Film	1
Filmredigering	1
Foreningsarbejde	1
Gemme musik mv.	1
Gfk	1
Hjemmeside	4
Høre netradio	1
Java	1
Komponering/notering af musik	2
Konkurencer	1

Fortsættes på næste side

Anden anvendelse	Antal
Lydmanipulation	1
Meget forskelligt	1
Musik	3
Musikprogrammer	1
Musiksamling	1
Mønstre til symaskine	1
Nodesats	1
Office-pakken	2
Porno	1
Privatøkonomi (Regneark)	1
Programmering	6
QSL	1
Reading	1
Regneark	12
Regnskab	10
SW udvikling	1
Skak	1
Slægtsforskning	3
Surfing	1
Svineprogram	1
Tegning	1
Troubleshooting moderator hos heavengame.com	1
Vedligeholde	1

A.3 Andre videnskilder

Samlede svar fra Q1.9 vedrørende hvilken andre kilder, som der er hentet viden fra, ud over de videnskilder, der eksplicit er nævnt i spørgsmålet.

Anden videnskilde	Antal
Alm. forsigtighed	1
Andre personer	1
AOF	1
Arbejdsgiver	1
Arbejdsplads	18
Artikler	1
Bank	1
Bank og e-boks	1
Bekendte	2
Blade/ugeblade	1

Fortsættes på næste side

Anden videnskilde	Antal
Bredbåndsleverandøren	1
Bøger/hæfter	8
Børn	10
Chat forums m.m.	1
”Computer for alle”	4
Computerblade	3
Computermagasin på arbejde	1
Del af kursus	1
EDB magasiner	1
En god/dygtig ven	2
Fagblade/faglitteratur	5
Familiemedlem	7
Folk i IT-branchen	1
Forhandlere	2
Forum og venner	1
Fra Stofa	1
Fra person til person	1
Fra personer som arbejder med computer	1
Fået i forbindelse med IT-kørekort	1
Generel erfaringssnak	1
Gennem andre	1
Interesse: har forhørt mig	1
Intet	1
It-afdelingen internt	1
It-afdelingen på arbejdsplads	1
It-blade	2
It-konsulent	2
It-ekspert	2
It-medarbejder på arbejde	4
It-tekniker	1
Jeg er Radioamatør	1
Jeg følger dagligt med i nyheder og lignende på nettet	1
Kollegaer	13
Konferencer	1
Konsulentfirmaer	1
Kurser	4
Landbrugsrådgivning	1
Leverandører	1

Fortsættes på næste side

Anden videnskilde	Antal
Litteratur og sund fornuft	1
Lærebøger	1
Magasiner	1
Magasiner, uddannelse	1
Microsoft	1
Microsoft, Mcafee	1
Mit netværk	1
Månedsblade	1
Nabohjælp fra ekspert	1
Nej	1
Netbank	1
Omtale	1
PC-firma	1
PC-blade/-magasiner	6
Personalehåndbog	1
Personer	1
Personer i min privatsfære	1
STOFA Safe-mail	1
Samarbejdspartnere	1
Selvlært	3
Sikkerhedspolitikker på arbejdet	1
Sikkerhedsbriefinger	1
Skolen	1
Softwarehuse	1
Stofa	2
Styresystemerne / XP f.eks.	1
Symantec m.fl.	1
Tidsskrifter	4
Tænk	1
Uddannelser	1
Usenet	2
VUC + arbejdsgiver	1
Venner og bekendte	13
Venner og familie	2
Venner og kolleger	6
”Von høren sagen”	1
Vores EDB leverandør	1
Øvelse	1

Fortsættes på næste side

Anden videnskilde	Antal

A.4 Andre, der tager sig af it-sikkerhed i hjemmet

Samlede svar fra Q1.10 vedrørende hvem der, ud over respondenten selv, tager sig af it-sikkerhed på computeren i hjemmet.

Anden person	Antal
Arbejdsgiver	1
Bekendt	3
Edb mand	1
En god/dygtig ven	5
Hjælp fra IT medarbejder	1
Internetudbyder	2
Kaspersky	1
Konsulent	1
Kæreste	1
McAfee	1
Min ægtefælles arbejdsplads	1
Nabo	1
Norton	2
Familiemedlem + ven	1
Privat konsulent	1
Prof.tekniker	1
Sikkerhedsprogrammerne	1
Skolens it-afdeling	1
Stofa saifsurf saifmail	1
Udbyder, eksperter	1
Ung mand, søn af en bekendt	1
Vores EDB leverandør	1
Ikke gjordt så meget.	1
Ingen	1

A.5 Medier til sikkerhedskopier

Samlede svar fra Q2.2 og Q2.6 vedrørende hvilken medier, der benyttes til at tage sikkerhedskopier på, ud over dem der eksplicit er nævnt i spørgsmålene.

