

@visen

netsikker nu!

Maj 2006

Test dig selv

Hvor sikker er du på nettet?
Tag testen på bagsiden og se,
hvor højt du scorer, når du går
i krig med spim, spam og
passwords.

16



Hvorfor styrer kvinder ikke it-sikkerhed?

Idéen om, at mænd er fra Mars, og kvinder er fra Venus, er ikke helt i skoven. I hvert fald ikke, når det kommer til it-sikkerhed. Men er det virkelig, fordi kvinderne ikke har styr på det med sikkerheden?

9

Svindlere på fisketur

Phishing bliver mere og mere udbredt. Med et arsenal af listige tricks lokker svindlere personlige oplysninger ud af folk, som helt uvidende om situationen gladeligt åbner for penge-skabet.

10

It-sikkerhed på arbejdspladsen

14

Sagde du virus?

6



Bliv online med dine børn

De spiller, chatter eller finder oplysninger på nettet hurtigere, end vi når at hive leksikonet ud af reolen.

De møder nye venner og henter ny musik.

Som forælder kan det være svært at følge med zappergenerationen. Men helt umuligt er det ikke. 3

SPAM

7

Ældre hjælper ældre med it

Over hele landet skyder datastuer op, hvor alle over 60 år kan få hjælp til at gøre internettet til en naturlig del af hverdagen.

12



Introduktion



Bliv netsikker nu!

Undersøgelser viser, at antallet af internetbrugere stiger markant, men når det kommer til viden om it-sikkerhed, står det mindre godt til. Konsekvenserne af manglende viden om it-sikkerhed kan være fatale – ikke bare for den enkelte, men også for virksomheder, hvor medarbejdere, uden at vide det, risikerer at invitere kriminelle ind.

Derfor har Videnskabsministeriet i samarbejde med en række partnere initieret kampagnen netsikker nu!, som sætter fokus på it-sikkerhed og giver gode råd til, hvordan du kan blive mere sikker på nettet.

Benyt chancen for at opdatere din viden på området. Bare for en sikkerheds skyld ...

www.netsikkernu.dk

Indhold

Sikkerhed er et af nøgleordene på Habbo Hotel - online community	3
Bliv online med dine børn	3
Konkurrenter og kammerater	4
Mobningens virtuelle ansigt	4
Børn giver råd om god webetik	5
STOP børneporno	5
Sagde du virus?	6
Bevar dine data for dig selv, når du bruger en computer	6
Spam - gode råd og fif	7
Spar tid med Digital Signatur	7
It-sikkerhed blandt heltinderne	8
Adam og Eva på mobilen	8
Lad kvinderne klare it-sikkerheden	9
Spring bare ud i det kvinder	9
Phishing – svindlere på fisketur	10
Kast ikke håndklædet i ringen!	11
Brug sund fornuft når du handler på nettet	11
Internettet er mulighedernes land	12
En hjælp i hverdagen	12
Gode råd om sikkerhed fra branchen	13
Spim	13
”Sikkerhedsbevidst bruger” - hvad er det?	14
Følg sikkerhedspolitikken	14
Beskyt dit privatliv på nettet	15
Ordlister	15
Test dig selv	16

Sikkerhed er et af nøgleordene på Habbo Hotel - online community

I dag mødes unge på nettet. Overalt blomstrer communities op, hvor unge spiller, diskuterer, danner venskaber og danser virtuelt. Et af mødestederne er det verdensomspændende ungdomscommunity Habbo Hotel.

Af Lars Kristiansen, Habbo Hotel

Siden opstarten af Habbo Hotel i år 2000 er næsten 50 millioner Habboer oprettet på verdensplan. På nuværende tidspunkt er Habbo Hotel repræsenteret i 18 lande og har samlet set omkring 6 millioner unikke besøgende om måneden. Med så mange besøgende er sikkerheden et hot emne.

Tilpasset sikkerhed

Man kan gøre meget teknisk, men langt hen ad vejen handler det også om at opføre sig til respekt for hinanden og god etik. Habbo Hotel opfordrer brugere til at følge ”Habbo-stilen”, regler baseret på respekt, standarder for internet-sikkerhed og god moral.

De tre overordnede hovedområder, der danner Habbo Hotels ”sikkerhedspakke” er moderation, teknologi og uddannelse. Tre leveregler, som konstant og konsekvent eksekveres

for at holde det eftertragtede community frit for misbrug som f.eks. chikane, bandeord og racistiske og pædofile handlinger. Men hvad betyder det?

Moderation

Alle Habbo Hotellerne over hele verden modereres 24 timer i døgnet af voksne, som selskabet Sulake, der er ansvarlig for Habbo Hotel, uddanner. De kan ved hjælp af et værktøj hjælpe, guide og smide uartige Habboer ud. Moderatorer fungerer som den aktive hjælpeforanstaltning på Habbo.

Teknologi

Alle samtaler og skrevne ord på Habbo bliver modereret af et teknisk filter ved navn ”Bobba-filteret”. Filteret erstatter bandeord, e-mail-adresser, telefonnumre eller andre personlige oplysninger ud med ordet ”Bobba”.

Hjælper ”Bobba” ikke, tager Habbo Hotel skrappe teknologi i brug og udviser brugere ved at spærre for deres adgang til Habbo Hotel. Alle, som opfører sig på grænsen af dansk lovgivning, bliver indrapporteret til myndighederne omgående.

Uddannelse

En af de mest effektive måder at effektivisere sikkerhedskravene på er uddannelse af Habboer til at bruge nettet på en sikker og ansvarlig måde. Alle hoteller i Habbo-regi har en dybdegående instruktion til Habboen, som omhandler sikkerhedstips, og som samtidig giver dem en indikation af, hvor højt Habbo Hotel prioriterer dette. Sikkerhed bliver desuden kommunikeret ud til Habboerne via vores ugentlige nyhedsbrev, sikkerhedscentraler (brugernes egne), konkurrencer om sikkerhed og meget mere.





Bliv online med dine børn



Har computeren ændret dit familieleven? Er du online sammen med din familie? Og ved du, hvad dine børn oplever på nettet? Medierådet for Børn og Unge anbefaler, at du bliver 'FIT' til at gå på nettet, dvs. sørger for, at du er opdateret med både firewall og it-kompetencer.

Af Brit Sung Kyung Kim Bech,
Medierådet for Børn og Unge

Måske er det din søn på 11 år, som sørger for familiens online-indkøb af såvel cd'er, bøger, tøj eller tog- og flybilletter, fordi du ved, at han er dygtig ved en computer og kender til nettet. I dag tilhører vi voksne en "offline-generation", og det kan nemt give en oplevelse af at blive overhalet af vores børn. Oftest er børn hurtigere og ved mere om internettet end forældrene. I skolerne vokser børn op med computer og mobil, som for de flestes vedkommende indgår som en selvfølge i dagligdagen. Derfor er det vigtigt, at forældre taler med deres børn om børnenes oplevelser

på nettet, og at forældre tør bede om en forklaring på udtryk, som de ikke selv kender til som f.eks. chat, blokering på messenger eller downloads. Jo mere du selv kender til nettet, jo bedre kan du sikre, at dit barn får gode oplevelser med mediet, og du kan være med til at lære dine børn nogle gode vaner fra starten.

Nettets muligheder og risici

Nye medier bringer nye muligheder med sig, og samtidig er der nye risici i forhold til børn, som ikke forholder sig kritiske, men er nysgerrige og udforskende i deres brug af nettet og mobilen. Derfor arbejder Medierådet for Børn og Unge som videnscenter for børns brug af internet, film og computerspil med at informere forældre om børns netkultur. Formålet er at klæde forældre på til at kunne tage en god snak med børnene, hvilket er udgangspunktet for den bedste børnebeskyttelse, nemlig uddannelse og gode vaner fra starten.

Nye medier vi ikke er vokset op med

Vi taler i dag om, at der er opstået en generationskløft mellem børn og forældre i forhold til nye medier og de ændringer, som følger med. Det er derfor vigtigt at huske på, at it-kompetencer også handler om at kunne sortere i informationer samt at have et godt sæt livsværdier, og her er forældrene stadig de væsentligste rollemodeller.

Fra tv-dinner til online-dinner

I 60'erne samledes hele familien omkring "hjemmets plakatøjle", tv'et. I dette århundrede står tv'et nu side om side med hjemme-computeren, hvis det da ikke er blevet skiftet ud med en storskærm og computer med tv-modtagerkort. De danske forældre er blevet flittige til at benytte nettet, og børnene følger godt med.

I Danmark havde 84 % af alle familier i 2005 en computer i hjemmet. Heraf havde 98 % af alle par med børn adgang til computer i hjemmet, og i 2004 havde 20 % af børn mellem 7 og 15 år internetadgang fra eget værelse. Tidligere kunne forældre nemmere beskytte deres børn mod indhold, som var uegnet for børn, fordi hele familien sad sammen foran tv'et. Nu sidder hvert 5. barn alene eller sammen med venner og veninder på værelset og surfer på nettet eller spiller computerspil og chatter.

Men hvordan ser det ud med forældrene, og er der forskel på, hvordan mor og far bruger nettet? Ifølge Kulturministeriets undersøgelse, Danskernes Kultur- og Fritidsaktiviteter 2004, benyttede 43 % af de voksne over 15 år internettet hver dag i 2004. 49 % af mændene bruger internet stort set dagligt mod 36 % af kvinderne. Undersøgelserne viser også, at kvinder og mænd på nogle områder benytter nettet forskelligt. Flere

kvinder end mænd benytter internettet til kurser og uddannelse samt informationssøgning om helbred og sundhed. Derimod benytter flere mænd end kvinder internettet til at spille online-spil og til at købe varer eller tjenester.

Tallene viser, at familien Danmark er gået online. Udover indkøb, netbank og uddannelse foregår kommunikation med skoler også online. Mange skoler har nemlig, udover computerrum og it-undervisning, også deres egen hjemmeside med et lukket forum, hvor forældre og lærere kan modtage og sende beskeder via en virtuel "opslagstavle".

Fælles europæisk viden og vejledning

Internettets udbredelse og nye teknologiers fremkomst har været på dagsordenen siden starten af 90'erne. Og i Europa-Kommissionen blev grundstenen lagt til en EU Safer Internet Action Plan, som er et større koordineret projektsamarbejde over landegrænser for at sikre børn og unge på nettet. Dette europæiske projekt er en mærkesag for Europa-Kommissionen, og 27. april 2006 åbnede Europe Direct, et kontor for EU-borgere, som her kan modtage direkte vejledning om specifikke spørgsmål vedrørende nettet og mobil.

En årlig Sikker Internet Dag

Med fokus på såvel potentialer som risici ved medierne koordineres en

årlig fælles europæisk kampagne-dag, Sikker Internet Dag. Dagen koordineres af Insafe under EU Safer Internet Action Plan, hvor i alt 23 nationale videnscentre fordelt på 21 lande er med til at koordinere de forskellige landes mange events for børn og forældre. I Danmark afholdes dagen af Medierådet for Børn og Unge, som har fungeret som videnscenter i de seneste 2 år. Videnscentret er åbent for henvendelser fra alle, som har oplevet situationer, hvor der har været brug for et godt råd, og samtidig har vi aktuel viden om, hvad der sker på området i Danmark og Europa.

Børneambassadørerne og netsikker nu!

2. maj 2006 på netsikker nu!-dagen præsenterer Medierådet for Børn og Unge et inspirationsmateriale på dvd om webetik. Børneambassadørernes arbejdsindsats har resulteret i en film om webetik, og på baggrund af deres egne erfaringer kommer de med 10 gode råd om webetik.

Fakta:

Få mere information på:
www.medieraadet.dk
www.saferinternet.org

Europe Direct kan kontaktes via den gratis telefonlinie på 00 800 678 910 11

Konkurrenter og kammerater

Selvom man er konkurrenter, er der mange områder, man kan være fælles om. Et af dem er kampen mod virus, hackere, orme og spam. Ni internetudbydere eller ISP'er, som de kaldes, er gået sammen for at forbedre sikkerheden på internettet.

