

@visen

netsikker nu!

Oktober 2007

Alder ingen hindring

Flere og flere seniorer tager internettet til sig. De har nemlig opdaget, at internettet byder på et utal af muligheder. Derfor sætter denne udgave af netsikker nu! især fokus på ældre og internet, læs også hvordan du færdes mere sikkert på nettet. **11**



4 trin til en sikker pc

Undgå virus, hackere og spionprogrammer. Se, hvordan du nemt garderer dig mod de værste angreb. **8**

Fra Korsbæk til computer

Kurt Ravn er garvet netbruger og har tilmed sin egen hjemmeside. Læs, hvad "Røde" fra Matador bruger nettet til og hvorfor han synes, det er vigtigt at følge med i internettets udvikling. **3**



netsikker nu!

Udgivet af Videnskabsministeret og en lang række eksterne partnere for at sætte fokus på sikker adfærd på internettet. I år henvender kampagnen sig til de seniorer, der gerne vil have mere viden om nettet.

Digital Signatur

Brug den digitale signatur når du vil i kontakt med det offentlige, se dine sundhedsdata, underskriv dokumenter eller udfyld blanketter direkte på nettet. **12**

Muldyr ved et tilfælde

Hold dig væk fra tilbud på nettet om at tjene lette penge. Det kan i værste fald ende med en tur i fængslet. **5**

Surf på nettet med sund fornuft

Gratis mobiltelefoner fra Nokia? 10.000 dollars for en minimal arbejdsindsats? Lyder det for godt til at være sandt, så er det sikkert løgn. Her er fem gode råd, der gør det nemt at styre uden om nettets faldgruber.

Af Kristian B. Bilenberg, TDC

Nettet er fyldt med gode oplevelser og nyttige sider. Men det er også et eldorado for svindlere, der jager godtroende brugeres penge. Heldigvis er det stadig nemt at slippe uden om langt de fleste svindelnumre, hvis du tænder for den sunde fornuft, inden du tænder for pc'en. Kombineret med opdateret software og antivirus på pc'en er du dermed godt rustet til at surfe sikkert.

1

Brug din kritiske sans

Virker noget for godt til at være sandt, skal din kritiske sans slå alarm. Løfter om gratis mobiltelefoner og hurtig økonomisk gevinst er eksempler på e-mails, du bare skal slette med det samme. Vær især på vagt, når du modtager e-mails på engelsk, fra ukendte personer eller med vedhæftede filer. Husk, at de fleste virusser automatisk forfalsker afsenderadressen i en e-mail. Derfor kan det være et faresignal, hvis du modtager e-mails på engelsk fra en, du kender.

2

Er du i tvivl, så slet eller luk

Når din kritiske sans har spottet en fare, er der ikke meget at betænke sig på: Slet omgående den mistænkelige e-mail. Eller forlad hjemmesiden, hvis det er på nettet, dine mentale advarselslamper blinker.

3

Vær kritisk over for advarsler

Mange netvindlere bruger frygten som løftestang, når de vil lokke godtroende internetbrugere. Derfor skal du være kritisk over for advarsler på nettet. Drivecleaner og ErrorSafe er eksempler på fup-firmaer, der popper op på mange hjemmesider og fortæller, at der er noget galt med din pc. (Se mere på side 6). Installerer du deres testprogram, bliver din pc langsom. Efterfølgende tager de sig betalt for at fjerne de problemer, de selv har skabt. Du kan tit spotte svindlerne på et lidt ubehjælpeligt dansk. Samtidig vil en Google-søgning på navnet næsten altid afsløre fupfirmaerne.

4

Afslør den falske hjemmeside

Svindlere sender nogle gange falske e-mails fra afsendere, du stoler på – eksempelvis din netbank. I e-mailen opfordrer de dig måske til at indtaste følsomme oplysninger – et fænomen, der kaldes phishing. Er du i tvivl, om e-mailen er ægte, skal du kontakte den påståede afsender. Du kan ofte selv afsløre svindlerne ved at holde øje med adressefeltet i din Internet Explorer. Tjek, hvad der står umiddelbart til venstre for ".dk". Det skal være et hjemmesidenavn, du stoler på, ellers er der noget galt. Du kan altid tjekke hjemmesidens ejer på www.dk-hostmaster.dk.

5

Vær på vagt, når det handler om penge

Du skal aldrig udlevere dankortoplysninger, personnummer, pinkoder, adgangskode osv. i e-mail eller på nettet. Selvfølgelig er det ok at indtaste dankortoplysninger og personnummer, hvis du handler på nettet eller er ved at melde dig selv som organdonor. Det kræver dog, at du stoler på siden, og at hjemmesidens adresse begynder med "https". S'et viser, at hjemmesiden bruger en sikker protokol til at overføre data.

Fakta:

Fire af nettets største farer

1. Skadelige vedhæftede filer i e-mails.
2. Falske e-mails, der lokker oplysninger ud af dig.
3. E-mails, der lokker med gratis mobiltelefoner eller hurtig gevinst.
4. Falske pop up-advarsler, der spiller på din frygt for virus og netvindlere.

Klip ud og gem
i nærheden af din computer.
Så har du de gode råd
ved hånden, næste gang
du er i tvivl om,
hvorvidt du er i fare for
at blive snydt
på nettet.

Med Kurt på internettet

Af Anders Frederik Gjesing, PBS

Vi kender ham som "Røde" i Matador, fra de skrå brædder i musicals og fra utallige koncerter. Men mange ved sikkert ikke, at Kurt Ravn siden 1999 faktisk også har været en garvet bruger af internettet.

Kurt Ravn indrømmer blankt, at han var lidt forsigtig med at hoppe med på vognen og begive sig ud på internettet for otte år siden.

"Jeg var nok lidt påpasselig i starten, og jeg tænkte, at det var svært og besværligt. Men i dag er jeg jo lykkelig for at have computeren og adgang til internettet", fortæller Kurt Ravn. Han er nu en erfaren bruger af internettet og har således både købt rejser, kamera og musik på internettet. Og så ordner han stort set alle sine bankforretninger i netbanken.

Sparer tid og penge

"Jeg sparer jo både tid og penge, når jeg bruger internettet. Det bedste er, at jeg i ro og mag derhjemme kan sammenligne priser og finde de bedste tilbud. Og så har jeg jo fundet ud af, at jeg som forbruger er rigtig godt sikret, når jeg bruger mit Dankort på nettet", siger Kurt Ravn.

Samtidig bruger han også internettet til at sende og modtage post: "Med e-mailen slipper man for den langsommelige postgang. Beskeden er fremme hos modtageren med det samme, så det er jo næsten som at føre en samtale over internettet. Jeg bruger derfor dagligt internettet til at sende e-mails, både privat og i forbindelse med mit arbejde", fortæller Kurt Ravn. Frimærkerne og konvolutterne får derfor lov til at samle støv hjemme hos ham. Det sker dog af og til, at han sender et rigtigt brev.

"For det er trods alt noget andet og måske en anelse mere personligt", som han siger.