Andet medie, når respondenten tager kopier	Antal
Back up ved antivirus program	1
Diskette	4
E-boks	3
E-Server	1
Ekstern server	1
Eksternt	1
Ftp-server	1
Internet backup	4
NAS	1
Netdrev	1
Nettet	1
Nr 2 disk	1
Online backup	1
Opbevares i brandsikkert skab	1
På papir	23
Papir gemt et sikkert sted	1
Papir i ringbind	1
Plads på internettet Norton	1
Raid 5 NAT	1
Separat partition på HD	1
Servere på nettet	1
Synkroniseres i ”skyen”vha. Dropbox	3

Andet medie, når andre tager kopier	Antal
Backup-server	1
Diskette	1
Formoder at bank mv gemmer kopi af det de sender til mig	1
Gemmer dokumenter på mail	2
Internet backup	4
Keep it	1
Net HDD	1
Online medier	1
Papirkopi og e-boks	1
Web backup	1

A.6 Gemning af sikkerhedskopier

Samlede svar fra Q2.4x og Q2.8 vedrørende anden placering af sikkerhedskopier end dem, der eksplicit er nævnt i spørgsmålene.

Placering af kopier taget af respondenten	Antal
Alt efter art	1
Bankboks	2
Boks i andet rum	1
Både ved PC, og på internet samt på arbejde (to USB-disk)	1
Både ved computeren, samt på nettet	1
Cd i et skab - mit USB har jeg oftest med mig og det ligger i en lille pung som er i min taske	1
De vigtigste i bankboks	1
E-boks	2
Ekstern harddisk	1
Ekstern harddisk på internettet.	1
Ekstern server	1
Eksternt	1
Flere steder	2
Forskelligt afhængig af tidspunkt	1
Gemt af vejen	1
Gemt i et andet rum i huset	1
Hos ekstern backupudbyder	1
I bunken af brændte cd/dvd	1
I en skuffe	1
I et andet rum i huset	1
I et skab	1
I et skab i stuen	1
I kasse på kontorrum	1
I kælderen	1
I mapper	1
I mit fysiske skrivebord	1
I særskilt rum / uden for huset	1
Lidt af hvert	1
Lige ved PC'en og udenfor huset	1
Netdrev (internetserver)	1
Online	2
På Nortons internet plads	1

Fortsættes på næste side

Placering af kopier taget af respondenten	Antal
På PC på arbejdsplads	1
På aflåst kontor på arb.	1
På mindst to computere i huset, på eksternt drev samt på jobcomputer på arbejdsplads	1
På USB nøgle	1
Reoler	1
Samme rum som PC'en	1
Skab i PC-rummet	1
Skuffe	1
Særskilt skuffe	1
Taske	1
Ved PC og på en anden matrikel	1
Ved pc og på nettet	1
En hemmelighed	1
Hemmeligt	1
Hemmeligt sted	1

Placering af kopier taget af andre	Antal
E-boks	1
Ekstern harddisk på nettet.	1
Flere steder !?	1
Hos familie.	1
I kasse på kontorrum	1
I servermiljøer	1
Internet	1
Keepit	1
På andre computere	1
På ekstern server	1
Hemmeligt	1

A.7 Hvordan huskes adgangskoderne

Samlede svar fra Q3.3 vedrørende hvordan respondenterne husker deres adgangskoder, ud over de metoder der eksplicit er nævnt i spørgsmålet.

Hvordan huskes koderne	Antal
Adgangskodet fil på computer	1
Alfanumerisk blanding	1
Banken husker jeg, resten er i krypteret fil	1
Bruger en tal- og ordsammensætning, der er let at huske.	1

Fortsættes på næste side

Hvordan huskes koderne	Antal
Bygger på undervisning fra mine studier	1
Både husker og gemmer på fil	1
De mere ”ligegyldige”, som er de fleste, er i en speciel mailmappe	1
De står i en notesbog	1
Der er et adgangssystem på computeren med fingeraftryk, så jeg bruger fingeraftryk for at komme ind på en given side.	1
Ekstern fil på PDA	1
En kombination af forkortelser, tal og tegn, som kun jeg kender baggrunden for.	1
En lille bog	1
En vigtig dato	1
Et bestemt bind i et andet rum	1
Ét simpelt password til ufarlige steder - f.eks. fora. Ét kompliceret ”basis password”med variationer til formålet - f.eks. kunne netbank passwordet indeholde ”nB”et bestemt sted	1
Familiemedlem + tal	1
Figurer i tegneserier + tal system jeg har labvet	1
Fil på ekstern harddisk	1
Flere metoder afhængig af om det er koder jeg selv har lavet og hvor tit de skal bruges	1
Forskellige metoder, afhængige af sikkerhedsniveau	1
Gemmer dem mellem noget andet	1
Gemmer på andet medie	1
Gemt bag mine madopskrifter	1
Gemt i andet rum.	1
Gemt i bog i andet lokale	1
Gemt i ringbind	1
Gentagelse af tegnene i hovedet til jeg kan dem.	1
Har 2-3 faste passwords	1
Har flere forskellige metoder alt efter kode	1
Har opfundet et ord der ikke findes	1
Huskeseddel som er gemt	1
Huskeseddel, men går ikke rundt med den!!	1
I en lommebog i huset	1
I mappe med andre oplysninger placeret andet sted i huset	1
I notesbog	1
Jeg anvender ord for begivenheder kun jeg kender til tilsat tal, kun jeg kender betydningen af	1