Af Stina Christiansen, TDC



Har du været uheldig at få en trojansk hest på din computer? Så er du ikke den eneste. Flere har oplevet, at en hacker har overtaget kontrollen med det resultat, at computeren f.eks. står og spytter en masse e-mails ud. Det er hverken i din eller internetudbydernes interesse.

Når en ny trussel viser sig i de danske internetskaber, mødes de ni udbydere derfor og bliver enige om, hvad der kan gøres for, at du



som bruger bliver mindst muligt berørt af problemet. Indtil videre har samarbejdet ført til slagkraftige spamfiltre, der har reduceret mængden af spam i de danske indbakker markant. Samtidig har internetudbydere forpligtiget sig til at gøre en stor indsats for at informere deres brugere og kunder om sikkerhed. Og et af de seneste tiltag, ISP Sikkerhedsforummet står bag, er børnepornofilteret, som dækker 98 % af alle danske internetbrugere.



”Der er større sandsynlighed for at få stoppet en stor virus, spam eller et ormeangreb, hvis alle internetudbydere trækker i de samme håndtag eller sætter de samme skodder op på internetforbindelserne i Danmark”, udtaler Per Rasmussen, Online direktør i TDC Privat og formand for ISP Sikkerhedsforum.

Fakta:

Kamp mod spam

ISP (Internet Service Provider) Sikkerhedsforum blev dannet i maj 2004. Formålet med samarbejdet er at tage kampen op mod virus, spam, orme og andet, der truer it-sikkerheden. Væsentlige indsatsområder er blandt andre: Spam, DOS-, hacker-, orme- og virusangreb, samt filtrering af børnepornografi.

Hvor der bl.a. fokuseres på:

- Iværksættelse af e-mail-scanning
- Nedlukning af specifikke porte
- Nedlukning af enkeltbrugere, der optræder som virus-spredere eller spammere
- Kommunikationsplan eller -beredskab for information til offentligheden

Mobningens virtuelle ansigt

I dag er mobning ikke kun noget, der foregår i klasselokalet og i skolegården. Den har fundet en ny og aggressiv form på internettet – specielt blandt børn og unge. Dialog og åbenhed kan være med til at ændre tendensen.

Af Kirsten Pantón, Microsoft

Julie og Malene er slyngveninder og deler alt fra yndlingsbluse til password på Messenger. En dag bliver de uvenner over en dreng fra parallellklassen, og et par uger senere opdager Malene, at Julie har sendt ubehagelige beskeder rundt i Malenes navn ved at logge på med hendes Messenger-password. Og vennerne er begyndt at lukke hende ude fra fælles samtaler på både Messenger og mobil. Eksemplet er opdigtet, men desværre ganske typisk for, hvordan et stigende antal børn og unge i dag oplever en ny form for virtuel mobning. En type

mobning, der kan være endnu mere barsk end traditionel mobning. Der er mange eksempler på, at den udbredte virtuelle mobning kan være mere avanceret og ondskabsfuld. Computeren eller mobilen er med til at skabe en distance, så man tør være langt mere grov, end hvis man står ansigt til ansigt med offeret.

Snak uden filter

Den virtuelle mobning, som flourer f.eks. på sms, i chatrum og på e-mail, er ligesom traditionel mobning meget svær at komme til livs. Men dialog med og mellem børn og unge kan være et vigtigt skridt på vejen. Derfor er Medierådet for Børn og Unge, Red Barnet, Det Kriminalpræventive Råd, UNI-C og Microsoft gået sammen om at gentage sidste års netsikker nu!-kampagnesucces. Dengang lod 153 medarbejdere fra Microsoft arbejde være arbejde i en dag og drog i stedet ud for at undervise og tale med børn og unge om sikker adfærd på pc og på nettet. I fællesskab har de fem organisationer nu udarbejdet et nyt præsentations- og undervisningsmateriale primært omkring virtuel mobning, som skal



få de unge i tale, når skolerne 2., 3. og 4. maj igen får besøg af en eller to af de godt 250 utraditionelle gæstelærere fra Microsoft.

Engagement og åbenhed

En af dem, der skal ud i de danske skoleklasser og få åbnet op for en åbenhjertig snak om mobning, er Jesper Riedel, der til daglig er

løsningsspecialist hos Microsoft. Han var også af sted sidste år og glæder sig til en omgang til:

”Det var faktisk ret skægt! Jeg mødte en hel masse engagerede og begejstrede børn og unge, der var aktive og interesserede. Mange havde allerede både gode og dårlige erfaringer, som de gerne ville dele

med andre, når det kom til stykket. Jeg oplevede klart, at børnene fik noget med sig hjem, og at formen med spørgsmål og dialog fungerede godt. Og for mig var det en fantastisk mulighed for dialog med en helt anden gruppe end de beslutningstagere i det offentlige, som jeg normalt har med at gøre”, fortæller Jesper Riedel.

Børn giver råd om god webetik

Vi voksne er jo eksperterne – i hvert fald når det gælder meget andet end lige netop børns brug af internettet og mobilen. Børn og unge har om nogen fingeren på pulsen, når det drejer sig om chat- og mobilkulturen. Det ses tydeligt i de ti klare råd om god webetik, som Danmarks første børneambassadører i webetik præsenterer 2. maj 2006 i forbindelse med den årlige netsikker nu! dag.

Af Lotte Drehn, Medierådet for Børn og Unge

Zappergenerationen, tomfingergenerationen eller online-generationen – kært barn har mange navne. Fælles for betegnelserne er en hentydning til, at børn og unge i dag vokser op med, at verden kan styres med få klik på tasterne eller musen. Men fælles for begreberne er også, at de er skabt af os voksne, der forudsiger de værste tænkelige uheld, når tommelfingrene suser hen over knapperne.

Men mange børn har heldigvis helt styr på det. De ved godt, at lige så vel som man skal have sikkerhedssele på og ikke køre over for rødt i den virkelige verden, så gælder der også en række regler, hvis man vil undgå uheld i den virtuelle verden. Det viser rådene fra Danmarks første Sikker Internet Ambassadører, 6.e. fra Maglegårdskolen i Gentofte, som blev kåret i forbindelse med den internationale Sikker Internet Dag 2006. Dagen blev i Danmark afholdt af Medierådet for Børn og Unge i februar i Filmhuset i København.

”Du må aldrig give navn og adresse til én, du ikke kender” og ”Tænk dig om, inden du sender en e-mail eller sms, for når modtageren har set den, så kan den ikke slettes”. Sådan lyder to af de ti gode råd, som Sikker Internet Ambassadørerne fik til opgave at udarbejde.

”Husk at du ikke ved, om den, du chatter med, virkelig er den, han eller hun giver sig ud for”, lyder et tredje råd. Børn og unge er meget opmærksomme på, at internettet er et oplagt sted at lege med - eller sløre sin identitet.

Faktum er, at godt 80 % af alle unge har prøvet at lege med deres identitet på nettet, hvilket der slet ikke

er noget galt i. For det første er børn og unges leg med identitet en helt naturlig del af deres udvikling, og for det andet er det jo netop noget af det, der er rigtig sjovt, når man f.eks. sidder og chatter.

Problemet opstår dog, når intentionerne bag sløring af identitet kan skade modtageren eller afsenderen selv, som når f.eks. unge piger udgiver sig for at være voksne. Billeder virker særligt tiltrækkende på os, hvis de associerer til emner som sex eller vold. På det punkt er børn ikke anderledes end voksne. Udfordrende billeder skaber opmærksomhed, og det er jo en forudsætning for f.eks. at få kontakt og nye venner på en chatside. Men billedets signaler stemmer jo ikke altid overens med afsenderens intentioner.

For at understrege denne pointe oprettede jeg en midlertidig, falsk profil på chatsiden Arto i forbindelse med en foredragsrække om webetik for 7. klasser i Københavnsområdet. På profilen var der et billede af en meget letpåkædet ung dame og en tilhørende tekst med ordene: ”Hej, jeg er en sød ung pige, som gerne vil have nogle nye venner, fordi jeg er ved at lave en bogklub. Hvis du er interesseret i at være medlem, skal du bare skrive til mig”. Efter at eleverne havde set på profilen i de 3-5 sekunder, vi i gennemsnit bruger på en webside, spurgte jeg eleverne, hvad og hvem de lige havde set. Svarene pegede som ventet i langt højere grad på, at det var en fræk babe, der var ude på ballade, de lige havde set, frem for en uskyldig studerende med interesse for bøger. At lægge billeder på nettet, kræver derfor, som ambassadørerne understreger, grundige overvejelser.



Men selv om de gode råd fra Sikker Internet Ambassadørerne viser, at det ikke er så galt fat med de unges forståelse for internettet, som vi voksne kan frygte, så viser eksemplerne om mobning og billeder med uheldige signaler jo deres eget kedelige sprog. De viser, at forståelse og adfærd ikke altid hænger sammen, og at der er brug

for vedvarende opmærksomhed på og debat om god webetik. Medierådet for Børn og Unge lancerer derfor 2. maj i samarbejde med Danmarks undervisningsportal EMU og IT- og Telestyrelsen en webside på EMU med undervisningsmateriale om webetik og relaterede emner. Materialet bliver offentliggjort løbende frem til november 2006 på www.emu.dk

Fakta:

De 10 gode råd

1. Du må aldrig give navn og adresse til én, du ikke kender
2. Du må gerne have et kælenavn eller udgive dig for noget andet, bare hensigten er god
3. Husk at du ikke ved, om den, du chatter med, i virkeligheden er den, han eller hun giver sig ud for
4. Lad være med at sige noget, du ikke mener, for det kan gå galt, hvis den, du siger det til, ikke forstår det
5. Lad være med at komme med racistiske udsagn, for det er faktisk ulovligt
6. Lad være med at drille med udseende, for det kan såre rigtig meget
7. Lad være med at mobbe og diskriminere andre - heller ikke for sjov
8. Tænk dig godt om, inden du sender en e-mail eller sms, for når modtageren har set den, kan den ikke slettes
9. Lad være med at true andre for sjov, for det er meget svært at gennemskue
10. Du skal lade være med at holde andre udenfor, hvis ikke du har en rigtig god grund

STOP børneporno

De ni store internetudbydere i Danmark har aktiveret et landsdækkende børnepornofilter, som skal hjælpe med til at bekæmpe børneporno på internettet.

Af Stina Christiansen, TDC

Børneporno er på flere måder en rigtig ubehagelig ting. Internetudbydere i Danmark vil gerne sikre deres brugere mod utilsigtet at komme ind på en side med børnepornografisk materiale.

98 % af den danske befolkning er derfor dækket af et filter, hvor sider med børneporno kan blive sorteret fra.

Det virker ved at blokere for adgangen til internetadresser, der indeholder ulovligt børnepornografisk materiale. I stedet for den blokerede side ser man nu blot en stopside, der forklarer, hvorfor man ikke kan se indholdet på siden. Det er udviklet i samarbejde med Rigspolitiet og Red Barnet.

Rigspolitiet udarbejder listen over de blokerede hjemmesider og sender dem til din internetudbyder. Rigspolitiet vurderer hjemmesiderne og indholdet i samarbejde med Red Barnet, der på internationalt plan identificerer og indsamler oplysninger om, hvor der findes børneporno på nettet.

Udover at beskytte brugere mod ved et uheld at se det børnepornografiske materiale, vil udbydere også gerne vanskeliggøre adgangen og reducere antallet af besøgende på siderne med de ulovlige materialer. Din internetudbyder registrerer ikke personlige oplysninger på dem, der bliver mødt af stopside, så filteret bliver ikke brugt til personforfølgelse.

Udbuddet af børnepornografisk materiale på nettet har været stigende, og det samme har trafikken på de ulovlige sider.

Sagde du virus?