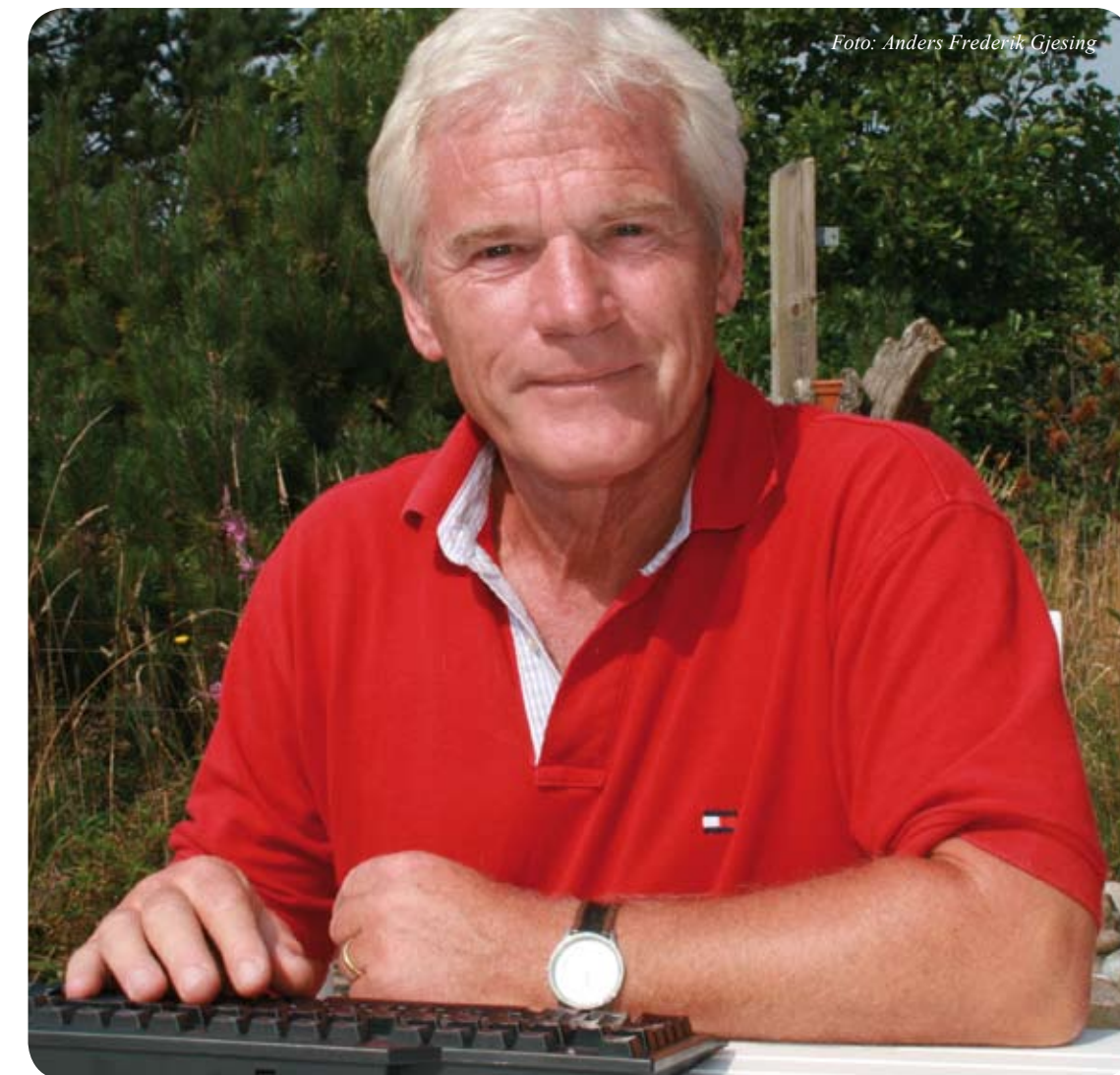


Foto: Anders Frederik Gjesing

Kurt Ravn har været på nettet i 8 år, og nu har han også fået sin egen hjemmeside.

Fakta:

Kurt Ravn

Kurt Ravn er født i 1947, og han blev uddannet på Statens Teaterskole i starten af 70'erne. Det store folkelige gennembrud fik han i rollen som "Røde" i Matador. Siden har Kurt Ravn haft utallige roller på teatre, i musicals samt på film og i tv. Han turnerer ligeledes land og rige rundt med kirke- og julekoncerter. Du kan læse mere om Kurt Ravn, hans koncerter og cd-udgivelser på hjemmesiden: www.kurtravn.dk

Tryghed på internettet

Kurt Ravn føler sig grundlæggende tryk, når han bruger internettet.

"Du skal jo bare tænke dig om, når du færdes på nettet. Jeg åbner ikke mistænkelige e-mails eller handler i internetforretninger, der ikke virker troværdige", fastslår Kurt Ravn.

Når regningerne skal betales eller saldoen tjekkes, bruger Kurt Ravn sin netbank. Og det gør han med ro i sindet.

"Jeg er tryk ved, at bankerne har styr på sikkerheden. Og det letter jo min hverdag gevaldigt, at bankforretningerne kan

ordnes hjemmefra uden skelen til åbningstider og kø ved kassen. I virkeligheden er det jo også ret nemt, når man først er kommet i gang", siger Kurt Ravn.

Børnebørnene er foran

AI begyndelse er svær. Men Kurt Ravns opfordring lyder, at du bare skal kaste dig ud i at bruge internettet. Hvis du bruger din sunde fornuft, venter der dig mange gode oplevelser, og du behøver ikke at være ekspert for at være sikker på nettet.

Det var sådan, Kurt Ravn kom i gang med at bruge internettet. Udgangspunktet var nysgerrighed og lysten til at

prøve nye ting. Men nu er det blandt andet børnebørnene, der kærligt presser Kurt Ravn til at følge med udviklingen.

"Jeg ved, at jeg er nødt til hele tiden at blive bedre til at bruge internettet, for mine børnebørn har jo allerede overhalet mig med flere længder. Så for ikke at virke som en støvet bedstefar, må jeg jo hele tiden sætte mig ind i tingene. Og seneste skud på stammen er, at jeg nu har fået min egen hjemmeside", griner Kurt Ravn.

Se netsikker nu! kampagnefilmen

Er du senior, og føler du dig indimellem overhalet af dine børnebørn på nettet?

Se årets sjove kampagnefilm om, hvordan du kan give børnebørnene baghjul. Klik dig ind på www.netsikkerne.dk og se filmen.

Sikker bank fra stuens bedste stol

Af Rita Modberg, Nordea

Hvorfor stå i kø på posthuset for at betale de månedlige regninger, når man lige så godt kan få det fra hånden derhjemme?

Det spørgsmål besvarer flere og flere danskere ved at oprette en netbank-aftale, som giver mulighed for at klare regninger og bankforretninger over hjemmecomputeren og internettet. For mange handler det om at undgå lang venten og korte åbningstider, mens det for andre i lige så høj grad drejer sig om tryghed. Det bliver nemlig unødvendigt at gå rundt med større pengebeløb på sig, der enten kan tabes eller i værste fald blive stjålet.

Pas godt på din computer
Tryghed på nettet afhænger dog af, at man sørger for at sikre sin

computer. Først og fremmest ved at have et opdateret antivirusprogram, der fanger eventuelle "sygdomme". Men også ved at bruge sin sunde fornuft – f.eks. ved at være varsom med at klikke på links og vedhæftede dokumenter i e-mails som kommer fra en ukendt afsender. Sikkerheden i selve netbank tager banken sig af.

"Et højt sikkerhedsniveau er alfa og omega både for kunderne og banken. Sagen er, at netbankerne altid vil blive udfordret på sikkerheden, og derfor er en konstant udvikling nødvendig", siger Martin F. Andersen, som arbejder med Nordeas Netbank. "Vi har nået et niveau i netbankerne, hvor brugerne kan være trygge ved at gå på nettet. De skal bare følge tommelfingerreglerne for, hvordan de selv sikrer sig".

En kode – flere adgange
Det kræver en personlig adgangskode at gå i netbank. Samme adgangskode kan nu også bruges til at komme ind og læse

egne data på andre hjemmesider f.eks. www.pensionsinfo.dk, www.e-boks.dk eller www.sygeforsikring.dk.

Fakta:

Sådan sikrer du dig selv

- Vær kritisk over for uopfordrede e-mails og ekstra forsigtig med at klikke på bilag og links. Slet e-mailen, når du er i tvivl.
- Slå automatisk opdatering af browser og operativsystem til. Så får du de seneste versioner og dermed den højst mulige sikkerhed.
- Når der er en "hængelås", bliver der sendt krypterede data. Klik på "hængelåsen" og tjek, hvem du kommunikerer med, før du indtaster fortrolige oplysninger.