Fortsættes på næste side

Hvordan huskes koderne	Antal
Jeg bruger en 3-4 forskellige koder	1
Jeg bruger et sikkert kode system som løbende ændres	1
Jeg bruger forskellige metoder	1
Jeg bruger krypteret sofware	1
Jeg har dem et hemmeligt sted	1
Jeg har et ord er går igen som er 2/3 resten varierer jeg	1
Jeg har et system der hedder roboform så jeg skal bare huske et pasword	1
Jeg har et system jeg varierer mine passwords efter	1
Jeg har klæbehjerne	1
Jeg husker de vigtige	1
Jeg husker dem/lærer dem udenad	18
Jeg husker dem, derfor må nogle være gengangere	1
Jeg husker dem, men har en seddel ved min pc, som fortæller hvor jeg bruger det samme password	1
Jeg husker dem uden videre, og de uvigtige skriver jeg i en krypteret fil	1
Jeg skriver dem på en huskeseddel der opbevares andetsteds, eller husker dem uden at skrive dem ned	1
Kombination af barns kælenavn og fødselsår	1
Kombination af lange sammenskrevne ord og tal	1
Kombination af navne og datoer, krypteret af mig	1
Kombination af navne og tal men i ændret rækkefølge	1
Kontekstbaseret	1
Krypteringssoftware	1
LastPass.com adgangskodehusker	1
Ligger et andet sted	1
Lille bog som er gemt væk	1
Mærkelig talkombinationer. Nogen gang har det noget med mig selv at gøre, andre gange har det ikke.	1
Mærkelige ord	1
Man er vil lidt autist	1
Men fortæller det ikke for at bevare sikkerheden.	1
Min egen regel med store og små bogstaver	1
Min telefonbog	1
Musikalsk lydudtryk	1
Navnet på et kæledyr efter fulgt af en talkombination	1
Nedskrevet men opbevaret i boks	1
Nogle af dem som de fire sidste cifre i opdigtede personeres numre kodet ind på min mobil	1

Fortsættes på næste side

Hvordan huskes koderne	Antal
Norton Internet Security	1
Ord jeg let kan huske, men som ikke kan forbindes til familie, venner, fødselsdag etc.	1
Ord og tal som kun jeg kender betydningen af	1
På en stik	1
Password manager app	1
PDA	1
Personlig ting	1
Program 1Pssword (mac)	1
PWDatabase på memorystick	1
Særlig fil på andet medie	1
Særlig fil på nettet	1
Særskilt opbevaret lister	1
Skiftevis konsonant vokal og tal i midten iblandet et tal	1
Skjult andet sted i huset	1
Skrevet i en lille bog, som er gemt og bruger også bestemte ting i mit liv til at oprette koderne med	1
Skriver dem ned, men gemmer dem ikke ved computeren	1
Skriver dem på en huskeseddel, som er gemt et sikkert sted	1
Skriver det i min kalender	1
Skriver en liste på papir	1
Specielle kombinationer af oplysninger	1
Specielt krypteret program	1
Spredt i mapper i reol	1
System med løbende skift	1
Tal og bogstaver	1
Tekstfil på USB-nøgle	1
Ting jeg personligt kan huske	1
Ved mindre vigtig data bruger jeg familiemedlem navn, ved mere vigtig data husker jeg en svære kodeord, og ved vigtig data har jeg selv lavet en som jeg kan lave om og stadig huske.	1
Vrøvleord + tal	1
Oplyses ikke	1
Som er hemmelig!	1
Vil ikke oplyse den	1

A.8 Hvordan ser en god adgangskode ud?

Samlede svar fra Q3.6 vedrørende hvordan respondenterne ville beskrive en god adgangskode, ud over de metoder der eksplicit er nævnt i spørgsmålet.

Hvordan beskrives en god adgangskode	Antal
Behovet kommer helt an på, hvad sikkerhedsløsningen ellers består af	1
Den skal være på mindst 13 tegn	1
DwryufTY75RFf	1
Fingeraftryk	1
Gerne mere end 8 tegn	1
Godt lydbillede eksempelvis ”palasa”	1
Kombination af tal og bogstaver min. 11 tegn	1
Mindst 12 forskellige tegn	1
Mindst 12 tegn er den regl jeg selv går efter.	1
Mindst 8 tegn både tal og bogstaver	1
Ord og tal	1
Skal indeholde ord, navne eller tal som ikke matcher ens cprnr, adresse, navn eller lignende. rissengrød er en god kode med mindre man har fødselsdag den 24.12	1
Tal bogstaver store og små og tegn	1
Tal, store og små bogstaver	1
Oplyses ikke	1

A.9 Opdatering af virusskanner

Samlede svar fra Q4.5 vedrørende hvem det er, der sørger for at virusskanneren holdes ajour, ud over de personer der eksplicit er nævnt i spørgsmålet.