Opfører din maskine sig mærkeligt? Som de fleste andre vil du formodentlig kategorisere problemet som "virus". Men der kan være helt andre ting på spil. Orme, trojanske heste og andre ubehagelige arter lurder nemlig derude. Her kan du læse en beskrivelse af de overordnede kendetegn ved de mest udbredte typer af skadelig kode.

Af Erik Jon Sloth, TDC



bestemt e-mail-adresse. Så sørg altid for at opdatere din computer med seneste versioner af dine sikkerhedsprogrammer.

Orm

En orm minder om en virus, men i modsætning til virussen har orme ikke brug for andre

virksomheds kommunikation, fordi mailserverne overbelastes.

Igen er det vigtigt, at du har de seneste sikkerhedsopdateringer på din computer. Ellers er der risiko for, at du kan blive angrebet, hvis du surfer forbi en hjemmeside, der er inficeret af en orm.

Trojanske heste

En trojansk hest er hverken en virus eller en orm, men blot en egenskab ved dem begge.

Når en orm installerer en trojansk hest på offerets computer, bliver der skabt en "bagdør", som kan udnyttes til at styre computeren udefra. Den trojanske hest kan nu enten sende en besked ud i verden, så en ondsindet person kan få at vide, at computeren er klar til at blive overtaget, eller den kan blot sætte sig til at vente og lytte. Enhver med den trojanske hests styreprogram vil herefter kunne få fuldstændig kontrol over computeren, dvs. starte programmer på den og overvåge, hvad der tastes på tastaturet.

En typisk hoax indeholder en skrækhistorie om en ny virus, som vil ødelægge vitale dele af din computer, ofte både data og harddisk og skærm. Afsenderen påstår også, at advarslen blev udsendt "for en uge siden" fra et stort firma som f.eks. IBM eller Microsoft.

En udbredt udnyttelse af en inficeret pc er at gøre den til en del af et netværk af computere, som kriminelle har kontrol over.

Et særligt kendetegn er, at der aldrig er et link til en artikel om den farlige virus i e-mailen, og du kan heller ikke finde noget hos de store antivirusfirmaer om virussen. Beskeden opfordrer altid til, at du hurtigst muligt sender den videre til alle, du kender.

Fakta:

Virusser eller vira?

Hvad hedder det så, når der er mere end én virus?

Ifølge Dansk Sprognævn er både "virus", "virusser" og "vira" korrekte flertalsformer af "virus" på dansk. Da virus oprindeligt er et masse-ord, som ikke kan bøjes på latin (virus er i forvejen flertal), er det frit, om du vil bruge det kunstige "vira" eller holde dig til det mere danskklidende "virusser".

Se mere hos www.dsn.dk

De mere godartede af slagsen har blot samme formål som et kædebrev. Det vil sige, at de bare spilder folks tid og belaster mailserverne med unødvendige e-mails.

Virus

En virus hedder en virus, fordi den minder om en forkølelse. Den er nødt til at have en krop at leve i, f.eks. et tekstbehandlingsprogram, et e-mail-program eller et Word-dokument, og den har egenskaber, der gør den i stand til at sprede sig selv.

Når du starter det inficerede program eller åbner dokumentet, virker alt normalt, men bagved er virussen også blevet startet. Ofte inficerer virussen andre programmer eller dokumenter, når du tænder computeren. På den måde bliver den spredt til andre computere, hvis du sender programmer eller dokumenter til andre eller har mapper på din computer, som andre har adgang til.

Virussen nøjes ofte ikke med at sprede sig. Den kan slette filer på din computer, f.eks. på en bestemt dato, eller den kan sende tilfældige dokumenter fra din harddisk til en

programmer for at blive spredt. De inficerer derfor heller ikke programmer på din computer, men lever i det skjulte og sørger ofte for at blive aktiveret som en del af opstarten, når du tænder computeren, eller når du starter bestemte programmer.

Hvis virussen har inficeret et program, er der i praksis ingen grænser for, hvad den kan, når først den kører.

Når ormen har inficeret en maskine, spreder den sig selv ved at udsende e-mails, der indeholder kopier af ormen, ofte til alle i dit adressekartotek eller ved at benytte din internetforbindelse til at søge efter andre maskiner med huller i sikkerheden. De mest aggressive orme spreder sig i så store mængder, at de får dele af internettet til at køre langsommere eller helt lammer en

En udbredt udnyttelse af en inficeret pc er at gøre den til en del af et netværk af computere, som kriminelle har kontrol over. Det bliver kaldt et robot-net eller bare botnet. Uden du har den mindste anelse, kan din computer lige nu stå og sende flere tusinde e-mails med tilbud om billig Viagra. Eller den kan være i gang med at angribe et stort firmas hjemmeside, fordi de ikke vil betale en bagmand penge.

Kombinationer

Der er intet til hinder for, at en orm kan indeholde både en virus, som inficerer dine programmer og sender orm ud i verden, og en trojansk hest, som åbner for styring udefra. Kun virusprogrammørernes ubarmhjertige kreativitet sætter grænsen.

Hoax

En hoax er en falsk virusadvarsel, som distribueres via e-mail.

Bevar dine data for dig selv, når du bruger en computer

Selv en husdør i massivt egetræ er et dårligt forsvar mod indbrudstyre, hvis låsen er lavet af billigt blik. På samme måde skal de passwords, du benytter for at holde uvedkommende ude, både på computeren og på internettet, være i en fornuftig kvalitet. Og du skal selvfølgelig holde dem hemmelige.

Du kan sikre kvaliteten ved at følge disse råd:

1. Vælg et password med mindst otte tegn
2. Brug både små og store bogstaver
3. Brug et eller flere tal

4. Brug eventuelt specialtegn som #, !, ? eller *
5. Brug forskellige passwords til forskellige internetsteder

Sådan husker du dine passwords

"Jeg går og hedder Frede, hvad hedder du?" er lettere at huske end "JgohFhhd?". Hvis du tilføjer et tal i huskesætningen, har du et sikkert password, der ikke er til at gætte: "JgohFhhd?11". Det er ganske enkelt: Find en sang og et tilfældigt nummer.

Spam

- gode råd og fif

Får du uønskede e-mails? Se hvad du kan gøre for at mindske problemet.

Af Stina Christiansen, TDC

Spam er uønskede e-mails, som du modtager uden at have bedt om det. Ofte har afsenderen fået fat i din e-mail-adresse ved at købe en million e-mail-adresser, hvor din e-mail-adresse er med i pakken. Resultatet kan være tilbud på både engelsk, tysk, fransk, japansk osv. og tilbud på ydelser, som kun gælder i Nebraska.

Hvad gør man ved spam e-mails? Der er to muligheder, når du modtager en spam e-mail. Enten kan du slette den med det samme, eller du kan forsøge at klage over den.

At sende spam irriterer ikke bare modtagerne. Det er også ulovligt i Danmark.

Ifølge Markedføringslovens § 6a er det ikke lovligt at sende reklamer ud til nogen, der ikke har bedt om det.

Modtager du uopfordret en reklame-e-mail, kan du sende den videre til Forbrugerstyrelsen.

Men med sund fornuft, omtanke og et par forholdsregler kan du undgå, at problemerne kommer så vidt.

Alternativ adresse

Hvis du deltager i konkurrencer, undersøgelser eller blot opgiver din e-mail-adresse for at få mere information omkring et eller andet, skal du ikke opgive din primære

e-mail-adresse. Opret i stedet for en alternativ e-mail-adresse.

Opret f.eks. bo-konkurrence@mail.dk. Den e-mail-adresse anvender du så, når du deltager i konkurrencer. Hvis du begynder at få mange spam-e-mails på denne e-mail-adresse, kan du blot ændre den til f.eks. bo-konkurrence-1@mail.dk og slette den gamle.

Hvis du skal skrive din e-mail-adresse på din egen eller en anden hjemmeside, kan du skrive den i et format, som mennesker forstår, men som ikke let kan opsnuses. Hvis din e-mail-adresse f.eks. er bo@mail.dk kan du skrive "bo hos mail punktum dk" eller "bo@SPAMmail.dk - fjern SPAM, når du skal skrive til mig".

På denne måde kan robotter ikke høste din e-mail-adresse ved blot at gennemsøge hjemmesider, nyhedsgrupper eller andre steder, hvor du har din e-mail-adresse stående.

Frameld ikke spam

Selvom der nederst i næsten alle spam-e-mails står en e-mail-adresse eller et link til en hjemmeside, hvor du kan henvende dig for at framelde din e-mail-adresse, skal du aldrig svare på e-mailen eller klikke på linket.

Hvis du svarer på den e-mail-adresse eller klikker på linket, så ved afsenderen, at der er et menneske i den anden ende, som læser e-mails sendt til den pågældende e-mail-adresse, og du vil bare få endnu flere spam e-mails.

Næsten alle links i spam-e-mails indeholder et unikt id, således at firmaerne ved præcis, hvem der trykkede på linket i deres spam-e-mails. I værste fald risikerer du, at linket fører dig til et sted, hvor du får installeret spyware.

Har du et autosvar på din e-mail, vil afsenderne af spam e-mailen jo få det og dermed også vide, at de har ramt plet. Så overvej om det f.eks. er nødvendigt at have et autosvar, der blot fortæller, at du har modtaget e-mailen og vil læse den senere.

Læs mere om spam og sikkerhed på:
www.tdconline.dk/sikkerhed

Spar tid med Digital Signatur

Ved hjælp af et enkelt program på din computer slipper du for at huske på 20 forskellige passwords til diverse hjemmesider, og du kan ordne dine ting med det offentlige, når du har tid.

Af Signe Rasmussen, TDC

Du har godt nok modtaget brevet, men du skal lige hente børnene, handle ind, lave mad og kigge på papirerne til mødet i morgen. Så papirerne fra SKAT ender i bunken på bordet.

Pludselig er der gået en uge, og du kommer i tanke om, at du da også skal gå ind på www.skat.dk og få tjekket, om din selvangivelse passer, så du kan se, om der er ekstra penge til sommerferien.

Cursorer blinker, klar til at du kan taste din kode ind og få selvangivelsen ud af verdenen. Men hvor er selvangivelsen med tast-selv-koden? Lige meget, hvor mange gange, du endevender bunken, dukker selvangivelsen ikke op. Lyder det bekendt?

Personligt program

Hvad enten det er tast-selv-koden til SKAT, din kode til ATP, dit police-nummer til "danmark" eller dit password til Post Danmark, der er

forsvundet i papirbunken, kan du få hjælp af den digitale signatur.

Digital Signatur er dit visitkort på nettet, der sikrer din kommunikation med andre på nettet. Signaturen er et program, der ligger på din computer. Og selv om der ligger en kompliceret teknologi bag, er det lige til at installere – og så er det endda gratis.

Signaturen indeholder dit navn og dit CPR-nummer, så du bliver identificeret automatisk, når du skal logge ind på en side ved hjælp af Digital Signatur. Ved hjælp af kodning og afkodning bliver de informationer, du modtager og sender, beskyttet af signaturen, og du kan logge ind på nettet uden risiko for, at nogen opfanger dit password.

Nettet har åbent 24/7

Digital Signatur sparer dig for meget. Ikke mindst spildtid ved at lede efter passwords på bortkomne papirer. Du slipper også for

Her kan du blandt andet bruge din signatur:

De fleste kommuner
Skat.dk
Postdanmark.dk
Det kongelige bibliotek
Sundhed.dk
ATP
Sygesikringen "danmark"
Klasselotteriet
Netborger.dk
Alm. Brand

Find den fulde liste på:
www.digitalsignatur.dk

Læs mere om Digital Signatur:
www.tdc.dk/digital
www.digitalsignatur.dk

irriterende køer på kommunen, på posthuset eller lignende. En anden smart ting ved Digital Signatur er, at nettet ikke lukker ligesom kommunkontorer og andre offentlige myndigheder.