Læs mere om sikkerhed på www.nordea.dk



Muldyr ['mul,dy'r] en hest, som er en krydsning mellem en æselhingst og en hestehoppe; bruges som ride-, træk- og lastdyr. (Kilde: Nudansk ordbog) I nyere tid: en person, som mod betaling hjælper kriminelle med at overføre stjålne penge til andres konti.

Lokket til

Kriminalitet på nettet

Bliv økonomiansvarlig og tjen lette penge! Hvis du synes, det lyder for godt til at være sandt, så hold fast i den tanke. For højst sandsynlig er der tale om et forsøg på at få dig til at medvirke i en kriminel handling som "muldyr". Eddie Kofoed, nysgerrig internetbruger, har været i kontakt med de kriminelle bagmænd.

Af Rita Modberg, Nordea

I efteråret 2006 stødte Eddie Kofoed fra Aalborg tilfældigt på en hjemmeside for et shippingfirma, som søgte medarbejdere til at modtage pakker eller penge og videresende dem mod betaling. Eddie Kofoeds nysgerrighed fik ham til at besvare ansøgningen, og inden længe modtog han en e-mail med den første opgave. Den handlede ikke om pakker, men om penge.

"E-mailen oplyste, at der var overført godt 80.000 kr. til min konto, og at jeg skulle videresende beløbet i to eller tre bidder til forskellige adresser i Rusland via MoneyGram eller Western Union. For min ulejlighed ville jeg få fem procent af beløbet, dvs. lidt

mere end 4.000 kr.", fortæller Eddie Kofoed.

Mistanke om, at transaktionerne ikke var helt stuerene, fik ham straks til at kontakte sin bank. Her fandt man frem til, at pengene kom fra en mindre erhvervsdrivende på Roskildeegnen, som altså uden at vide det var blevet 80.000 kr. fattigere.

Endnu et læs til "muldyret"

Og inden de kunne nå at sige ordet politi, var den allerede gal igen. Et tilsvarende stort beløb blev sat ind på Eddie Kofoeds konto, denne gang penge fra en jysk idrætsforenings netbank-konto, og nu blev både bank og politi inddraget. De sørgede for, at pengene gik tilbage til rette

ejermand og overtog desuden Eddies kononummer til brug i den videre efterforskning. "Bagmændene kommer ind i folks netbank ved at sende dem en e-mail med en vedhæftet fil. Når modtagerne klikker på virus ind i deres pc, der giver adgang til deres personlige data", forklarer Philippe Roy, risk manager i Nordeas Netbank. "Bagmændene arbejder meget professionelt og giver et tillidsfuldt indtryk på deres hjemmesider og i e-mails. Så folk tror på, at det er et regulært job, de får stillet i udsigt, men mit råd er helt klart at holde sig væk fra tilbud om at tjene lette penge. De findes simpelthen ikke", slår han fast.

Han slap med skrækken
Jobbet som "muldyr" er kriminelt, og i flere tilfælde er der sket anholdelser, når personen er dukket op i sin bank for at hæve de overførte penge. Netop pengeoverførsler er lette at spore og risikoen for afsløring stor. "Muldyret" kan sigtes for hæleri, der i værste fald giver op til 6 års fængsel. Eddie Kofoed gjorde således det eneste rigtige i situationen, som da heller ikke har fået nogen konsekvenser for ham.

Fakta:

Undgå at blive "muldyr"

- Vær på vagt, hvis nogen du ikke kender, opfordrer dig til – mod betaling – at hjælpe med at overføre penge til andres konti.

- Opfordringen til at hjælpe kan være udformet som et jobtilbud på internettet eller komme via en e-mail.

- Behovet for hjælp forklares f.eks. med, at det i nogle dele af verden er meget dyrt eller helt umuligt at overføre penge mellem konti.

Ordlister

Adware: Program, der samler oplysninger om din netadfærd, så man kan sende dig målrettede og påtrængende reklamer.

Antivirusprogram: Program, der fjerner virus, orme og trojanske heste fra din pc.

Browser: Et program til at vise hjemmesider på internettet. Den mest kendte browser i dag er Microsoft Internet Explorer.

Chat: En internettjeneste, hvor brugerne kan kommunikere direkte med hinanden online.

Download: Hente en fil fra nettet for at gemme den lokalt på egen pc. Modsætningen til download er upload, dvs. at lægge noget op på serveren.

E-mail/e-post: Den elektroniske version af normal post. Postforsendelsen foregår imellem computere på internettet eller i mindre netværk.

E-mail-adresse: En e-mail-adresse kan f.eks. se sådan ud: navn@firma.dk (udtales: navn snabel-a firma punktum dk).

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 over nettet.

Internettet: Globalt netværk af pc'ere, der er koblet

sammen i et netværk, hvor der er mulighed for at hente, sende og dele informationer.

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

Orm: En slags virus, der kan kopiere sig selv automatisk fra pc til pc. Orme kan fjernes med de fleste antivirusprogrammer.

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

Privacy policy: Vilkår for hvordan en virksomhed behandler oplysninger som navn, adresse, telefonnummer og lignende ved oprettelsen af f.eks. en tjeneste.

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

Spam: E-mails med reklamer som er uønskede. De er ofte sendt via andre e-mail-servere ude i verden og kan være svære at spore tilbage til afsenderen.

Spamfilter: Minimerer risikoen ved spam e-mails. Gennemser e-mails inden de kommer i indbakken og

fjerner spam efter opsatte regler.

Trojansk hest: Virus eller program, der udgiver sig for at være noget, men i virkeligheden er noget andet. Oftest spredt via e-mail.

Upload: Flytte en fil fra egen pc ud til en anden pc på internettet.

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

WWW: Forkortelse for World Wide Web.

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

Vælg den rigtige hjælp på nettet

Advarslens dukker pludselig op på skærmen: "Din pc er muligvis i fare, klik her". Det lyder umiddelbart som et godt tilbud, men kan i virkeligheden være en grim fælde, der først for alvor giver dig problemer, hvis du følger anbefalingen og klikker.

Af Torben B. Sørensen, Computer for alle

Der findes gode muligheder for at få testet sin pc for virus på nettet. Vi fortæller dig, hvordan du kan lære at se forskel, selv om de ligner hinanden til forveksling.

De rigtige scannere

De rigtige online scannere er tjenester, der finder og fjerner skadelig software på din pc. Online scannere fungerer lige som almindelige antivirus- og antispywareprogrammer – de ligger bare på nettet i stedet for på din pc. Og de er tilmed helt gratis at bruge. Virus. Spyware. Orme. Trusler er der nok af. Forskellige typer skadelige programmer kan genere dig i hverdagen, hvis du er så uheldig at blive ramt af

dem. Som regel kan et antivirusprogram på pc'en holde skadede fra døren. Men hvad nu, hvis du bliver ramt af en ny trussel, som programmet ikke beskytter mod endnu? Eller hvis du slet ikke har installeret antivirus? Så er der hjælp at hente på nettet. Mange antivirusproducenter tilbyder gratis online udgaver af deres programmer. Du bruger dem typisk ved at besøge en hjemmeside, som giver dig adgang til at scanne din pc for skadelige programmer. Alle antivirusprogrammer er ikke lige gode. Nogle kan genkende virus, som andre endnu ikke har opdaget. Derfor kan det være en god idé at benytte flere antivirus-

programmer. Her er online scannere nyttige, idet du kan bruge flere programmer ganske gratis.

Kør flere antivirusprogrammer samtidig

Det tager dog nogen tid at køre en fuld virusscanning. Hvis du har modtaget en enkelt fil, som du frygter, kan du tjekke den på en lang række antivirusprogrammer på én gang. På webstedet Virustotal kan du på én gang bruge 25-30 forskellige antivirusprodukter.

Pas på spionsoftware og trojanske heste

I Homers fortælling om den trojanske hest, gemmer en flok græske soldater sig inde i en stor hest af træ. Trojanerne opfatter hesten som en gave, og ruller den ind i deres borg. Om aftenen springer soldaterne ud og går i gang med at angribe trojanerne.