Hvem holder virusskanneren ajour	Antal
Antivirus-udbyderen	1
Antivirusprogram selv opdaterer automatisk	26
Automatisk ved logon	1
En dygtig ven	2
Internetudbyderen	11
Jeg har verdens bedste program	1
Leverandøren af programmet	6
Mac computer	2
Min søn	1
Stofa	12
Stofa Safe Surf	4
Telia Stofa	2
Virksomhed	1
Ingen	1
Jeg bruger ikke AV	1

A.10 Fjernelse af virus

Samlede svar fra Q4.6 vedrørende hvordan respondenterne får fjernet virus, ud over de metoder der eksplicit er nævnt i spørgsmålet.

Metode til fjernelse af virus	Antal
Bruge flere virusscannere såvel installerede som online og i safemode eller fra DOS-disk.	1
Det der er nødvendigt for at slippe helt af med den	1
Det kommer an på, hvad den er inficeret med. Mange trusler kan blot fjernes, mens andre er så systemnære, at der skal skrappere midler i brug	1
Først bruge virusfjerneren, hvis ikke virker, bruge min seneste virusfri backup	1
Få et godt råd	1
Få hjælp af familiemedlem	1
Få maskinen tømt	1
Hente hjælp hos en ekspert/sagkyndig	3
Hive fast i min svoger	1
Hvad der er nødvendigt !?	1
Jeg bruger Mac, så jeg tænker ikke voldsomt meget over virusangreb!!	1
Klage til min netleverandør	1
Kommer an på virussen	1
Konsultere min søn	3
Kontakte spywarefri.dk	1
Pakke en imagefil ud som genskaber systemet	1
Rense hardisk med Dereks nukem	1
Skulle det ske, indsender jeg den til programudbyderen	1
Slukke og tilkalde vores EDB firma	1
Søge råd hos svigersøn	1
Tilkalde reparatør	1
Virusfjerneren + Ego slette	1

A.11 Hvordan bestemmes, om links følges

Samlede svar fra Q5.5 vedrørende hvordan respondenterne bestemmer om links skal følges, ud over de metoder der eksplicit er nævnt i spørgsmålet.

Hvordan bestemmes, om links følges	Antal
Alt fis fra familie og venner bliver uden videre slettet	1
Benytter en ”mail vasker”	1
Bruger det stort set aldrig	1

Fortsættes på næste side

Hvordan bestemmes, om links følges	Antal
Checket linket i mailens properties	1
Holder musen hen over linket og ser adressen.	1
Hvis jeg er i tvivl googler jeg den	2
Hvis jeg har mistanke om en falsk mail, ringer jeg først til vedkommende.	1
Hvis tvivl efter ovenstående, tjekker mailens Egenskaber om linket der er OK.	1
Jeg er meget mistænksom/mistroisk	3
Jeg kigger på den URL der henvises til i linket	1
Jeg kigger på link-adressen om den ser OK ud	1
Jeg ser på om websitet er til at stole på	1
Kan som regel se om det er en ”rigtig”mail, i modsat fald sletter jeg den	1
Kigger på URL mv.	4
Om den faktiske URL ser harmløs ud	1
Ser i statuslinjen hvor linket peger hen	1
Som Q5.4	1
Spurgte Stofa i dette tilfælde	1
Sund fornuft	1
Sund fornuft og en del viden	1
Tjekker koden !	1
Vurderer afsender og tekst i emne fra oversigten	1

A.12 Harmløse linknavne

Samlede detaljerede svar på spørgsmål Q5.6. Svarene er grupperede efter den overordnede strategi for håndtering af links.

Harmløse linknavne	Antal
Relateret til navnets struktur:	
Ikke .exe eller lignende	1
At linknavnet ikke er som : www.sporrt.com/adidsex	1
F.eks. www.damske.bank der kan forveksles i stedet for det korrekte www.danske.bank	1
Stavemåden landekode	1
Baseret på forhåndskendskab til navnet:	
A la youtube eller links til hjemmesider mine venner og jeg interessere os for.	1
At den kommer fra et kendt sted f.eks. dr.dk og at det er en filtype jeg kender	1
Det er et jeg kender til på en eller anden måde!	1