Så det er altså slut med at stresses igennem trafikken for at nå på posthuset, inden de lukker. Alt det praktiske omkring indflytning, kan du i ro og mag klare hjemme foran skærmen.

Mulighederne med Digital Signatur vokser hver dag, så bestil dit id-kort på nettet med det samme, og spar en masse tid.

Fakta:

Flere faktorer gør, at den digitale signatur er sikker som id-kort på nettet. For det første er det kun dig, der kan bruge den. Signaturen består af to nøgler, en privat og en offentlig, og den private forlader aldrig din computer. Den offentlige ligger hos TDC, og det er den, der bliver brugt, hvis du f.eks. sender krypterede e-mails til din advokat. Så skal han bruge den offentlige del af din signatur (sammen med sin egen digitale signatur) for at kunne læse din e-mail.

Desuden er din signatur beskyttet af et password, som yderligere sikrer, at det kun er dig, der kan bruge dit digitale visitkort. Så hvis det utænkelige skulle ske, og en hacker får adgang til programmet, der indeholder din digitale signatur, så kan han ikke bruge den uden dit password.

It-sikkerhed blandt heltinderne

Der har været følere ude i netværket "Morgendagens Heltinder" for at finde ud af, hvordan de forskellige kvinder, der er med i netværket, egentlig ser på it-sikkerhed.

Af **Henriette Weber Andersen**, Morgendagens Heltinder

Kvinderne, der melder sig ind i Morgendagens Heltinder, er såkaldte "I-kvinder", innovatorer, idéudviklere, initiativtagere, igangsættere og inspiratorer. Mange er med egen virksomhed, mens andre er ansat et sted og bare nyder godt af vidensdelingen mellem 1200 af danmarks mest banebrydende kvinder.

Det, vi har til fælles, er, at vi alle sammen er stolte af at kalde os heltinder, på den ene eller anden måde.

Når snakken falder på it-sikkerhed bliver man dog nødt til at vride svarene ud af medlemmerne – måske som Karin Bonnesen fra bybonnesen.com siger,

"Jeg har fortrængt alt om it-sikkerhed vedrørende min computer, fordi jeg helt automatisk går ud fra, at den it-mand, som har installeret alt på den, har taget højde for det".

En indstilling, som jeg selv kan nikke genkendende til. Man føler ikke, at man behøver at forholde sig til it-sikkerhed, før den første virus kommer igennem mailboksen eller internettet. Igen siger Karin Bonnesen fra bybonnesen.com,

"Der er nok lidt naivitet forbundet med min indstilling til it-sikkerhed, når det gælder mig selv. Det er altid de andre, der er uheldige, ikke mig".

Derudover er der også kvinder, som tager it-sikkerhed som en naturlig del af debatten med de virksomheder, der implementerer deres hjemmesider. Søs Wollesen fra

nukleus.dk fortæller, hvad hun har gjort for at sikre sin it-sikkerhed,

"Først og fremmest har jeg læst, hvad jeg kunne overkomme omkring det at sikre mine "elever" på nettet. Jeg har haft en del samtaler med it-supportere/ansvarlige i mindre software-virksomheder omkring netsikkerhed - nu og i fremtiden.

Mit program er specielt programmeret til mig og min opbygning af min undervisning. Det har de sikkerhedsforanstaltninger, som kan garantere elevernes integritet, og som gør programmet i stand til at kommunikere med andre systemer - uden at de fletter ind over hinanden og forstyrrer hinandens sikkerhed".

Generelt er tendensen dog i netværket, at informationerne om it-sikkerhed er vigtige. Helle Munk fra stress-a.dk siger,

"Jeg vil gerne vide, hvad jeg som minimum bør have og helst i en super kvalitet og til så få kroner som muligt, da der er meget andet at bruge kronerne på".

Så hvis man kombinerer informationerne omkring it-sikkerhed med en ændring i bevidstheden fra befolkningen generelt, er man godt på vej.

Eller hvad ?

Der kommer hele tiden nye tiltag fra hackere og spammere, der kan bryde ind i computere. Og måske er kvindernes bevidsthed omkring it-sikkerhed lavere end mænds.

Dette er en af grundene til at Morgendagens Heltinder er gået ind i netsikker nu!-projektet og holder en stribe foredrag rundt omkring i landet fra 2. maj.

Se www.netsikkernu.heltinder.dk for mere information og cases omkring netsikkerheden set med et kvindesynspunkt.

Adam og Eva på mobilen

Hvilken mobil ville Eva mon vælge for at kunne ringe til Adam? Og hvilken mobil ville du selv vælge, hvis du nu skulle vælge mellem en "haute couture"-model fra Samsung eller én med 18-karats guldcover fra Vertu?

Af **Brit Sung Kyung Kim Bech**, cand.mag.visuel kultur, projektmedarbejder

Vi kvinder elsker tilbehør som smykker eller designvedhæng til tasken, men hvordan er det lige med kvinder og højteknologiske gadgets? Nej vel? Det er noget for mænd, iklædt nålestribet, der forsøger at give den som en hverdagens James Bond. Men jeg ved bedre, for hør lige her, statistikker viser, at du som kvinde med 92 % sikkerhed har en mobil i håndtasken, og formentlig har du ydet din indsats for, at antallet af sms'er røg op på 4 mio. i første halvår af 2005. Og nu er min yndlingsgadget, mobilen, også til at få i "haute couture"-design.

Eva ville have valgt DVF-mobilen

Et af de stærkeste udspil fra mobilbranchen for at brande mobilen som andet og mere end for de "nålestribede" (mænd), må være det indledte samarbejde mellem Samsung og Vogue. Samsung lancerede i 2004 en "haute couture"-mobil, designet af Diane Von Furstenberg, også kaldet DVF-mobilen. Vogue's ("nålestribede") leder, Tom Florio ser mobilen, som den "ultimate accessory" og udtaler, "Samarbejdet mellem Vogue og Samsung repræsenterer, hvordan kvinders forhold til design og teknologi er blevet mere personlig".

Hvis Eva havde kunnet købe en Diane Von Furstenberg-mobil fra Samsung, var hun blevet medlem af en eksklusiv klub sammen med de andre 999 kvinder, idet der kun produceres 1.000 stk. Af ekstra tilbehør reklameres med en chick "City-mobiltaske til lip-gloss'en og kreditkortene" og selvfølgelig selve trofæet, som leveres med signeret screensaver og ikke at forglemme en skærm, der, ligesom på Nokia 7380, har spejlfunktion til at checke make-up'en. Og når alt dette er

nævnt, er mobilen i øvrigt kompatibel med CDMA 800 og 1900 netværk og understøtter Sprint PCS Vision Pack. Læste du hurtigt hen over denne sidste linie, så er du formentlig kvinde. Vi interesserer os ikke nødvendigvis for de tekniske detaljer, så længe "den" virker, som den skal. Man behøver jo ikke at være automekaniker for at køre bil eller cand.it for at tale eller sms'e fra mobilen, vel?

Kvindens forhold til design og teknologi?

Og der er jo det, som er kernen. Kvinder er vilde med højteknologiske gadgets, som f.eks. mobilen. Den giver en frihed og gør det nemmere at holde den daglige kontakt med ens personlige netværk. Og så er der også det mobile internet og spil. Så et lækkert design er kun en bonus.

At mobilen så i øvrigt er et teknologisk vidunder bestående af nanokredsløb på chippen, og at vi faktisk kan kommunikere via radiobølger og satellitter i rummet lige ned i håndtasken, er jo ikke vigtigt at vide for at kunne benytte den. Hov, nu ringer min mobil. Det må være Adam.

"Hej skat. Hvor er du?", siger Adam fra sin nye Vertu med 18-karats guldcover. Eva holder ømt om hendes haute couture DVF-model, "Jeg står lige midt i haven under et æbletræ. Kigger du forbi?".



DVF-model
Copyright Samsung

Signature 18-karat.
Copyright Vertu

Lad kvinderne klare it-sikkerheden

Mænd har mere styr på it-sikkerheden end kvinder, viser undersøgelse. Alligevel er der god fornuft i at inddrage kvinderne i sikkerheden på hjemme-pc'en, mener en kønsforsker.

Af Søren Aaes, TDC

Mænd er mere tilbøjelige til selv at installere antivirusprogrammer og sikre computerens trådløse netværk end kvinder. Det viser en rapport om danskernes holdning til it-sikkerhed, som IT- og Telestyrelsen fik udarbejdet i fjor.

Rapporten viser, at kun 35 % af de adspurgte kvinder selv sørger for it-sikkerheden på deres computer, mens tallet for mændenes vedkommende er 62 %.

Klaus Kristensen er tidligere it-sikkerhedschef ved TDC og medejer af konsulentfirmaet Parkegaard & Kristensen Sikkerhed, som udarbejdede undersøgelsen. Han mener, at mænd opfatter it-sikkerhed som et typisk mandeområde, som de nok skal klare.

"Kvinder søger oftere hjælp end mænd, der formentlig opfatter sig selv som mere kompetente. Det betyder, at mænd er hurtigere til at prøve tingene af, mens kvinderne er mere forsigtige", siger han.

Undersøgelsen baserer sig på det såkaldte KFE-indeks, der tager pulsen på, hvad befolkningen kender til it-sikkerhed, hvorfor

den er vigtig, og hvorvidt befolkningen efterlever råd om god it-sikkerhed. Igen får kvinderne en væsentligt lavere score end mændene. Klaus Kristensen mener, at det handler om interesse for det tekniske.

"It-sikkerhed er et område, som oftest forklæres i tekniske termer. Det kan være en årsag til, at kvinder typisk ikke prioriterer det højt. Hvis funktionaliteten er der, så er de ligeglade med den bagvedliggende teknik. Sagen er bare, at it-sikkerhed har mere med adfærd og orden at gøre end det tekniske".

Brug kvindernes kompetencer

Netop det, at man både kan betragte it-sikkerhed som noget teknisk og noget adfærdsmæssigt, ser kønsforsker og adjunkt, Ph.d., Chris Mathieu, som en væsentlig pointe.

"Det kan sagtens tænkes, at kvinder er mere disponerede for at tage sig af det rent adfærdsmæssige omkring it-sikkerhed. En del forskning har vist, at kvinder typisk har bedre sociale kompetencer og mere indlevelsesevne end mænd. Desuden er kvinder bedre til at tænke i helheder, mens mændene i højere grad fokuserer på enkelte interesser såsom teknik".

I sin forskning på Institut for Organisation og Arbejdssociologi på Copenhagen Business School, har han undersøgt, hvordan kvinder klarer sig i den mandsdominerede it-branche i Sverige. Her var det tydeligt, at kvinder oftere bliver sluset over i de mere bløde funktioner som projektledelse, kundekontakt og kommunikationsopgaver, mens mændene holder fast i de rent tekniske opgaver som systemudvikling.

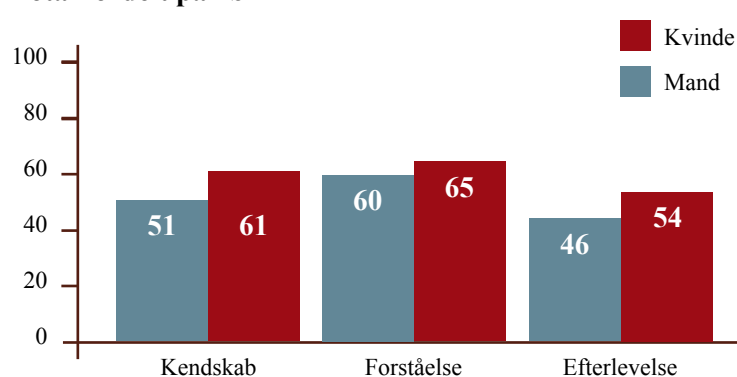
"Selvom de mænd og kvinder som var med i undersøgelsen havde samme tekniske færdigheder, var det alligevel kvinderne, der blev overtalt til at påtage sig de mindre tekniske opgaver. Simplethen fordi ledelsen på forhånd forventede, at deres sociale kompetencer ville give et bedre resultat", fortæller Chris Mathieu.