Metoden har siden lagt navn til en type skadelig software. En trojansk hest i software er altså et program, der giver sig ud for at være nyttigt og uskadeligt, men som i virkeligheden kan volde skade.

Fleere af producenterne af skadelig software lader som om, deres programmer er nyttige. Nogle af dem er ligefrem forklædt som online scannere. De giver sig ud for at være programmer, der bekæmper skadelig software, men i virkeligheden er de selv skadelige. De er trojanske heste.



De falske reklamebannere giver sig ud for at gøre det samme som en online scanner. Men i virkeligheden scanner de ikke din pc, de er enten reklamer for dyre og dårlige sikkerhedsprodukter, eller de installerer uønskede programmer på din pc. De værste af slagsen er endda rene virusspredere.

Klik ikke før du er sikker

Du har måske allerede mødt en falsk online scanner, når du har surfet på nettet. De dukker som regel op med en besked om, at din pc har et alvorligt sikkerhedsproblem. Du bliver opfordret til at klikke på en knap for at løse problemet. Det er forskelligt, hvor skadelige de falske online scannere er. Ofte finder de angiveligt en stor mængde sikkerhedsproblemer, når man kører en scanning.

De oplyser så, at den eneste løsning på problemet er at købe og installere et bestemt program. Det kan godt være et rigtigt antivirusprogram, men det vil som regel være så dårligt, at det ikke er pengene værd. Og de trusler, scanningen har fundet, er fri fantasi. Hvis du vil være på den sikre side, skal du i stedet besøge en ægte online scanner og tjekke din pc der. Du vil sikkert opdage, at der ikke er nogen fare på færde.

Fakta:

Online scannere, du kan stole på:

- BitDefender: www.bitdefender.com - Klik på "scan online"
- Kaspersky: www.kaspersky.com/virusscanner - Klik på "kaspersky online scanner"
- McAfee: dk.mcafee.com/root/mfr/default.asp (uden www)
- Panda: pandasecurity.com/activescan (uden www)
- Trend Micro: housecall.trendmicro.com (uden www)

Sådan tjekker du en mistænkelig fil for virus:

Åbn din internetbrowser og besøg www.virustotal.com
Klik på knappen "Gennemse..."
1. Vælg den fil, du har mistanke til, og klik på knappen "Send"

2. Så bliver filen sendt op til webstedet, hvor den bliver lagt i kø til at blive tjekket af en lang række antivirusprodukter. Lidt senere dukker analyseresultaterne op på skærmen.



Ekstra sikkerhed

Fleere og flere danske og udenlandske butikker er gået over til at benytte en yderligere kontrol af betalingskortets ægthed for at hæve sikkerheden yderligere. Derfor kan du opleve, at du ved betalinger med VISA og MasterCard bliver viderestillet til din netbank, hvor du skal indtaste koden

til netbanken. Dette er et ekstra sikkerhedsэлемент, der kaldes "Verified by VISA" og "MasterCard SecureCode". Desuden har PBS lanceret eDankort, hvor betalingen finder sted via netbanken. Internetforretninger, der har de ekstra sikre løsninger, skiller med disse logoer.



på internettet!

Sikker handel

- kort og godt

Det er nemt, sikkert og hurtigt. Så der er ingen grund til at lade være med at handle på nettet, hvis du blot udviser lidt snusfornuft. Og fordelene er til at få øje på: Udvalget af varer er uendeligt, konkurrenternes priser kan tjekkes på skærmen og varerne bliver leveret lige til døren.

Af Anders Frederik Gjesing, PBS

Vil du have fremkaldt billeder fra den seneste familiefest eller købe en autostol til barnebarnet, så kan du finde gode tilbud på internettet. I ro og mag hjemme foran computeren kan du handle uden stress og jag - og det er faktisk ganske sikkert. Samtidig kan du spare både tid og penge.

Som i alle andre forhold i livet, så skal du alligevel lige tænke dig om, inden du kaster dig ud i at købe varer på internettet. Men følger du et par enkelte gode råd, så er du som forbruger i Danmark faktisk stillet utroligt godt. Det sørger den danske forbrugerlovgivning for.

Sund fornuft

Langt de fleste danske betalinger på nettet behandles af PBS. Og her siger direktør Johnny

Bennedsen: "Det er egentligt ganske simpelt. Man skal kun handle i butikker på nettet, som man har tillid til. Lad derfor være med at handle i net-butikker, der ikke oplyser salgs- og leveringsbetingelser, der ikke oplyser kontaktsadresse eller bare ikke virker troværdige. Man skal med andre ord huske at bruge sin sunde fornuft på internettet".

Forbrugerrettigheder

Som dansk forbruger er du godt stillet, når du handler på internettet. Som hovedregel har du som forbruger 14 dages fuld returret for varer, du køber i en dansk internetbutik. Betaler du varerne med Dankort, kan din bank tilbageføre beløbet til din konto, hvis du mod forventning ikke modtager de bestilte varer.

Det gælder også, hvis butikken går konkurs, inden du har modtaget varen. I den situation er du derfor bedre stillet ved betaling med Dankort end ved en bankoverførsel, der normalt ikke kan fortrydes.

Ekstra sikkerhed

Direktør Johnny Bennedsen understreger, at det er vigtigt kun at udlevere betalingskortoplysninger i forbindelse med en egentlig betalingssituation. Og man skal aldrig oplyse sin firecifrede pinkode.

Ved betaling med VISA og MasterCard kan du i enkelte tilfælde opleve, at du bliver viderestillet til din netbank, hvor du skal indtaste koden til netbanken. Det skal du ikke blive urolig over - det er et

Fakta:

Forbrugerrettigheder

Køber du varer på nettet i en dansk internetbutik, så har du som forbruger som hovedregel 14 dages fortrydelsesret. I de 14 dage er det tilladt at afprøve varen, så længe, den returneres i "væsentlig samme stand og mængde", som reglerne fastslår. Undtaget herfor er dog varer som eksempelvis musik cd'er,

computerprogrammer og varer fremstillet på bestilling efter mål. Hvis bestilte varer ikke dukker op, kan banken tilbageføre pengene til din konto.

Læs mere om dine rettigheder på Forbrugerstyrelsens side: www.net-tjek.dk

ekstra sikkerhedsэлемент, som kaldes "Verified by VISA" og "MasterCard SecureCode". Desuden har PBS lanceret eDankort, hvor betalingen også finder sted via netbanken.

Du kan læse meget mere om dine rettigheder som forbruger på Forbrugerstyrelsens side på www.net-tjek.dk

Nettets fire alvorligste trusler

Fire trin til en sikker pc

Af Torben B. Sørensen,
Komputer for alle og
Lauritz Hansen,
Bullguard

Vi gennemgår fire af de mest udbredte trusler på nettet. Det kan måske lyde skræmmende – men til gengæld skal der også kun fire forholdsvis overskuelige sikkerhedsforanstaltninger til for at blive garderet mod de værste ulykker.

Din pc kan, uden at du ved det, være under en andens kontrol. Den kan deltage i ulovlige aktiviteter eller sende i bunkevis af spam e-mails af sted, uden at du aner det. Det kan også være, at dine private ferie billeder eller

musikfiler på pc'en er ved at forsvinde sporløst. Så alvorlige kan konsekvenserne være, hvis pc'en bliver ramt af en virus, trojansk hest eller en af de andre trusler, du kan støde ind i på nettet.

Her gennemgår vi fire af de mest udbredte trusler på nettet: Virus (herunder e-mail-orme og trojanske heste), phishing/spam, spyware og hackerangreb. Du får at vide, hvad hver enkelt trussel egentlig betyder, hvad den kan gøre

ved dig og din pc, hvordan den spreder sig, og vigtigst af alt: Hvordan du undgår den. Vi giver dig også links til programmer og værktøj, der beskytter dig mod truslerne. Selv de bedste sikkerhedsprogrammer kan imidlertid ikke

beskytte dig effektivt, hvis du selv lukker truslerne ind. Det vigtigste middel i kampen for bedre netsikkerhed er derfor din sunde fornuft: Optræd varsomt, når du er på nettet. Hent kun programmer fra hjemmeside, du har tillid til. Og dobbeltklik

aldrig på filer eller links i en e-mail, du får tilsendt uopfordret eller vedhæftede filer, hvis indhold du ikke er 100 pct. sikker på at kende.