Fortsættes på næste side

Harmløse linknavne	Antal
En hjemmeside man kender, men her skal man se efter om navnet også er stavet korrekt, ellers kan man blive henvist til en falsk hjemmeside	1
En hjemmeside, jeg kender i forvejen for eksempel.	1
En jeg ikke kender smider jeg ud	1
En link som indeholder en gennemskuelig sti.	1
Et harmløst link, linker til et domæne jeg kender eller kan se ikke virker suspekt	1
Et site jeg kender	1
Firmahjemmeside du kender. Sjov hjemmeside du kender i forvejen mailen er skrevet i et sprog, som du ved afsenderen bruger til dagligt. Linket til denne test var forudsigeligt, selv om jeg ikke kendte afsenderen	1
Fx som http://www.dr.dk/ Linket går til en kendt side. Links til hjemmesider af tvivlsom karakter googler jeg ofte først.	1
Hedder ikke noget med 'gratis' eller 'xxx'. Links til hjemmesider jeg kender.	1
http://surveys.imm.dtu.dk/limesurvey/index.php	1
Hvis det "lyder" rigtigt.	1
Hvis det er et link til en forenings hjemmeside som jeg kender. Som oftest checker jeg mine e-mails via web-mail fra en anden computer end min egen. Disse computere har kraftige internetsikkerheds programmer så her vil jeg roligt kunne åbne et link jeg har mistanke til.	1
Hvis det virker bekendt i forhold til de sider jeg normalt besøger. Tjekker også om linket peger det samme sted hen som teksten antyder	1
Ikke alene - skal kædes sammen med en harmløs URL	1
Man kan se i navnet om der er kendte navne i linket, f.eks. dr.dk eller folketinget.dk	1
Om domænet er et jeg kender	1
Som skrevet alt "sjovt" fra familie og venner bliver slettet. Det flyder rundt med underlige links. Den slags slettes. Hvis jeg er det mindste i tvivl virusscannes linket eller mailen slettes	1
Webadresser, man kan genkende	1
www.elgiganten.dk	1
Relateret til afsender:	
Det kommer fra en adresse, jeg i forvejen kender. Det har ikke underlige vedhæftede filer med syntaktisk, sproglige pudseløjerlige navne.	1
Det vigtigste er, at jeg har tillid til afsenderen. Der må ikke være stavefejl i linket. Hvis jeg er i tvivl, så undlader jeg at klikke på linket.	1

Fortsættes på næste side

Harmløse linknavne	Antal
Relateret til mailens emne:	
Emne af relevans til mailen	1
For mig er et harmløst linknavn selve linket som kan læses i selve mailen.	1
Generelt tjekker jeg altid linket i mailens egenskaber hvor jeg også ser på mailens Header.	
Ikke noget med porno/viagra/funny links/lette penge i Afrika/genvej til store muskler	1
Diverse svar, inkl. uklare strategier:	
Det kan f.eks. være inden for sport el. mode	1
Junk mails	1
Kommer af sig selv efter lang erfaring.	1
Læs mere om at rejse til London her	1
"Ved ikke" og lignende svar: Nej	14
Nej ikke rigtig - men oftes når der er sendt link med til de mail jeg modtager - så er det fra familie, som måske har lavet link til billeder på pisca eller youtube, ellers er det link til undersøgelser som jeg selv har sagt ja tak til at deltage i så som denne	1
Nej ikke umiddelbart	1
Nej, ikke helt, men så snart jeg er i tvivl bliver den straks slettet.	1
Nej, kan ikke forklare det. Det er en blanding af forskellige parametre.	1
NEJ. Men ser det blot mystisk ud bliver det kasseret.	1
Vanskeligt, men tror ikke det er et problem.	1

A.13 Hvordan bestemmes, om vedhæftede filer åbnes

Samlede svar fra Q5.7 vedrørende hvordan respondenterne bestemmer om de skal se på vedhæftede filer, ud over de metoder der eksplicit er nævnt i spørgsmålet.

Hvordan bestemmes, om filer åbnes	Antal
Benytter en "mail vasker"	1
Billeder er JPG filer, andet er TXT eller wordfiler	1
Er det forventet dokument, eller er det noget jeg ikke har bedt om at få	1
Er jeg i tvivl kontakter jeg først afsender. Ellers sletter jeg mailen.	2
Er opmærksom på de farlige endelser som .exe	1
Filtyper, kilde og om mailen ser legitim ud	1
Hvilken filtype	1
Hvis jeg er det mindste i tvivl sletter jeg mailen	1
Hvis jeg er i tvivl tjekker jeg filendelsen	1
Hvis jeg har godkendt mailen stoler jeg også på indholdet og attachments	1

Fortsættes på næste side

Hvordan bestemmes, om filer åbnes	Antal
Hvis jeg ikke er orienteret om attachment af anden kanal, åbner jeg det ikke	1
Jeg åbner ikke en vedhæftet fil hvis jeg ikke ved hvor den kommer fra	2
Jeg åbner ikke noget som jeg ikke har tiltro til	1
Jeg åbner kun ikke-eksekverbare vedhæftede filer	1
Jeg kigger på filnavnet. Jeg er udmærket klar over hvilke filer der kan være skadelige.	1
Jeg scanner altid attachments	2
Jeg scanner vedhæftningen for virus	4
Meget forsigtig med at åbne noget fra andre	1
Mit styresystem er indstillet til at vise filtype navnet for alle filer.	1
Scanner ofte vedhæftede filer før download	1
Ser på det vedhæftede dokuments extension	4
Tjekker koden !	1
Åbner aldrig filer af usikre typer, exe, com, bat, vbs, og lign.	1
Åbner aldrig vedhæftede filer hvis jeg er det mindste i tvivl om afsender	1

A.14 Harmløse filnavne

Samlede detaljerede svar på spørgsmål Q5.8. Svarene er grupperede efter den overordnede strategi for håndtering af vedhæftede dokumenter.