Og denne adfærd kan måske overføres til hjemmet, hvor arbejdsdelingen kan være, at kvinder tager sig af de overordnede regler for god sikkerhedsskik, mens manden installerer og opdaterer programmerne.

Ifølge Chris Mathieu skal man dog ikke undervurdere kvinders generelle evne til at forstå it-sikkerhed.

Total fordelt på køn

Kilde: IT- og Telestyrelsen 2005



Undersøgelsen af befolkningens it-sikkerhedskultur viser en væsentlig forskel på kvinder og mænd. De tre søjler beskriver befolkningens kendskab til regler om it-sikkerhed, deres forståelse af hvorfor reglerne er vigtige og endelig, hvorvidt disse regler bliver efterlevet.

"Der findes studier, som har vist, at yngre kvinder på arbejdspladsen f.eks. er bedre til at tilegne sig tekniske færdigheder end ældre mænd. Og det kan måske være med til at nuancere debatten om kønnets betydning. Man skal jo heller ikke glemme, at enlige kvinder godt selv kan finde ud af at købe en pc", siger han.

Brug for oplysning

Chris Mathieu mener dog fortsat, at man skal forsøge at gøre it-sikkerhed mere lettilgængelig.

"Det er vigtigt, at it-sikkerhed også er et fremtrædende emne de steder, hvor kvinder får deres information

f.eks. i ugeblade og månedsblade", siger Chris Mathieu.

Hos IT- og Telestyrelsen, der står bag netsikker nu!-kampagnen, er man opmærksom på den skævhed, der er i mænd og kvinders holdning til it-sikkerhed.

"I løbet af efteråret vil vi igen lave statistik, som netop tager højde for problematikken omkring kvinder og it-sikkerhed. Derudover har vi jo allerede i den nuværende kampagne valgt fokusere på kvinder, fordi vi ved, at det er vigtigt at få dem i tale, for it-sikkerhedens skyld", siger projektleder i IT- og Telestyrelsen, Anne Frederiksen.

Spring bare ud i det kvinder

It-sikkerhed er pærenemt, mener Annette Kofoed, der selv tog affære, da en virus fik hjemme-pc'en til at bryde sammen.

Af Søren Aaes, TDC

I Annette Kofoeds hjem, er det hende, der er chef for it-sikkerheden på hjemme-pc'en. Godt nok var det hendes samlever, der købte computeren i sin tid, men

it-sikkerheden er hendes domæne. "Jeg tager jævnligt sikkerhedskopier af vores dokumenter, billeder og andre uundværlige data. Og så bruger vi vores sunde fornuft, når vi færdes på nettet. Det er f.eks. slut med at opkalde passwords efter hunden", siger Annette Kofoed.

Annette Kofoed tog musen i egen hånd, da en drilsk virus slettede alle data på hendes og kærestens private computer.

"Det var ret træls. Vi havde ikke taget sikkerhedskopier af vores

dokumenter og havde ikke installeret noget antivirusprogram, som kunne advare os. Derfor besluttede jeg, at der skulle gøres noget".

Spring ud i det

Oplevelsen fik hende til at anskaffe en sikkerhedspakke med et antivirusprogram og en firewall, som hun installerede helt uden problemer.

"Jeg blev overrasket over, hvor pærenemt det var. Hvis jeg var i tvivl om noget, ringede jeg bare til mit teleselskab eller spurgte en

kollega i it-afdelingen", fortæller Annette Kofoed, der til daglig er idrætskoordinator i DGI.

Hun synes ikke, at kvinder skal være bange for at kaste sig ud i det.

"En del kvinder tror måske, at de ikke kan finde ud af det, og overlader det derfor til manden. Men man skal jo ikke ned og pille ved ledninger og printkort. Det hele foregår foran skærmen", beroliger Annette Kofoed, som også har fået sin mor, der er sidst i 50'erne, med på vognen.



Phishing

- svindlere på fisketur

Svindlere håber, at de kan lokke dig i nettet og stjæle dine personlige oplysninger og penge. Phishing er et mere og mere udbredt begreb, og der ses hele tiden en stigning i antallet af forsøg. Bagmændene udvikler og forfiner deres teknik for at få flere til at gå i fælden.

Af Stina Christiansen, TDC

En e-mail fra din bank om, at du skal ændre dit password.

Et firma, du aldrig har hørt om, beder dig bekræfte dine brugeroplysninger.

Superbilligmusik.com lokker med cd'er til en krone.

Det er alle sammen velkendte phishingforsøg. Hackere sender dig e-mails, som ser ud som om, de kommer fra et velkendt firma. Håbet er, at du hopper i med begge ben og giver dem de oplysninger, de skal bruge for at tømme din bankkonto. Metoderne til at få dig til at klikke på et link eller åbne en vedhæftet fil er mange. Det kan være et løfte om gratis fodboldbilletter, som vi så det i virussen Sober.p i maj 2005 eller den store I love you virus, hvor de fleste var ivrige efter at læse den vedhæftede kærlighedserklæring og dermed aktiverede virussen.

Oftest ses forsøgene på phishing som masse-e-mails med et fælles budskab. Et tænkt eksempel kunne være en e-mail fra en bank, som beder dig om at indtaste dine oplysninger

på din netbank for at undgå, at din konto lukkes. Hvis det ikke er dér, du har dine penge, er du udmærket klar over, at der er tale om en fup-e-mail. Men bruger afsenderen navnet på lige netop den bank, du har, er det svært at gennemskue, at der er tale om fup.

Uopfordret kontakt

En vigtig huskeregel er, at der ikke er nogen firmaer, der kontakter dig uopfordret og beder dig om kontooplysninger, passwords, kortnummer eller kontrolcifre - hvad enten du er kunde hos dem eller ej. Tonen i e-mailen er ofte stressende, og man skal virkelig skynde sig at få det gjort, ellers har det nogle frygtelige konsekvenser. Vær altid tilbageholdende med personlige oplysninger på nettet.

Lokker informationer frem

En e-mail med et phishingforsøg vil bede dig om at sende oplysninger tilbage eller at gå ind på en hjemmeside. E-mailen kan jo sagtens komme fra et firma eller en instans, som du kender og har tillid til. Men det er relativt let at forfalske adresser og endnu lettere at lave en falsk afsenderadresse på en e-mail.

Når du kommer ind på den falske hjemmeside, vil man på forskellige måder lokke informationerne ud af dig. Det kan være ved at love dig cd'er til en krone, gratis software eller andet - bare du vil bytte med kontooplysninger, og hvad de ellers skal bruge for at kunne udgive sig for at være dig, når de bruger dine penge på nettet.

Du kan naturligvis også blive lokket ind på en falsk hjemmeside på en anden vis end via en e-mail.

Læs mere om sikkerhed på:
www.tdconline.dk/sikkerhed

Værktøjer til at undgå phishing

Microsoft har udviklet et Phishing Filter, som virker sammen med MSN's search toolbar. Så den skal du altså installere først. Er du på vej ind på en hjemmeside, der er sat i forbindelse med phishing, vil du blive advaret af filteret.

Firmaet Earthlink har udviklet en værktøjslinje, som du kan installere i din browser, så du får en advarsel, hvis du er inde på en hjemmeside, der er kendt som phishing-side.

Det vil naturligvis hovedsageligt være udenlandske hjemmesider.

Et andet værktøj er Netcraft Toolbar, som ligeledes blokerer mod phishing-sider, brugerne har anmeldt.

Dit spamfilter kan også indeholde beskyttelse mod phishing-e-mails.

Se mere på:

www.microsoft.dk/phishing
www.earthlink.net/software/free/toolbar
www.toolbar.netcraft.com

Fakta:

FBI's råd mod phishing

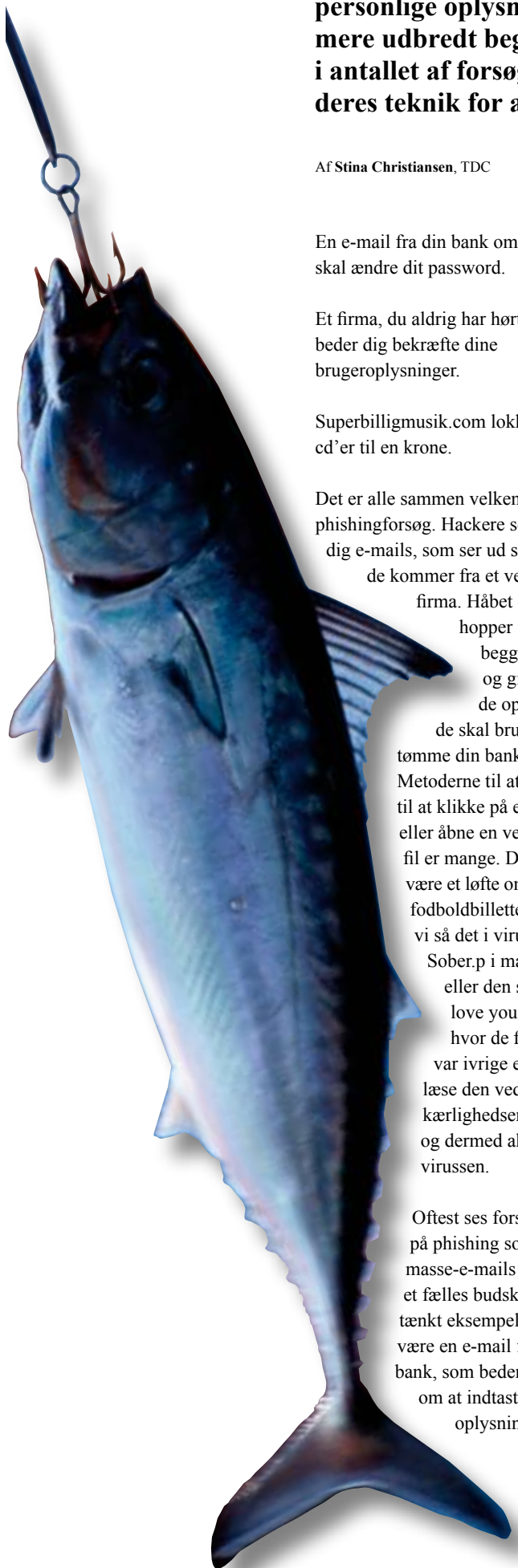
FBI har skrevet en række gode råd om, hvordan du undgår phishing.

- Vær på vagt over for uopfordrede e-mails, der beder dig om at give private oplysninger i en e-mail eller på en hjemmeside
- Brug den samme proces, som du har brugt før, når du behov for at opdatere dine informationer online
- Siger adressen på en hjemmeside dig ikke lige noget, er den formentlig falsk. Brug kun den adresse, du kender og har brugt før
- Anmeld altid ulovlige eller mistænkelige e-mails til din internetudbyder
- De fleste firmaer har en procedure, hvor du logger på en sikker side. Kig efter låsen i bunden af din browser og "https" i starten af sidens adresse. Tjek certifikatet, firmanavnene og udløbsdatoen

• Læg mærke til adressen i browseren. Falske hjemmesider har typisk en temmelig lang adresse, hvor firmanavnet ikke er nævnt som det første - eller måske slet ikke er der

• Hvis du har nogen som helst tvivl om en e-mail eller en hjemmeside, så kontakt det rigtige firma direkte, og spørg, om e-mailen kommer fra dem, eller siden virkelig er deres

• Bliver du udsat for en falsk e-mail eller hjemmeside, bør du kontakte det lokale politi - eller kontakte FBI's Internet Fraud Complaint Center på www.IFCCFBI.gov



Kast ikke håndklædet i ringen!