Gratis TDC Sikkerhedspakke

Lige nu kan du få en TDC Sikkerhedspakke gratis på prøve i 60 dage. Sikkerhedspakken beskytter din computer med firewall, antivirus, antispysware og forældrestyring.

Download dine prøveversion inden 1. december 2007 på: www.tdc.dk/netsikker

1

Virus, e-mail-orme og trojanske heste

Mange skadelige programmer ankommer i form af uskyldigt udseende e-mails. Det er de såkaldte e-mail-orme. Måske kender du afsenderen – eller det tror du i hvert fald, for e-mail-ormene kan i visse tilfælde forfalske afsenderadressen! E-mailen indeholder ofte en vedhæftet fil, som teksten opfordrer dig til at klikke på. Det skal du ikke gøre, heller ikke selvom den vedhæftede fil ligner et billede eller et uskyldigt videoklip. I virkeligheden er den nemlig program, der inficerer din pc. Programmet sender så sig selv videre til alle adresser, den finder i din pc's adressekartotek. På den måde er du med til at sprede ormen videre til dine

venner. Ormeprogrammet kan også give en hacker mulighed for at fjernstyre din pc, så han kan bruge den til at udsende spam eller angribe andre pc'er.

De nyere e-mail-orme kan være svære at kende, for de indeholder slet ikke vedhæftede filer. I stedet har de et link til en hjemmeside. Et klik på linket kan føre til, at du bliver spurgt, om du vil hente og køre et program. Det skal du altid svare nej til. I værre tilfælde bliver du slet ikke spurgt. Så udnytter hjemmesiden f.eks. en sikkerhedsbrist i Internet Explorer til at installere et skadeligt program, helt uden at du opdager det. Du kan mindske risikoen ved at slå funktionen

"Automatiske opdateringer" i Windows til, så du altid har den nyeste version med de seneste rettelser af programfejl.

Klassisk virus spreder sig ved at inficere programfiler. De er ikke længere særlig udbredte. I stedet er der mange trojanske heste på spil. Det er programmer, der giver sig ud for at være nyttige, men som i virkeligheden er skadelige.

Antivirus

Et antivirusprogram beskytter pc'en mod at blive ramt af virus, orme og trojanske heste. Er du ramt, kan et antivirusprogram også fjerne infektionen. Programmet har den svaghed, at de som regel kun fjerner virusformer, som de kender. Derfor skal et antivirusprogram opdateres med nye typer virus mindst en gang om dagen.

Antivirusprogram:
www.bullguard.dk
www.tdc.dk/netsikker
Links:
www.microsoft.dk/windowsupdate

2

Spyware og adware

Spyware (spionprogrammer) er programmer, der ændrer på din pc's opsætning mod din vilje. F.eks. kan spyware give Internet Explorer en ny startside (ofte desværre af den meget mindre pæne slags). Egentlige spionprogrammer er f.eks. tastaturnusere, der så at sige aflytter dine tastetryk og sender data til en hacker. På den måde kan han finde frem til dine brugernavne og adgangskoder. Sidstnævnte slags ser man heldigvis meget sjældent i brug. Spyware spreder sig ved hjælp af trojanske heste,

der narrer dig til at installere spyware i den tro, at du får et nyttigt program ud af det. Ofte anvender spyware også sikkerhedshuller i browsere til at sprede sig med. Så risikerer man at få spyware på pc'en, blot fordi man besøger en hjemmeside. Adware er annoncefinsierede programmer. Nogle reklamerer med, at du får programmet gratis, mod at du accepterer at se dets annoncer. Andre sniger sig ind på pc'en i form af trojanske heste eller ved at udnytte programfejl og

sikkerhedshuller. Så dukker der pludselig en mængde pop-op-vinduer med reklamer op på skærmen.

Antispysware

Du kan undgå at blive ramt af spyware, hvis du er forsigtig med at hente og installere programmer fra hjemmesider. Du kan installere et anti-spyware- eller antiadware-program. Også her er det vigtigt at holde pc'en opdateret mod nye typer af adware og spyware op.

Antispyswareprogram:
www.bullguard.dk
www.tdc.dk/netsikker

3

Phishing og spam

Phishing er navnet på en form for svindel, der er blevet uhyre udbredt de senere år. Phishing er en lidt omskrevet variant af det engelske ord fishing, som betyder at fiske. Et phishing-angreb starter med, at du modtager en e-mail, der angiveligt kommer fra f.eks. din bank. I e-mailen står der måske, at du af sikkerhedsgrunde skal bekræfte dine brugeroplysninger. E-mailen indeholder så et link, som du opfordres til at klikke på. Hvis du klikker på det, kommer du til en hjemmeside, der ligner bankens til forveksling. Her kan du indtaste brugernavn, kontonumre, adgangskode og andre fortrolige oplysninger. Men gør det ikke! De går direkte videre til phishing-svindlerne. Hjemmesiden er nemlig en forfalskning. Phishing-

svindlerne går gerne efter hjemmesider for banker, auktionshuse, netbutikker og andre steder, hvor der er penge eller andre værdier at hente. Spam er sådan set ikke en egentlig trussel mod din pc-sikkerhed, men er bare meget irriterende. Spam er e-mails med reklamer, der forsøger at få dig til at købe alverdens ting. Ofte er varerne ulovlige – det kan være piratkopier eller medicin, der ikke er godkendt i Danmark. Hvis man køber dem, løber man også en risiko for, at ens kreditkortoplysninger bliver misbrugt. Det kan også være, at der slet ikke er noget at købe. Masser af spam har kun til formål at hoste e-mail-adresser for så at sælge disse til nye spam-sendere.

Toolbars og spamfiltre

Phishing handler ikke om teknik, men om tillid. Derfor er det bedste middel heller ikke et produkt men sund skepsis: Hvis du modtager en e-mail med et link til din bank, skal du ikke klikke på linket. Gå i stedet ind i din browser (f.eks. Internet Explorer) og indtast adressen eller vælg den fra dine bogmærker. Så bliver du ikke ført hen til en forfalsket hjemmeside. Endvidere findes der værktøjsbjælker (toolbars), der giver et bud på, hvor pålidelig en hjemmeside er. Dem kan du også støtte dig til.

Mange internetudbydere tilbyder at fjerne spam automatisk. Ellers kan du bruge et spamfilter som f.eks. det danske program Spamfighter. Lige meget hvad du gør, er der

dog en vis risiko for at visse "rigtige" e-mail fejlagtigt opfattes som spam og bliver slugt af filteret. Det er den pris, man må regne med at betale for at have en lidt mere ryddelig e-postkasse.

Spamfilter:
www.bullguard.dk
www.tdc.dk/netsikker

4

Hackere og orme

Hackere angriber som regel ved at udnytte sikkerhedshuller i programmer. Når din pc er på nettet, kan enhver anden computer på nettet kommunikere med den. Det udnytter hackerne til at undersøge, om din pc har sikkerhedshuller, de kan udnytte. Det samme gælder orme. Orme er programmer, der automatisk spreder sig til alle computere, der har et bestemt sikkerhedshul. Orme er sjældne,

men når de forekommer, kan de lave megen ravage på meget kort tid. Det skyldes, at de i modsætning til e-mail-orme og virus ikke kræver menneskelig hjælp til at sprede sig tværs gennem hele internettet.

Firewall

En firewall (brandmur) er et program eller en boks, der beskytter din pc mod angreb udefra. Firewallen tillader kun kommunikation, som du selv har taget initiativ til. Et hackerangreb vil derfor ikke få lov til at slippe igennem. Endvidere kan du beskytte dig ved at holde pc'en opdateret med de seneste sikkerhedsrettelser til Windows og andre programmer.