Harmløse filnavne	Antal
Baseret på filens type:	
.doc	2
.doc .txt .jpg	1
.pdf og .doc opfatter jeg f.eks.som harmløst. De må desuden gerne hedde noget på dansk hvis det er fra en dansker og det må gerne være noget jeg har bedt om/interesserer mig for (eks. ønskeseddel eller opfølgning på en tilmelding til noget/en handel). Eksekverbare filer åbner jeg ikke.	1
At den er fra bekendte mailadr som jeg kender	1
Det ender ikke på mere end eet filtype navn, f eks .doc er OK, .doc.exe er ikke.	1
Det kan f.eks. være .doc eller .pdf eller billeder	1
Det kan jeg ikke, det skal ihvertfald være sendt fra en person jeg har tillid til.	1
Det kan være en kendt filtype som f.eks. et word-dokument	1
Det må ikke være eksekverbare filer, men ellers er jeg ikke helt sikker. Alt der er vedhæftet, som ikke synes relevant for mig, lades uåbnet.	1

Fortsættes på næste side

Harmløse filnavne	Antal
Det må ikke være en exe-fil.	1
Efternavnet på filen - f.eks. *.exe *.wpd	1
Eksekverbare filer skal man passe på. PDF filer tør jeg normalt godt åbne.	1
Eksv. Word fil fra en jeg kender	1
En filtype jeg kender og betragter som rimelig ufarlig f.eks. pdf	1
Ender på doc, pdf ikke exe	1
Et dokument der ikke er en executable	1
Filen afsluttes med docx	1
Filer, der ikke har underlige extensions	1
Fil-extensionen skal svare til den dokumenttype man forventer	1
Fx .dok	1
Hvis det ender på .doc eller .pdf og ikke på .exe eller lign.	1
Hvis det er et format min computer kender, og de øvrige betingelser er opfyldt, vil virusscanneren med stor sandsynlighed finde eventuel virus - hvis det er en exe fil eller anden fil, som aktiverer noget på min computer, tjekkes mailen grundigt. Åbner stort set aldrig exe filer eller lignende.	1
Invitation.doc	2
Jeg åbner ikke programfiler. Men fx .pdf, .jpeg, eller .doc åbner jeg, hvis jeg har tillid til afsenderen.	1
Jeg kan forklare det modsatte. Hvis der står noget udenlandsk vil jeg under omstændigheder åbne.	1
Nej, men potentielt skadelige filer man skal være forsigtig med er f.ex. exe, scr, m.m. og ukendte extentions	1
Pdf, doc, txt	1
Som i sidste svar, så vil en .exe fil være en jeg ikke vil åbne hvis den kom fra en fremmed.	1
Svært, men her er et bud: Et dokumentnavn der har en endelse der indikerer at det er et tekstpogram altså word, wordperfect eller openoffice tekstprogrammet. Hvis der er en .exe fil er det ikke et dokument.	1
Tantesofies sang.txt, Onkel frede.JPG, Publisherfiler og Wordfiler	1
Typen af de vedhæftede filer skal være ikke eksikverebare (exe, bat, com, pif, osv.)	1
Uden .exe, .ddl i filnavnet	1
Uden exe, dll og lignende	1
Virusskanner e.l. godkender den og filtype acceptabel:	
Godkendt af virusskanneren. Ikke en programfil.	1
Jeg har en mailscanner med blackliste og whiteliste	1
Virusscanner accepterer det samt at det ikke er en .exe - .zip - .rar osv fil.	1
Kun pdf og doc der findes ok af virusscanner + fra en kendt afsender.	

Fortsættes på næste side

Harmløse filnavne	Antal
Relateret til afsender:	
En oplysning jeg ved hvor, hvem det kommer fra.	1
En vits sendt fra en bekendt afsender	1
Fra venner/familie	1
Generelt åbner jeg kun dokumenter, som jeg forventer at få noget fra. Der skal være en forklaring på dokumentet i selve mailen.	1
Hvis det er et billede, som en af mine venner har beskrevet i emalen jeg skal og vi evt. også har talt om i anden sammenhæng. Jeg er meget på vagt for for vedhæftelser der slet ikke må være .EXE filer.	1
Navn, som man kender.	1
Ser efter hvor den kommer fra	1
Svært at beskrive, da det kommer an på afsenderen (om det er fra en web-butik eller lign.)	1
Relateret til den kontekst, hvori mailen modtages:	
Det skal have relevans i forhold til mailen. Skal være ventet eller normalt fra afsender at vedhæfte en fil.	1
Et relevant navn i forbindelse med mailens emne.	1
Hvis dokumentnavnet henviser til emnet i mailen, kan det vel betragtes som harmløst. Selvfølgelig afhængig af emnet...	1
Hvis jeg ved at jeg venter en fil eller hvis der er noget vedkommende i filnavnet, ie. ikke noget spamagtigt	1
Ja, det har en titel, som relaterer specifikt til mig arbejdsmæssigt eller privat.	1
Kontext mellem afsender og navn og mine aktuelle gøremål	1
Relevant til emnet i mail	1
Svært, åbner aldrig noget, jeg ikke forventer at modtage - kikker på fil-type, .doc el. lign. intet programmæssigt	1
Diverse svar, inkl. uklare strategier	
Det skal være en filnavn jeg kan kende	1
Hvis jeg kender selve dokumentet.	1
Ikke helt, men måske har den et mærkeligt sprog/udseende	1
Kikker på filtypen	1
personalemøde.ppt	1
Ser på hvad det er for slags filer som er vedhæftet	1
skoleskema	1
turen-til-Sverige.txt	1
"Ved ikke" og lignende svar:	
Nej	24