Af Anne Viksøe, IT- og Telestyrelsen

Sund fornuft og naturlig skepsis hænger uløseligt sammen med it-sikkerhed, når vi færdes på internettet. Mange forbinder it-sikkerhed med komplicerede løsninger, der kræver stor teknisk indsigt – og smider derfor på forhånd håndklædet i ringen i forhold til at udnytte internettets mange muligheder. Men du behøver ikke være it-sikkerhedsuddannet for at kunne forbedre din egen sikkerhed på nettet. Det kræver blot lidt sund fornuft – krydret med naturlig skepsis.

Computere og internet er blevet en stadig vigtigere del af danskernes hverdag. Derfor er det afgørende, at folk føler sig trygge ved at bruge de mange nye muligheder. Det gør de kun, hvis de ved mere om disse muligheder og bliver fortrolige med dem.

Kun 16 % af de 60-74-årige danskere handler i dag over internettet. Mange af de ældre fravælger muligheden, fordi de er nervøse for sikkerheden. Ofte kunne en større viden om, hvordan man bedst begår sig på nettet, mindske disse bekymringer.

Der er ingen grund til at føle sig skræmt over at bruge nettet og drage gavn af dets mange muligheder – f.eks. nem kommunikation med familie og venner, informationssøgning og e-handel. Det handler bare om at bruge sin sunde fornuft.

En god tommelfingerregel er at opføre sig på internettet, som man selv ville gøre i sin dagligdag. Lige som vi ikke udleverer vores kontonummer eller CPR-nummer til en

tilfældig forbipasserende på gaden, skal vi heller ikke på nettet udlevere personfølsomme oplysninger til personer, vi ikke føler os trygge ved.

Træthed, travlhed eller dårligt vejr er ikke længere en forhindring for at komme i banken eller på biblioteket. Du kan nemlig både bestille bøger og ordne bankforretninger over internettet. Husk blot at bruge din sunde fornuft.

Med internettet bliver afstanden til familie og venner kortere, og mulighederne for at kommunikere er mange – fra udveksling af e-mail til samtaler med lyd og billede ved hjælp af et webkamera. På den måde kan man hjemme i stuen med et par museklik høre nyt fra barnet på Borneo og se billeder af familien i Australien. Mulighederne er større, end man tror!

Ligesom sikkerhed i trafikken i høj grad kræver, at du selv er opmærksom, så er det farligste på nettet ofte dig selv. Men med fornuft og omtanke er den fare ikke særlig stor.

En ud af fem personer over 60 år undlader at bruge internettet til visse ting på grund af manglende viden om sikkerheden.

Kilde: IT- og Telestyrelsen

Otte ud af ti personer over 60 år forbinder it-sikkerhed med teknik. En ud af tre forbinder det med deres egen adfærd.

Kilde: IT- og Telestyrelsen



Brug sund fornuft når du handler på nettet

Danskerne handler i stigende grad over internettet, og de danske netbutikker oplever en klar vækst i antallet af kortbetalinger. Nethandlen er sikker, hvis forbrugerne blot husker nogle enkle regler.

Af Klavs Valskov, Nordea

Danskerne har fået øjnene op for internettets bekvemmeligheder og muligheden for at undgå lange køer. Fra 1999 til 2005 er antallet af kortbetalinger på internettet ifølge PBS steget fra 100.000 til 19 mio. Betalingskortet ryger specielt op af lommen, når der skal tankes taletid til mobilen, bestilles rejser eller købes nyt computerudstyr.

Forbrugerne har ofte bedre vilkår og rettigheder, når de handler på internettet.

”Danskerne bliver gradvis mere trygge ved nethandel, og de behøver ikke at frygte misbrug, hvis de bruger anerkendte betalingsmetoder såsom kortbetaling eller bankernes e-betalinger. Faktisk er kundens rettigheder bedre, når man handler i netbutikker end i de fysiske butikker, fordi man som udgangspunkt har 14 dages fortrydelsesret ved handel i netbutikker”, forklarer Lasse Fonager Nørgaard, der til dagligt arbejder med elektronisk betaling i Nordea.

Det er også betryggende, at banken kan tilbageføre ens penge, hvis man benytter kort- eller elektronisk betaling.

Man skal tage sig i agt for snu forretningsdrivende, der forsøger at fraliste penge fra kunderne uden at levere varen. F.eks. skal man være forsigtig med at indsætte penge direkte på butikkens bankkonto gennem en såkaldt konto-til-konto-overførsel. I disse tilfælde vil forbrugeren selv være ansvarlig for at få sine penge retur, hvis der opstår problemer.

”Generelt er det bedste råd ved handel på internettet at bruge sin sunde fornuft. Undersøg sælger, inden du handler på nettet. Brug samme fornuft ved internethandel, som når du undgår lyssky handlende”, afslutter Lasse Nørgaard.

Læs mere om sikker nethandel på: www.forbrug.dk

Her kan du bl.a. downloade Forbrugerstyrelsens håndbog ”Køb trygt på internet og postordre”, som du også kan hente i Nordeas filialer landet over.

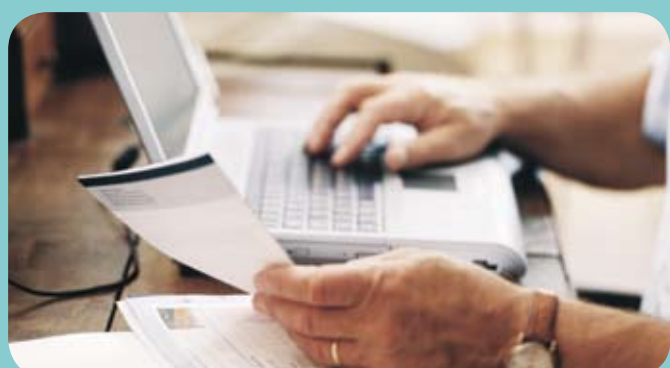
Fakta:

Du kan få dine penge tilbage ved internethandel:

- Hvis det hævede beløb fra din konto overstiger det aftalte beløb
- Hvis varen ikke leveres på aftalte tidspunkt
- Hvis du fortryder købet inden for 14 dage

Guide til internethandel

- Kend sælgers navn, adresse, telefonnr., e-mail og CVR-nr.
- Kig efter en hængelås nederst i skærbilledet – ved at klikke på den kan du kontrollere, hvem du kommunikerer med
- Brug betalingskort eller bankernes e-betaling
- Betal aldrig forud med check
- Undgå at indsætte penge direkte på butikkens bankkonto, konto-til-konto-overførsel
- Kend virksomhedens betingelser for levering og mulighederne for at klage
- Få en kvittering på købet
- Udskriv ordrebekræftelse og tjek betalingen i din netbank eller på din kontoudskrift fra banken





En hjælp i hverdagen

Bare fordi man ikke er opvokset med internettet, er der ingen grund til at stå af. På datastuer over hele landet tilbyder Ældremobiliseringen alle over 60 år hjælp til at gøre internettet til en naturlig del af hverdagen. Og det er det hele værd, når f.eks. børn og børnebørn dukker op på skærmen.

Af Annette Schiøler, Den fynsk/jyske Sammenslutning af Pensionistforeninger

”At Ældremobiliseringen deltager i kampagnen netsikker nu! er en naturlig forlængelse af organisationens indsats for, at de ældre generationer også kan blive fortrolige med og have glæde af de muligheder, som computere og internettet byder på”, fastslår organisationens næstformand, Olav Mikkelsen

”I dag bor familierne langt væk fra hinanden, og afstandene er ofte for store til, at forældre og børn bare kan mødes et par timer en aften. Vi mødes heller ikke så tit med børnebørnene. Derfor må vi lære nye måder at opretholde kontakten på. Både børn og børnebørn sidder jo ved computeren som en del af deres hverdag, så det er et oplagt sted at fange dem med en e-mail”, fortsætter han.

Ældremobiliseringen står bag oprettelsen af omkring 100 datastuer, hvor ældre landet over kan stifte bekendtskab med computere og internettet. Og yderligere omkring 40 datastuer er på vej. Idéen er, at man mødes, hjælper hinanden og kan få undervisning i forskellige programmer, internet og e-mails. Bortset fra et symbolsk beløb til kaffe, papir og lignende, er det gratis.

Men det er ikke kun i forhold til familien, at afstandene er blevet større, påpeger Olav Mikkelsen ”Vi får også længere til at kunne klare mange af vores ærinder. I mange mindre byer er butikker, apoteker og bankfilialer lukket, og når kommunalreformen og retsreformen træder i kraft, vil vi givetvis også få længere til det offentlige”.

”Det er efterhånden også nødvendigt for ældre at kunne bruge e-mail og benytte de muligheder, som internettet tilbyder, f.eks. for at kunne opretholde kontakten til familien”, siger Olav Mikkelsen.

Med mulighederne for at ordne bankforretninger, købe ind og kommunikere med det offentlige, kan internettet på mange områder være den ældre til stor hjælp i hverdagen. Derfor er det så vigtigt, at de ikke alene får mulighed for at lære at benytte nettet, men også får forståelsen af, at det ikke er farligt at gøre det.

Internettet er mulighedernes land

- Også for ældre. Du skal bare bruge din sunde fornuft og din kritiske sans, lyder budskabet fra Ældremobiliseringen.

Af Annette Schiøler, Den fynsk/jyske Sammenslutning af Pensionistforeninger

Sid derhjemme og find ud af, om du stadig har penge på kontoen her, to dage før pensionen går ind. Når det viser sig, at det har du, så bestil billetter til en tur i biografen med børnebørnene – begge dele uden at løfte telefonrøret.

Reserver den bog, du gerne vil låne på biblioteket - uden at skulle ud i regnen og blæsten. Slip for køen på posthuset og betal dine regninger – uden at skulle betale gebyrer.

På internettet ligger banken, biografen, biblioteket, posthuset og utallige forretninger kun et par klik borte, og så har de endda åbent døgn rundt. Mulighederne er mange, det handler bare om at springe ud i det.

Ingen grund til bekymring

”Der er ingen grund til at være bange for at bruge internettet. Du skal bare bruge din sunde fornuft og din kritiske sans - præcis som du gør det ude i den virkelige verden. Der lægger du jo heller ikke dit Dankort eller kortet til din bankkonto på fortovet med en lille seddel med koden på ved siden af”, siger projektkonsulent på kampagnen netsikker nu!, Morten Lembke fra Ældremobiliseringen.

Det er vigtigt at have en firewall og et antivirusprogram installeret på din computer. Det lyder teknisk, men begge dele kan klares med en sikkerhedspakke, som ens internetudbyder kan hjælpe med. Har du sikret din computer, kommer du rigtigt langt ved at bruge din sunde fornuft f.eks. aldrig åbne en e-mail fra en afsender, du ikke kender.

Frihed, albuering og god beskyttelse

”Med den sunde fornuft og den kritiske sans ved din side er internettet mulighedernes land”, siger Morten Lembke.

Udover at internettet giver frihed og albuering til at handle, når du vil, og du sparer penge til gebyrer, har du faktisk også større beskyttelse, når du handler på nettet end i virkelighedens butikker. Bliver din konto misbrugt, uden at du selv er skyld i det, dækker bankerne tabet. Desuden har du 14 dages fortrydelsesret på varer, du køber over internettet, hvor det i den virkelige verden er den enkelte forretning, der afgør, om du må returnere en vare og få pengene tilbage. ”Uanset om vi vil det eller ej, så går udviklingen i retning mod mere og mere internet”, spår Morten Lembke.

”Et godt eksempel er det offentlige, som i højere og højere grad kommunikerer via nettet. Men i stedet for at se det som et nødvendigt onde at skulle kaste sig ud i f.eks. en Digital Signatur, så er der virkelig meget at vinde ved at benytte sig af mulighederne”, afslutter han.



Gode råd

om sikkerhed fra branchen

Syv organisationer inden for it-branchen er blevet enige om en række fælles sikkerhedsråd. Se her, hvordan du kan blive sikker på internettet.