Firewall:
www.bullguard.dk
www.tdc.dk/netsikker
Links:
www.microsoft.dk/windowsupdate

Privatlivets fred

- hvem må vide, hvem du er?

Af Martin H. Nielsen, Ernst & Young



vedrørende indsamling, anvendelse og opbevaring af oplysninger på nettet. Her kan f.eks. nævnes persondataloven og forvaltningsloven.

I EU er virksomheder - ud over national ret - også omfattet af bl.a. Europa Parlamentets og Rådets direktiv 95/46/EF om databeskyttelse. På Europa-Kommissionens hjemmeside findes en liste over en række tredjelande - som uden for EU er vurderet til at have et højt beskyttelsesniveau. At listen er kort og pt. kun består af USA, Canada (begge dog med visse begrænsninger), Schweiz, Argentina, Isle of Man og Guernsey gør, at du som bruger skal være opmærksom på, hvilke hjemmesider du frivilligt afgiver personlige informationer til, og fra hvilke lande de kommer.

Kun nødvendige oplysninger

Det er derfor ikke lige meget, hvor og hvordan du giver dig til kende på nettet. Hvis du skal handle og afgive oplysninger om dig selv så brug nogle minutter på at undersøge, hvad virksomheden gør for at beskytte dine oplysninger. Du skal stille spørgsmålstegn ved, om de oplysninger, du giver, er nødvendige for dem, der indsamler dem. Skal du for at læse et nyhedsbrev virkelig give privatadresse, telefonnummer eller lignende? Du skal bruge din sunde fornuft. Giv dig til kende, når det er nødvendigt, og er du i tvivl om kvaliteten af den hjemmeside, du besøger, så lad tvivlen komme dig selv til gode.

Love og regler

I Danmark er virksomheder og offentlige institutioner omfattet af en række love



Helt trådløs - helt sikker

Er dit trådløse netværk ubeskyttet? Så risikerer du, at din forbindelse misbruges til it-kriminalitet - og at sporene peger på dig. Heldigvis kan du selv gøre meget for at lukke de it-kriminelle ude.

Af Kristian B. Bilberg, TDC

Har du én gang siddet i sofaen med din bærbare pc og surfet rundt på nettet helt uden ledninger, så er du sikkert enig i, at trådløst internet er kommet for at blive. Men med følelsen af frihed følger også en række risici. For når du kobler dig på netværket trådløst, risikerer du, at gratister og it-kriminelle følger lige i hælene på dig. Din opgave er at gøre livet så surt for dem, at de vælger et andet netværk at udnytte.

Farer ved åbne netværk

Men hvorfor overhovedet bruge tiden på at beskytte sit netværk? Her er de tre bedste grunde til at holde andre ude fra sit trådløse netværk:

1. Uvedkommende kan lave kriminalitet på dit netværk. De kan f.eks. distribuere børneporno eller bestille

dyre computere - alt sammen fra din netforbindelse, så sporene peger på dig.

2. Slipper du andre ind på netværket, er de et skridt nærmere din pc og dermed et skridt nærmere din netbank og dine penge.

3. Gratisterne hugger din netkapacitet. Og hvis naboen sidder og suger på din netforbindelse, betyder det mindre hastighed til dig.

Vil du undgå de tre farer, skal du skjule navnet, kryptere trafikken og kun slippe kendte pc'er ind på netværket. Det kan du læse mere om i faktaboksen. Du kan også finde mere hjælp i artikler i Komputer for alle (www.kortlink.dk/3yt4) og på tdc-online.dk (www.kortlink.dk/3yt5).

Åbne netværk kan være en fælde

Husk i øvrigt, at du også udsætter dig for fare, hvis du selv logger dig på andres trådløse netværk. Som en stor skål slik lader nogle hackere deres trådløse netværk være åbent, så du frit kan logge på det og bruge løs af deres båndbredde. Til gengæld aflytter de din maskine og overvåger alt, hvad du foretager dig. Det gælder eksempelvis dine e-mails og din netbank.

Fakta:

Sådan gør du dit netværk sikkert

1. Skjul og omdøb dit netværk

Vil du beskytte dit trådløse netværk, skal du først og fremmest sørge for, at dit netværk ikke dukker op på naboens computer. Det gør du ved at skjule netværkets navn. Samtidig bør du omdøbe netværkets navn, så det er sværere at gætte.

2. Ny adgangskode til routeren

Routeren er det apparat, der styrer trafikken mellem de tilkoblede pc'er og internetforbindelsen. Sørg for at ændre den forudindstillede adgangskode, så det ikke er de samme som alle andre routere af samme mærke.

3. Kryptér trafikken

Sørg for at kryptere trafikken mellem routeren og de tilsluttede pc'er. Så kan du surfe i fred, uden at uvedkommende kigger med.

4. Lad routeren lege dørdame

Indstil routeren, så den kun slipper velkomne pc'er ind. Alle apparater har en unik adresse. Når du fodrer routeren med disse adresser, vil alle andre pc'er blive afvist.

Da konsulenten fik en trojansk hest

63-årig vejleder i Faaborgs nye datastue hjalp Ældremobiliseringens konsulent af med computerproblem.

Af Annette Schiøler, Den fynsk/jyske Sammenslutning af Pensionistforeninger

"Mus, virus, orme og trojanske heste.

Det lyder som noget fra biologi og oldtidstimerne i skolen, men det handler nu om computere - og de tre sidstnævnte ting handler specifikt om (manglende) sikkerhed på computeren. Alene udsigten til at få disse skadedyr inden for dørene får nogle ældre til allerede på forhånd at opgive at lære at bruge en computer - men det er der ikke nogen grund til", fastslår Svend Lyngsø.

Og den 63-årige efterløner ved, hvad han taler om. Som noget af det første som frivillig vejleder i Ældremobiliseringens nye datastue i Faaborg hjalp han Ældremobiliseringens 49-årige konsulent med et computerproblem:

"Jeg kender kun til computere som almindelig bruger og har ikke spor forstand på det tekniske. Så jeg var på den, da min computer begyndte at lukke ned, så snart jeg havde tændt for den. Det irriterede, og det var ikke til at arbejde med", fortæller John Jørgensen, der øjnede mulighed for hjælp, da han mødte Svend Lyngsø til et informationsmøde om den nye datastue.

"Han ville godt kigge på computeren, så jeg afleverede den til ham en tirsdag aften, og allerede onsdag fik jeg den tilbage", husker John Jørgensen imponeret.

Almindelig omtanke og lidt teknik

Svend Lyngsø konstaterede hurtigt, at konsulenten havde fået en trojansk hest i sin



Foto: Nana Reimers

Der undervises i it-sikkerhed i en af de mange datastuer.

computer - altså et program, der installerer sig i computeren og deler sig i to, der deler sig i to osv.

"Det var den ufarlige slags, der bare driller og irriterer, men der findes jo også de farlige, der aflurer ens bankkode", bemærker han, men afviser i samme åndedrag, at det er risikabelt at bruge computer:

"Det går sjældent galt, hvis du har installeret en såkaldt firewall (en slags elektronisk brandmur, red.), en virus-scanner, der opdaterer sig selv, og antispyware, der fjerner spioner, på din computer, og så kombinerer teknikken med almindelig omtanke - så som ikke at åbne en vedhæftet fil i en e-mail fra en ukendt", fastslår han.

Alder ingen hindring

92-årige Kaj Krebs "gik i skole" med den computer, børne- og oldebørn gav ham i 90 års fødselsdagsgave.

Af Annette Schiøler, Den fynsk/jyske Sammenslutning af Pensionistforeninger

"Om morgenen ser jeg lige, hvem der har e-mailet til mig, og svarer. Og så tager jeg gerne et spil syv-kabale", fortæller 92-årige Kaj Krebs fra Frederiksberg.

Kaj Krebs har hovedrollen i en lille reklamefilm om Ældremobiliseringens datastuer, som der bl.a. har været vist klip af i DR's OBS-udsendelser.