Fortsættes på næste side

Harmløse filnavne	Antal
Nej :-)	1
Nej egentlig ikke	1
Nej egentlig ikke men mener at kunne vurdere det	1
Nej, det er selvfølgeligt et usikkert kriterium	1
Nej, det vurderes fra gang til gang	1
Nej. En vurdering hver gang	1
Noget jeg ikke har kenskab til klikker jeg ikke på men kasserer	1
Næh..	1
Næh, kan godt se logikken i, at en skadelig fil har et “harmløst” navn.	1

A.15 Håndtering af fortrolige e-mails

Samlede detaljerede svar på spørgsmål Q5.16. Svarene er grupperede efter den overordnede strategi for håndtering af fortrolige mails.

Håndtering af mail	Antal
Bruger særlige sikkerhedsprodukter:	
Firewall	1
Flere forskellige antivirusprogrammer	1
Har installeret et sikkerhedsprogram	1
Indtaster data i Norton internet security	1
Mc Fee sikkerheds programmer	1
Virus program	1
Virusskanner, adgangskoder	1
Gemning et særligt sted:	
Arkiverer dem i en låst mappe - og sletter den derefter helt.	1
Gemmer dem i en mappe, hvor til kun jeg har adgangskoden	1
Gemmer dem i en special side	1
Gemmer dem særligt sted	1
Gemmer den et sted	1
Gemmes/Printes ud	1
Jeg har dem på diskette	1
Kan ikke gøre andet end at placere dem et sted hvor jeg mener at andre ikke umiddelbart vil kunne finde dem på min pc’er.	1
Mail krypteres under transmission:	
Benytter en mailservice der sørger for kraftig kryptering af mails	1
Bruger en krypteret line eller et digitalsignatur	1
Digital signatur. Bank - Krypteret.	1
Enten ved kryptering eller også gennem websidens kryptering feks. netbank	1

Fortsættes på næste side

Håndtering af mail	Antal
Håber at afsenderen bruger min digitale signatur til kryptering	1
Mails ligger kun på serveren og kan kun læses via VPN forbindelse.	1
Med digital signatur	2
PGP	1
Sender som “sikker e-post”	1
Sendes som sikker mail krypteret	1
Brug sikker forbindelse	6
Sikker forbindelse, krypteret	2
Via vpn	1
Mail gemmes på krypteret form:	
De er krypterede	1
De kan krypteres	1
Flytter mailen eller krypterer den	1
Jeg gemmer fortrolig information på et krypterede drev	1
Kryptering	4
Krypteret, og i password sikret mappe	1
Ved at anvende en kryptonøgle	1
Mail slettes:	
Fjerner dem hurtigst mulig fra min mailboks.	2
Fjerner det fra min pc ved at videresende eller printe ud	1
Følsomme mails bliver så vidt muligt slettet efter behov/brug	1
Jeg skanner altid mails. Når jeg har fået den printer jeg den ud, bagefter sletter jeg mailen	1
Jeg sletter dem når jeg har læst dem og så er de altid krypteret	1
Jeg sletter dem og sletter dem fra “Slettet post”	1
Kopier til ekstern disk og sletter mailen	3
Kopierer dem omgående og fjerner dem fra computeren	1
Sikkerhedskopierer og sletter oprindelige dokumenter	2
Gemmer dem på en USB Pen og sletter dem derefter	1
Sletter (dem)	9
Sletter dem hurtigst muligt	2
Dobbeltsletter mailen	2
Sletter dem efter at have printet dem ud (e.l.)	9
Sletter dem eller flytter dem væk fra indbakken	1
Sletter dem når de er læst/behandlet	2
Sletter dem når de er registreret	1
Sletter dem når jeg har anvendt dem	2
Sletter dem når jeg har læst dem	12

Fortsættes på næste side

Håndtering af mail	Antal
Sletter dem når jeg har læst dem, eller har printet dem	3
Sletter dem, når jeg har læst dem. I enkelte tilfælde gemmer jeg filen på backup først, hvis filen er meget lang. Eller jeg sletter de følsomme dele af en mail eks. CPR nr.	1
Sletter dem efter at have læst dem, eller lægger dem i e-boks	1
Sletter efter læsning og gemmer sommetider på et sikkert sted	1
Sletter efter læsning/gemmer krypteret.	1
Sletter mail efter modtagelse og/eller gemmer på ekstern disk	1
Sletter mail, når oplysinger er registreret for det, jeg har brug for.	1
Stoler på computerens adgangskontrol:	
Adgangskode	1
Adgangskode til at åbne computer	1
Bruger adgangskode	1
Bruger adgangskode på PC	1
Code på min pc	1
Computeradgang kun med password	1
Der er ikke andre der har adgang til min computer	1
Der er normalt ikke adgang til min computer med mindre andre har skaffet sig adgang.	1
Det er en PC jeg har. Det betyder Personlig Computer. Der er ikke andre der nogensinde bruger den!	1
Gemmer dem på min PC, som er beskyttet af firewall, password og slukket når den ikke bruges	1
Her i huset er det kun mig der åbner computeren - og læser indkomne mails	1
Jeg har adgangskode på min bærbare pc	1
Kun indviede har adgang til computeren	1
Det er jo ikke de andres pc...men min	1
Det er kun mig der har adgangskode til min mailboks	1
Det er kun min kone og jeg selv, der har adgang til computeren.	1
Ved det kun er mig der har adgang	1
Ved at det kun er min kone og nærmeste familie der har adgang til computeren. At der er en fiwall så udvekommen fra internettet ikke har adgang til min pc, dog er jeg ikke helt sikker på om hullet er lukket - jeg bruger Microsoft.	1
Holder folk væk fra min PC	1
I never disclose my pass word	1
Password	1
Password på pc'en	1