Af Stina Christiansen, TDC

Stod det til det tidligere "Rådet for it-sikkerhed", så er sikkerhed noget, der automatisk følger med, når du køber en ny computer eller forbindelse. Men sådan er det desværre ikke, så du skal have antennerne ude og holde hovedet koldt, når du er på nettet med din computer. Som hjælp får du en række gode råd, som branchen i fællesskab er blevet enige om, er de bedste.

Syv organisationer, DANSK IT, DK-CERT, Finansrådet, IT-Branche-foreningen, ITEK, Prosa/1984.dk samt TDC har givet deres bud på de vigtigste råd, som en almindelig internetbruger bør kunne i søvne og ikke mindst i vågen tilstand. Det er blevet til fem generelle gode råd og ti bonusråd, der handler om, hvordan du passer på dine personlige og fortrolige oplysninger.

Sådan beskytter du dig selv og undgår at sprede sikkerhedsproblemer til andre:

1 Brug et antivirusprogram med automatisk opdatering, en firewall og et antispywareprogram. Sammen beskytter programmerne din pc mod mange angreb og skadelige programmer.

2 Anvend opdaterede versioner af dit styresystem, din webbrowser og dit e-mail-program. Slå automatisk opdatering til, hvor det er muligt, så glemmer du det ikke.

3 Vær ekstra opmærksom, når du åbner vedhæftede filer. De kan indeholde virus. Pas især på filer med underlige eller lokkende navne, også hvis de kommer fra nogen, du kender.

4 Hvis du benytter trådløst internet, så slå kryptering til – ellers kan andre kigge med eller misbruge din internetforbindelse. Vælg stærk kryptering.

5 Bed andre om hjælp, hvis du er i tvivl, og brug i øvrigt din sunde fornuft. Selv om du har en god sikkerhedspakke, så forhold dig kritisk til de netsteder, du besøger.

... og sådan passer du på dine personlige og fortrolige oplysninger:

6 Passwords er den vigtigste beskyttelse af dine personlige oplysninger.

7 Vær påpasselig med at afgive personlige oplysninger via e-mail. Det svarer til at sende åbne postkort. Hvis du sender fortroligt materiale som e-mail, så brug kryptering og Digital Signatur. Hold øje med, om netsteder, der beder om fortrolige oplysninger, benytter kryptering (se efter hængelås nederst i browseren).

8 Slet spam uden at åbne det, og svar ikke på spam. Hvis du åbner eller svarer på spam, kan afsenderen se det, og så får du sandsynligvis mere spam. Benyt eventuelt et spamfilter.

9 Hent kun programmer fra internettet, hvis du stoler på netstedet, du henter det fra. Undersøg, om du siger ja til reklamer og afgivelse af private oplysninger, før du installerer.

10 Undgå spyware og adware. Det er programmer, som opsamler oplysninger om din identitet og adfærd og udsætter dig for uønsket annoncering.

11 Reager ikke på e-mails fra banker og betalings-tjenester, hvis de indeholder links, du skal klikke på eller anmoder dig om personlige og fortrolige oplysninger.

12 Brug password til log-in på din computer.

13 Indstil sikkerhedsniveauet i din browser, så du altid bliver spurgt, når informationer, filer og programmer overføres til din computer.

14 Vær påpasselig, når du bruger chat og instant messaging. Disse tjenester er nye og spreder sikkerhedsproblemer endnu hurtigere end e-mails. Klik kun på links, hvis du kan gennemskue, hvor de fører hen, og du har tillid til afsenderen.

15 Lav sikkerhedskopier af dine vigtige dokumenter og filer og tjek, at de kan genindlæses.

Du kan finde rådene på: www.it-borger.dk

Fakta:

Det er forskelligt fra computer til computer, hvordan du krypterer. Læs derfor altid vejledningen til din computer, hvor du kan finde de relevante informationer.

Gratis

TDC Sikkerhedspakke
Lige nu kan du få en TDC Sikkerhedspakke gratis på prøve i en måned. Sikkerhedspakken beskytter din computer med firewall, antivirus, antispyware og forældrestyring.

Download din prøveversion inden 1. juli 2006 på: www.tdc.dk/netsikker

Spim

Du kender spam – men kender du spim?
Det er spam over på ICQ, Messenger og lignende.

Af Stina Christiansen, TDC

Bruger du Instant Messengers, små chatprogrammer som f.eks. ICQ og MSN Messenger, har du måske allerede prøvet at blive kontaktet af fremmede, der sender dig links og andet.

Spim er en ny trussel og et nyt problem, som vi formentlig kommer til at se mere og mere til på internettet. Sikkerhedseksperter forudser, at vi kommer til at se en fortsat stigning af spim de kommende år.

For dem, der gerne vil af med et budskab eller have dig til at besøge en bestemt hjemmeside, er Instant Messengers et rigtig dejligt redskab. Her kan de nemlig tit søge efter folk, så de finder dem

med det rigtige køn og den rigtige alder - og har du udfyldt rigtig mange oplysninger om dig selv, kender de endda måske dine interesser.

Det handler selvfølgelig om omtanke, men du kan også tage et par forholdsregler for at undgå alt for meget spim.

- Lad være med at acceptere kontakt fra personer, som du ikke kender
- Lad være med at downloade vedhæftede filer fra folk, du ikke kender
- Hav altid et antivirusprogram på din maskine, og hold dit operativsystem opdateret



”Sikkerhedsbevidst bruger”

- hvad er det?

Du bruger internettet hver dag som et led i dit arbejde. Du har måske endda en hjemme-arbejdsplads. Stedet, hvor du arbejder, har både antivirus og en firewall. Så hvorfor har it-sikkerhed noget med dig personligt at gøre? Og kan du i det hele taget lære noget?

Af Claus Fønnesbech,
PricewaterhouseCoopers

Lad mig give et eksempel. Vivi arbejder som koordinator på et rejsebureau. Hun har en hjemme-arbejdsplads, som hun benytter flittigt. Vivi sidder en søndag aften og søger på internettet efter gode

rejsemuligheder til sommerferien. Pludselig kommer der en besked op på hendes computerskærm. Beskeden fortæller, at hendes computer ikke er opdateret mod de

nyeste computervirusser. Beskeden fortæller hende også, at hun ved at klikke på knappen kan installere et gratis antivirus program. Vivi klikker på knappen. En ny kasse kommer frem på skærmen. Der står, ”vil du installere og køre programmet”? Vivi klikker på ”ja”. Programmet bliver installeret. Bagefter sker der ingenting. Vivi går tilbage til internetsiden. Men nu viser internettet kun den samme side hele tiden, uanset hvad Vivi taster ind. Vivi tænker, at hun kan fortsætte sin søgning på arbejdet dagen efter. Hun skriver navnene på de gode rejse-hjemmesider ned i et word-dokument og gemmer dokumentet på en diskette, som hun kan tage med ind på rejsebureauet. Næste dag vil hendes internet på arbejdet heller ikke virke. Hvad er det dog, der sker?

Virus på computeren kan medføre et langt og smertefuldt nedbrud

I virkeligheden blev Vivi udsat for snyd og bedrag, der er udtænkt af skumle mennesker på internettet. Hun blev lokket til at hente en virus, der ødelægger søge-

programmet og samtidig gemmer sig i alle word-dokumenter. Vivi ”bar” virusen med ind i firmaet, som så også blev ramt.

Historien om Vivi er et tænkt eksempel, der bygger på tusindvis af virkelige hændelser. Mit gæt er, at når Vivi fortæller sin historie til sin it-afdeling eller til den it-kyndige i afdelingen, vil hun blive mødt med en holdning som ”herregud, det er da sund fornuft, at man ikke ...”!

Men for langt de fleste computerbrugere er det ikke sund fornuft. Sund fornuft, det er, at man aldrig ville modtage et tilbud om en eller anden gratis ydelse fra én, der springer ud fra en tilfældig butik, mens man shopper, mod at vi afleverer vores dankort og pinkode ved indgangen. Det har vi alle lært, fra vi var små. Stol aldrig på

mærkelige mennesker, der tilbyder noget gratis! Gå aldrig med en fremmed!

Udvis sund skepsis

Det er nøjagtig den samme skepsis, du bør udvise på internettet. Fordi internettet ikke er andet end en stor verden, der er indrettet fuldstændig som den virkelige. Med samme muligheder. Og med samme trusler.

Du skal ikke kunne loven udenad

For at undgå alle de sjove fremmedord, som ”computer worm”, ”spam” og ”phishing”, må man som bruger udvise ”it-sikkerhed”. Der er bare dét, at it-sikkerhed ikke er det mest spændende for pc-brugere, hverken på arbejdet eller derhjemme. Men ingen vil nogensinde kræve, at du som almindelig bruger skal kunne forklare, hvordan computeren behandler sine data. Eller at du skal kunne antivirusloven udenad. Nøglen ligger i, at du opnår den

sikkerhedsviden, der er relevant for dig. At du viser ansvarlighed i dine handlinger. Fuldstændig som du naturligt ville gøre ude i den virkelige verden.

Al sikkerhed starter og slutter hos dig

Når du til denne erkendelse, så er du allerede ved at blive til en sikkerhedsbevidst bruger. Det er ikke nok at sige ”det har it styr på i vores virksomhed”. Man kan kun komme en del af vejen gennem sikkerhedsteknik og restriktive regler for computeranvendelse. Al sikkerhed starter og slutter hos brugerne. Et større kendskab til konsekvenserne ved forkerte eller ubevidste handlinger foran

Spam er til skade for dig og dine omgivelser

computeren er medvirkende til, at du som bruger ikke længere er en sikkerhedsrisiko for din virksomhed. Målet er nået, når du gennem din adfærd er tryk på nettet ved blot at følge nogle simple spilleregler i de daglige rutiner.

Følg sikkerhedspolitikken

Har din virksomhed en sikkerhedspolitik? Og hvad går den ud på? Kan du besvare disse spørgsmål, er du formodentlig en af de få. Men når din virksomhed har en sikkerhedspolitik, er det ikke for sjov. Det kan koste dyrt, hvis du som medarbejder ikke tænker over eller ved, hvilke døre du åbner på nettet.

Af Henning Mortensen, ITEK/Dansk Industri

De fleste virksomheder har i dag en sikkerhedspolitik, du som medarbejder skal følge. Det er der god grund til. Sikkerhedspolitikken har til formål at understøtte og sikre virksomhedens forretning og værdigrundlag, og gennem sikkerhedspolitikken og de retningslinier, der ofte følger med, kan virksomheden styre risikoen for, at it-systemerne ikke går ned med store tab til følge. Men politikken gør det ikke alene, slet ikke når den sidder i sit ringbind og ofte er den mest støvede mappe på reolen. For

at få effekt, kræver det, at du som medarbejder efterlever politikken i dagligdagen.

Gå på opdagelse og spørg løs

Måske kender du til sikkerhedspolitikken, men hvad betyder den reelt for arbejdet i hverdagen? Politikken vil ofte indeholde nogle bestemmelser om, hvad du som medarbejder har lov til at bruge it-systemerne til, og hvordan de skal bruges. Er der steder, hvor politikken ikke er tilstrækkelig klar,

eller føler du, at den kan være svær at efterleve i det daglige arbejde, er det vigtigt at få en dialog om det på arbejdspladsen. Stil hellere et spørgsmål for meget end for lidt.

Hvem giver du adgang til virksomhedens systemer?

Meget af det arbejde, du udfører, hører kun til i virksomheden og må ikke videregives til fremmede personer. Ligesom du aldrig i den virkelige verden ville lukke én, du ikke kender, ind i virksomheden, bør du også være på vagt på nettet. Tyveri af data er ikke betinget af fysisk adgang. I dag kan elektroniske data stjæles endnu lettere ved at forsøge at bruge en medarbejders password til systemet. Det er derfor vigtigt, at du tager dig tid til at finde et sikkert password og sørger for at holde det personligt.

Hvad afslører du om din virksomhed?

Når du surfer eller sender en e-mail, efterlader du spor forskellige steder.