"Kan en gammel hund lære nye tricks", er titlen på filmen, der selv besvarer spørgsmålet med et utvetydigt "Ja!".

"Hvis man ikke kan se og ikke kan høre, kan det knibe. Men ellers kan alle lære at brug en pc", fastslår Jørn Jensen, 66 år og pensioneret postbud.

I kontakt med familien

Han er frivillig underviser på den datastue, hvor Kaj Krebs lærte at bruge den computer, som børne- og oldebørn forærede ham, da han fyldte 90 år.

"Da jeg havde fået det apparat, var jeg klar over, at jeg ikke ville få meget glæde af det, hvis ikke jeg kom lidt i skole med

det", fortæller Kaj Krebs. "Skolen" han gik i, er Ældremobiliseringens datastue på H.C. Ørstedesvej på Frederiksberg, og nu tænder Kaj Krebs for computeren hver dag. Han finder dagens nyheder på internettet, og via e-mail holder han nu også en nær kontakt med de mange familimedlemmer, der er spredt rundt omkring i verden.

Bare begynd!

Budskabet fra den 92-årige mand er da også klart: Alder er ingen hindring for at lære at

Fakta:

Om datastuerne

De første datastuer startede i 1998. I dag findes der 132 datastuer på landsplan.

500 ældre vejledere underviser på årsbasis ca. 5000 ældre over 60 år. Undervisningen er gratis, men der opkræves betaling til dækning af driftsudgifterne oftest et beløb på 50 - 200 kr. pr. sæson. Undervisningen sker ud fra "Ældre hjælper Ældre - tankegangen". I datastuerne styrkes såvel kendskabet til teknologien som det sociale fællesskab.

Se om der ligger en datastue nær dig. Gå ind på www.aeldremobiliseringen.dk og klik på menupunktet "Datastuer" og herunder "Datastuer m.v.".

Muligheder med internettet og Digital Signatur

I dag går udviklingen mod mere digital kommunikation - færre blanketter på papir, hurtigere behandling af sager på offentlige kontorer og kortere kø på posthuset.

Af Suzette Wagner, Videnskabsministeriet

Kommune er tiden for at behandle en sag ved ejendomshandler gået fra tre uger til 10 minutter.

I alle tre tilfælde sker det via internettet. Og de tre tilfælde er blot blandt de allerførste i en udvikling, der vil give både borgere, virksomheder og myndigheder store fordele. Den digitale signatur giver mulighed for en sikker identifikation i den digitale verden, og det er denne sikre identifikation, som giver alle de ovennævnte muligheder.

Der er mange fordele

Du kan kommunikere med det offentlige 24 timer i døgnet, få hurtigere svar og et bedre overblik over informationer. Og så kan du slippe for at skrive et brev i hånden eller på computeren, derefter printe det ud, finde en konvolut, købe et frimærke

og gå i postkassen med det. Og den digitale signatur er ligeså bindende, som den underskrift du skriver på papir.

Log på hjemmesider eller underskriv blanketter

Din digitale signatur er en personlig kode, som du kan bruge til at underskrive et dokument på en hjemmeside. Det kan f.eks. være en blanket, en indberetning eller lignende. Du kan også bruge din digitale signatur til at få adgang til hjemmesider. F.eks. kan du få adgang til dine personlige sundhedsdata på www.sundhed.dk

På www.digitalsignatur.dk kan du se en liste over steder, hvor du kan bruge digital signatur.

Her kan du blandt andet bruge din digitale signatur:

Alle kommuner
Apoteket.dk
ATP
Borger.dk
BorgerWeb
BRF Kredit
Det kongelige bibliotek
eBoks.dk
JØP Pension
Klasselotteriet.dk
Medicinprofilen.dk
Postdanmark.dk
PensionDanmark
Skat.dk
Sundhed.dk
Sundhedsstyrelsen
Sygeforsikringen Danmark
TDCOnline.dk

Se den fuldstændige liste på www.digitalsignatur.dk

Fakta:

Hvad er en digital signatur?

Din digitale signatur er dit id-kort på nettet. Når du bruger signaturen på en hjemmeside eller i en e-mail, viser du, at du nu også er den, som du udgiver dig for. Du kan bl.a. bruge din digitale signatur til at ordne selv-angivelsen, logge på e-boks, søge SU, skrive dit barn ind i en daginstitution, se dine sundhedsdata m.m. Og du kan underskrive dokumenter og blanketter, mens du er online.

Læs mere på: www.digitalsignatur.dk

I Aalborg Kommune kan borgerne selv hente information om deres egen skattesag. På Hvidovre Hospital kan forældre læse deres indlagte børns journaler. I Næstved

Otium blev vejen til internettet

Da Henning Ottesen gik på pension som 66-årig for otte år siden, havde han aldrig før brugt en computer. I dag er den en uundværlig del af hans hverdag.

Af Karina Velling Olesen, Videnskabsministeriet

"Med tiden er jeg bare blevet mere og mere interesseret i at bruge internettet, og jeg kan slet ikke forestille mig en hverdag uden. For eksempel har jeg nogle gode venner i Næstved og København, og dem kommunikerer jeg blandt andet med via e-mail. På den måde har nettet betydet, at jeg oftere er i kontakt med venner og familie", siger Henning Ottesen og tilføjer med begejstring i stemmen, at han sidste sommer modtog en e-mail fra nogle venner på ferie i Spanien.

Når Henning Ottesen i ny og næ støder på problemer på nettet, er han ikke bange for at søge hjælp. Især er børnebørnene trofaste hjælpere,

der gerne træder til, når morfar må smide håndklædet i ringen.

Spændende universer

Selvom det hovedsageligt er e-mailen, Henning Ottesen benytter sig af i hverdagen, bruger han også internettet til meget andet.

"Det er ikke kun e-mailen, jeg bruger. Jeg bruger det hele. Jeg har fået den her digitale signatur, og med den kan jeg komme rundt i en masse universer, som har gjort mange ting lettere for mig i hverdagen. Hvis jeg skal have fornyet mit kørekort, så bruger jeg den, eller hvis jeg skal kommunikere med SKAT", fortæller den begejstrede pensionist, mens



Henning vil gerne dele sine pc-erfaringer med andre, og for to år siden deltog han i opstarten af datastuen i Undløse og Jernløse Pensionistforening.

han fisker den lille cd med den digitale signatur op ad lommen. Henning Ottesen ynder også meget at surfe rundt på en masse hjemmesider. Han bruger meget tid på at

læse feriebetretninger, som mange mennesker lægger på nettet for at dele deres oplevelser med andre.

Ingen barrierer for ældre

Ifølge Henning Ottesen er der intet til hindring for, at man som ældre kan begynde at bruge nettet.

"Jeg kendte ikke noget til internettet for bare få år siden, men jeg har lært det lidt hen ad vejen og i mit eget tempo. Man kan finde ud af meget mere, end man tror - også selvom man er lidt oppe i årener", lyder det fra pensionisten, der ser både stolt og tilfreds ud.

Langt størstedelen af alt det Henning Ottesen kan på pc og internettet i dag, er selvlært. Han har taget enkelte AOF-kurser for nybegyndere, som har givet et godt fundament.