Fortsættes på næste side

Håndtering af mail	Antal
PC har adgangskode - ellers udskrives og slettes dokumenter	1
Gør ikke noget:	
Det gør jeg ikke. Bruger virus program og fire wall.	1
Det har jeg ikke overvejet.	1
Det kan jeg ikke, da jeg modtager mailen	1
Det sikrer jeg mig ikke	3
Ens cpr nummer bruges efterhånden “offentligt”	1
Folder hænderne og håber	1
Gør ikke noget aktivt	1
Gør ingenting	1
Gør jeg nok ikke	1
Hjemme gøres intet. Arbejdet via sikker mail.	1
Holder dem for mig selv eller sletter.	1
Ikke sikker nok	1
Ikke sikret, jeg er den eneste der bruger pc’en.	1
Ingen særlige foranstaltninger	1
Jeg foretager mig intet aktivt for at undgå det	1
Jeg kan ikke være 100% sikker, kun håbe på at de ikke kommer til andres kendskab.	1
Jeg skriver ikke fortrolige mails.	1
Diverse svar, inkl. uklare strategier:	
Afsenderen hvis det er en bank, vil ikke sende via mail hvis det var usikker	1
Benytter webmail	1
Bruger koder, hvor det kan lade sig gøre	1
Datasikkerhed om brugen af mails	1
De er digitalt signerede.	1
De ligger i min pc	1
Det står så man kan gemme det	1
Jeg giver dem kun til mennesker jeg er fortrolig med	1
Jeg har min private konto på mit operativsystem	1
Kodeord	1
Med de eksempler der var nævnt, kan man jo kun svare ja. Da mail ikke er en sikker kanal (og derfor kan udveksling af password godt foregå sikkert), vælger jeg, hvilke typer af fortrolige oplysninger jeg sender. Arbejdsmæssigt er alt krypteret.	1

Fortsættes på næste side

Håndtering af mail	Antal
Net bank er krypteret	1
Stoler på min opkobling	1
Svarer kun på fortrolig dokumenter	1
Sørger for at IT-samarbejdspartnere opretholder datasikkerhed og kryptering. Arbejder kun via deres "produkter"/tjenester	1
Påpasselighed	1
Sender dem ikke videre	1
Sikrer min computer mod angreb	1
Ved at bruge https og sikre hjemmesider	1
Ved hjælp af Safesurf	1
"Ved ikke" (og lignende svar):	
Det ved jeg ikke (e.l.)	13
Ingen kommentarer	1
Spørgsmål ikke forstået?	1
Tja ??	1
Øhh	2
-	1
?	7

Litteratur

[1] Rachna Dhamija, J.D. Tygar, and Marti Hearst. Why phishing works. In Rebecca Grinter et al., editors, *CHI2006: Proceedings of SIGCHI Conference on Human Factors in Computing Systems, Montréal, Canada*, pages 581–590. ACM, April 2006.

[2] Lisa Gjedde and Robin Sharp. Questions as pathways to learning – implicit learning in a simulated environment. In D.G. Kinshuk, editor, *Proceedings of CELDA 2009: Cognition and Exploratory Learning in a Digital Age, Rome*, pages 516–519. IADIS, November 2009.

[3] Lisa Gjedde, Robin Sharp, Preben Andersen, and Helle Meldgaard. Safeguarding the user – developing a multimodal design for surveying and raising internet safety and security awareness. In A. Mendez-Vilas, editor, *Research, Reflections and Innovations in Integrating ICT in Education*, volume 1, pages 568–571, 2009.

[4] Nick Pidgeon, Roger Kasperson, and Paul Slovic, editors. *The Social Amplification of Risk*. Cambridge University Press, Cambridge, July 2003. ISBN 0-521-52044-4.

[5] Ronald W. Rogers. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In John Cacioppo and Richard Petty, editors, *Social Psychophysiology*, pages 153–176. Guilford Press, New York, 1983.

[6] Robin Sharp and Lisa Gjedde. Improving on tacit knowledge through a media-rich survey. In *Proceedings of the World Conference on e-Learning in Corporate, Government and Higher Education, Vancouver*, pages 1962–1965. AACE, 2009.