Og er det virksomhedens udstyr, du bruger, er det virksomheden, der efterlader sig spor. Som medarbejder er det derfor vigtigt at vurdere, hvor det har interesse, og hvor det ikke har interesse, at virksomhedens spor kan registreres. Ofte vil der i virksomhedens sikkerhedspolitik stå, at du kun må anvende virksomhedens udstyr til privat formål i begrænset omfang. Mange af de mindre seriøse hjemmesider, som man besøger i sin fritid, har ofte et lavere sikkerhedsniveau. Et

besøg på en sådan hjemmeside kan ødelægge virksomhedens netværk.

Som i den virkelige verden

Anvendelsen af it er ikke forskellig fra anvendelse af ting i den virkelige verden. Det handler om at efterleve nogle regler og så ellers bare bruge sin sunde fornuft. Og skulle det ske, at der sker underlige ting på computeren, så bed om hjælp – hellere en gang for meget end en gang for lidt.



Beskyt dit privatliv på nettet

Har du nogensinde tænkt over, hvad du ubevidst fortæller om dig selv på nettet? Når du surfer, henter programmer eller søger oplysninger generelt, efterlader du digitale spor. Ikke nødvendigvis spor, som vil blive misbrugt af andre, men spor, der giver andre mulighed for at trænge ind i din "privatsfære".

Af Peter Kruse, CSIS

For mange af os har ordet "privatsfære" i den virkelige verden stor betydning. Vi tager vores forholdsregler, sørger for at låse døren og sikrer, at ikke alle kan komme for tæt på. Men når det gælder vores færden i den virtuelle verden, ser billedet noget anderledes ud. Måske fordi man let taber pusten, når man i denne sammenhæng støder på begrebet "privacy", fordi det er så uhyggeligt bredt.

Vær konstruktivt kritisk

Egentlig skal der ikke så meget til at opnå privacy på nettet. Der findes nogle enkle spilleregler, som helt overordnet går ud på at være konstruktivt kritisk. Hvem deler du f.eks. oplysninger med? Og hvilke oplysninger siger du ja til at lade gå videre til en tredjepart? Det gælder både oplysninger, du selv indtaster, når du skal have adgang til forskellige onlinetjenester, og oplysninger, som du giver i forbindelse med installation af programmer og værktøjer.

Dele-computer?

Hvis I er flere om at anvende samme computer, vil de data, du henter ned, måske kunne læses af andre,

der efterfølgende bruger maskinen. For at undgå, at andre kan se, hvilke sider du har besøgt med f.eks. Internet Explorer, er det en idé løbende at tømme mellemlaget. Man kan gøre det med regelmæssige intervaller eller sætte Internet Explorer til automatisk at tømme cache, når browseren lukkes eller efter x antal dage.

De oplysninger, der bliver gemt i browserens mellemlager, kan være adresser på de sider, du har besøgt, brugernavne og passwords til onlineservices som f.eks. MSN, Yahoo og andre tjenester, der kræver, at du logger på. Hvis oplysningerne ikke er krypterede (dvs. beskyttet mod at kunne tyde teksten), kan andre læse dem og f.eks. logge på som dig, læse e-mails eller modtage og afsende beskeder i dit navn. De fleste browsere kan indstilles, så dine login-oplysninger automatisk bliver krypteret og beskyttet af et "hovedpassword", eller så mellemlaget automatisk slettes, når man logger af.

Spioner bag pornosider

Pornosider og sider med ulovligt software er et mekka for personer,

der ønsker at få kontrol med din computer eller ønsker at installere adware eller spyware. Konsekvensen er, at du risikerer, at private oplysninger sendes fra din maskine uden din viden. Typisk vil de data, der opsamles af spywareprogrammer omhandle dine internetvaner – hvor du surfer, hvor du kommer fra, hvilken version af Windows du kører, hvilken anden type software du har installeret osv.

De indsamlede oplysninger bliver solgt videre til en tredjepart og bruges typisk til markedsføringsmæssige formål. Spyware-programmer er tit tavse og trives bedst ubemærket. De skal danne sig et billede af dig som forbruger og har derfor en interesse i at ligge på dit system længst muligt.

Adware

En anden type uønsket software, man risikerer at møde på pornosider, er adware. Her er der tale om reklamer, der popper op på alle mulige tidspunkter. Ofte åbner adware software for flere reklamer, så systemet til sidst bliver så over-

dænget, at det stort set ikke kan anvendes. Svar altid nej til pop-ups, som vil auto-installere programmer med indhold, du ikke kender.

Kædebrev

Du har sikkert prøvet at modtage en sjov film, som er blevet videresendt til dig af én i din vennekreds. Som de fleste andre har du sikkert også prøvet at sende den videre til flere af dine venner, for at de også skal få en sjov oplevelse. Men er du opmærksom på, at de fleste kædebrev indeholder en historik over, hvem der har modtaget og sendt e-mailen videre. Du kan ved at optræde på en sådan liste indirekte skade dig selv og firmaets ry. Så slet kædebrevene på arbejdspladsen – bare for en sikkerheds skyld.

Fakta:

Husk, at du som medarbejder repræsenterer din virksomhed, hver gang du er på nettet i arbejdstiden.

Følger du branchens gode råd om it-sikkerhed (se artikel s. 13) er du godt hjulpet - især, hvis du også husker på at beskytte din pc med pauseskærm og password, når du forlader den uden at lukke den ned.

Ordlister

Adware: Program, der samler oplysninger om din internetadfærd, så det bagefter er muligt at sende dig målrettede og påtrængende reklamer.

Antivirusprogram: Program, der fjerner virus fra din pc.

Cache: Midlertidigt lager af sider og billeder, brugeren har set i en browser. Når browseren bevarer de senest viste sider i en cache, undgår du at skulle vente på, at siden hentes igen, hvis du surfer tilbage til et sted, du har været før.

Community: Et samlingssted på internettet. Ofte brugt i sammenhæng med hjemmesider, hvor brugere kan møde hinanden eller hente informationer om et givent emne.

Firewall: Du kan sikre dig mod ubudne gæster på din pc ved at installere en firewall. Den fungerer som et filter på både ind- og udgående trafik mellem din pc og internettet.

Hacker: Person, der tvinger sig adgang til din pc via internettet.

Kryptering: At kryptere er at gøre information ulæseligt for andre end den, indholdet er tiltænkt.

Mellemlaget: En mappe, hvor dine midlertidige internetfiler gemmes.

Phishing: En måde svindlere forsøger at lokke oplysninger ud af dig på, uden at du opdager det. Typisk er det en e-mail, hvor afsenderen tilsyneladende er din bank. Her bliver du bedt om at klikke på et link og indtaste dit brugernavn og password. Og nu kan svindleren misbruge dine oplysninger.

Privacy policy: Vilkår der fortæller, hvordan en given virksomhed behandler de oplysninger, f.eks. navn, adresse, telefonnummer og lignende, du giver ved oprettelsen af f.eks. en fototjeneste.

Server: En computer på internettet, der kan give dig adgang til andre computere og mulighed for at hente informationer fra den eller sende informationer til den.

Spam: E-mails, som er uønskede for modtageren. De er ofte sendt via andre mailservere ude i verden og kan være svære at spore tilbage til afsenderen.

Spim: Spam, der sendes over din instant messenger f.eks. MSN Messenger, ICQ og lignende.

Virus: Den samlede betegnelse for små ondsindede programmer, der spreder sig via internettet.

Spyware: Program, der kan opsnappe adgangskoder samt andre personlige oplysninger og sende dem til programmets skaber, som i værste fald kan låse sig ind i din netbank.

Trojansk hest: Virus eller spionprogrammer, der er overført til din pc – typisk med små gratis spil eller programmer. Når den trojanske hest ligger på pc'en, sender den oplysninger til skaberen af programmet. Det kan f.eks. være om certifikater, adgangskoder eller internetadfærd.

Støder du på andre internetbegreber, du ikke kender, kan du slå dem op i TDC Onlines internetordliste på www.tdconline.dk/kursus

Test dig selv

Har du styr på sikkerheden? Se hvor mange spørgsmål, du kan svare rigtigt på.

- 1.** Hvad er det klogeste at gøre, når du modtager en spam-e-mail?
- a** Skriv til afsenderen, at du ikke vil modtage mere fra vedkommende
- b** Tryk på eventuelle links i e-mailen for at afmelde den
- c** Slet den omgående
- 2.** Ét af de vigtigste sikkerhedsråd er:
- a** Hold al software på din maskine opdateret
- b** Hold dit tekstbehandlingsprogram opdateret
- c** Hold din indbakke opdateret
- 3.** Hvad er en sikkerhedskopi?
- a** En kopi af vigtige dokumenter printet på papir
- b** En kopi af vigtige dokumenter på din pc's skrivebord
- c** En kopi af vigtige dokumenter på cd-rom, dvd eller usb-nøgle
- 4.** Børnepornofileret dækker
- a** Hele Sjælland
- b** Alle modembrugere i Danmark
- c** 98 % af Danmark
- 5.** Internetudbydere i Danmark er gået sammen i kampen mod:
- a** Computerspil, ludomani og pyramidespil
- b** Børneporno, virus, hackere, orme og spam
- c** Happy slapping og mobning
- 6.** En phishing-e-mail er:
- a** En e-mail, hvor en ven spørger dig, om du vil med ud at fiske
- b** En e-mail med reklamer for fiskeudstyr, som kan købes billigt online
- c** En e-mail, der forsøger at lokke personlige oplysninger ud af dig
- 7.** Hvad er spim?
- a** Spam på mobiltelefonen
- b** Spam på e-mail
- c** Spam over instant messaging
- 8.** Hvad er en hoax?
- a** En e-mail med en falsk besked om en virus eller lignende
- b** En e-mail, der ikke skulle have været sendt til dig
- c** En e-mail med vigtigt indhold om noget, du skal skynde dig at gøre
- 9.** Hvordan skal du opføre dig med hensyn til vedhæftede filer?
- a** Hvis den kommer fra én, jeg kender, åbner jeg den bare
- b** Hvis den kommer fra én, jeg ikke kender, skal jeg ikke åbne den
- c** Jeg skal altid være på vagt over for vedhæftede filer – uanset hvem de kommer fra
- 10.** Hvad er et godt password?
- a** Ét med flere specialtegn og på mindst 8 tegn
- b** Ét som både jeg og min familie nemt kan huske
- c** Mit navn eller børnenes navn er godt
- 11.** Samarbejdspartnerne omkring børnepornofilteret er:
- a** Red Barnet, Rigspolitiet og internetudbydere
- b** Disney og Rigspolitiet
- c** Røde Kors og internetudbydere
- 12.** Hvad er Digital Signatur?
- a** Det er mit navn, der står i bunden af en e-mail
- b** Dit digitale visitkort på internettet
- c** Din autosignatur
- 13.** Er det en god idé med en pauseskærm med password på pc'en?
- a** Ja, så kan andre ikke få adgang til min pc, når jeg er væk
- b** Nej, så er der jo ikke adgang til min pc
- c** Nej, så er der for mange passwords at huske på
- 1.c 2.a 3.c 4.c 5.b 6.c 7.c 8.a 9.c 10.a 11.a 12.b 13.a
- Hvor mange rigtige havde du?**
- 0-3:** Gå omgående hen til din computer. Find stikket til internettet og træk det ud. Hvis du stadig har returret på pc'en, så benyt den. Eller få styr på internetsikkerheden!
- 4-7:** Grib telefonen. E-mail-kontakt er ikke sikker for dig. Få én til at komme hjem til dig og være der, når du går på nettet, og se så at blive bevidst om internettets faldgruber.
- 8-11:** Det er ikke så ringe. Du kan godt bevæge dig ud på internettet på egen hånd. Husk at tage din kritiske sans med dig hver gang.
- 12-13:** Hurra hurra tillykke. Du har styr på it-sikkerhed og bruger din sunde fornuft. Bliv ved med det!

vi støtter



habbohotel.dk



kom nærmere