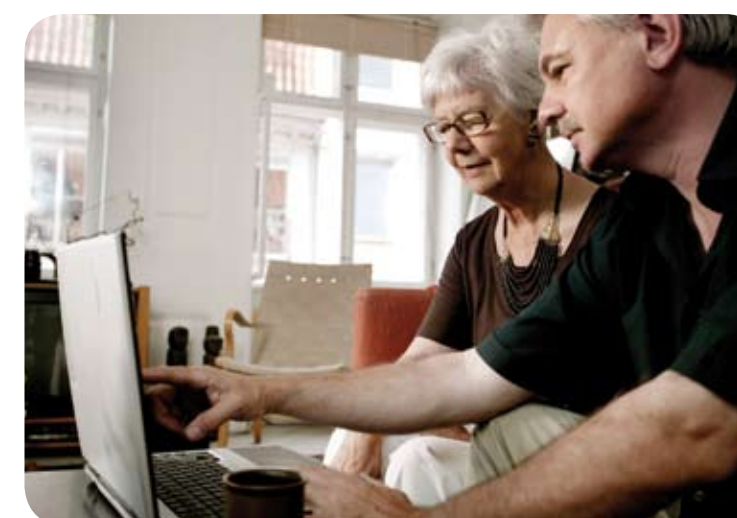
Digital Signatur

Brug Digital Signatur på

www.sundhed.dk

Nogle oplysninger skal ikke deles med andre. Digital Signatur bevarer privatlivets fred, når du besøger www.sundhed.dk, Skat og andre offentlige instanser.

Af Morten Godiksen, Sundhed.dk



På www.sundhed.dk finder du generel information fra hele sundhedsvæsenet om sundhed og sygdom, du kan finde behandlere og sammenligne f.eks. sygehuse. Men sundhedsvæsenet vil gerne give alle borgere muligheden for at bruge internettet endnu mere til at støtte kontakten med sundhedsfaglige. Så du som borger og patient kan blive medinddraget og have de bedste muligheder for selv at spille en aktiv rolle, stille spørgsmål og se, f.eks. hvilken medicin du har fået recept til osv. For at få adgang til f.eks. personlige sundhedsdata på www.sundhed.dk skal du først have en digital signatur, som er gratis.

Brug Digital Signatur flere steder

www.sundhed.dk har valgt at basere sikkerheden på den fælles standard for digital signatur, som den offentlige sektor har tilsluttet sig, og som TDC er udbyder af. Det betyder, at du kan bruge den samme signatur til www.sundhed.dk, som f.eks. til Skat og andre offentlige instanser. www.sundhed.dk bruger den digitale signatur til at sikre, at du er den, du giver dig ud for

at være, når du logger dig på. Digital signatur er et certifikat, der ligger på din computer. Signaturen er en personlig og helt unik nøgle, som kun indehaveren kender adgangskoden til. Når du første gang besøger www.sundhed.dk efter at have anskaffet dig en digital signatur, kan du bruge feltet "log på". Herefter vil adgangsmekanismen selv finde din digitale signatur på computeren, og du kan bekræfte, at du vil bruge den samt indtaste din adgangskode. Herefter får du adgang til "min sundhed.dk" som leder dig hen til alle de data, du har adgang til på www.sundhed.dk

Dine oplysninger er godt beskyttet

Du kan f.eks. se oplysninger om dit køb af receptpligtige

lægemidler og hvis du er tilmeldt donorregistret. På sigt vil du også få adgang til oplysninger om din personlige sygehistorik. Sundhedsdata stammer fra nationale og regionale registre. De når frem til dig gennem sikre forbindelser mellem datakilde, www.sundhed.dk og dig, hvor data er krypterede og ulæselige, indtil de oversættes på din computer. Dit privatliv er beskyttet af loven. Får du mistanke om, at nogen uretmæssigt har fået fat i dine data, kan www.sundhed.dk spore hvem, der har set dine data og hvornår. Samtidig kan du i din personlige log på www.sundhed.dk se, hvis nogen har kigget i dine oplysninger og hvornår.

Sådan får du en gratis Digital Signatur

Det er nemt at bestille en Digital Signatur – og så er den gratis.

Gå ind på hjemmesiden www.digitalsignatur.dk og klik på knappen "Bestil digital signatur" midt på siden. Du har nu flere valgmuligheder for at bestille din digitale signatur. Det nemmeste er at bestille den med dit personnummer og din e-mail-adresse. Klik på linket, udfyld formularen og umiddelbart herefter får du tilsendt en e-mail med et link, som du skal gemme. For at installere signaturen skal du nemlig bruge linket og en pinkode, som du normalt får tilsendt med posten et par dage efter bestillingen.

Når du er klar til at installere din digitale signatur, skal du klikke på linket i den tilsendte e-mail, indtaste din pinkode og ellers følge vejledningen i installationen, som selvfølgelig er på dansk.

Undervejs bliver du bedt om at vælge en adgangskode til din signatur. Du kan få hjælp til at lave en god kode i artiklen side 14.

Bestil din digital signatur på: www.digitalsignatur.dk

Vælg din adgangskode med omhu

Det tager en erfaren hacker 12 sekunder at knække et kodeord på fem små bogstaver. Bruger du de samme kodeord mange steder, er der herefter fri adgang til alle dine private tjenester. Vi giver dig en række tips til, hvordan du laver den perfekte adgangskode.

Af Henning Rasmussen, Computer for alle

Tip 1

Lav et system med mindst otte tegn

En kode på fire-fem tegn er usikker, uanset hvilke tegn, den består af. Den bør være på otte-ti tegn eller mere. Nogle systemer accepterer mellemrum i koden, så du kan lave en sætning som adgangskode. Du kan f.eks. lave en kode, der hedder "Min bror Matias er 22 år", som dermed både indeholder små og store bogstaver og tal – og med garanti ikke kan gættes af et hacker-program med en indbygget ordbog. Kan du ikke anvende en sætning, kan du i stedet f.eks. anvende forbogstaverne i din sætning. Eksemplet fra før kan så blive til "MbMe22aa".

Tip 2

Kombiner bogstaver, tal og symboler

Den sikreste kode får du, ved at blande tal, bogstaver (store og små) og specielle tegn – og helst i en kombination, som ikke umiddelbart giver nogen mening. Det er for nemt at gætte, hvis du blot sætter et 0 eller 1-tal efter din kode. Brug i stedet et tal midt i koden. Specielle tegn og tal kan du anvende ved f.eks. at udskifte et "a" med "@" eller bogstavet "o" med tallet "0". Din adgangskode bliver sværere at bryde, hvis der er en blanding af store og små bogstaver. Smid et enkelt eller to store bogstaver ind midt i.

Tip 3

Pas på med kendte ord og navne

Det er en dårlig idé at bruge din kærestes eller kæledyrs navn eller en fødselsdato i dit kodeord. Dels er der risiko for at skumle personer, som kender en smule til dig, vil kunne gætte koden, og samtidig kan hele kendte ord findes i store ordbogslister, som anvendes af hackerens software. Det betyder ikke, at du slet ikke må anvende ord, for

det er naturligvis nemmere at huske reelle ord end en tilfældig blanding af karakterer. Et navn, som gør det nemmere for dig at huske koden, kan godt bruges, blot du supplerer koden med tal, tegn og store bogstaver – f.eks. "3pjEvs*3", hvor Pjevs f.eks. er navnet på din kat.

Tip 4

Lav adgangskoder til forskellige kategorier

Hvis du bruger kodeord til forskellige steder, skal du huske på ligeså mange, og jo mere komplicerede kodeordene er, desto sværere er de at huske. Det problem kan du eliminere ved at opdele de steder, du anvender kodeord, i forskellige sikkerhedskategorier – og så lave adgangskoder, der svarer til risikoen ved et indbrud. På hjemmesider, der kræver log ind, kan du sagtens anvende en mindre sikker kode, der er nem at huske. Mellemkategorien kan være log ind til hjemmesider, hvor du har gemt din adresse, telefonnummer eller lignende. Her bør du vælge en mere sikker kode, som er forholdsvis let at huske. Til gengæld bør du anvende alle sikkerhedsråd til

koder, hvor du har gemt dine kreditkort-oplysninger eller CPR-nummer, og hvor der er risiko for økonomisk tyveri eller identitetstyveri – f.eks. log ind til det offentlige eller din netbank.

Tip 5

Gør det ikke for nemt for hackerne

De fleste bygger koden op af vaner og systemer, som gør den nem at huske – desværre også nemmere at knække. Her er de mest almindelige kode-fejl:

- Undgå at bruge en sekvens af bogstaver eller tal eller en stribe ens tegn i koden, som f.eks. være "123456", "22222" eller "abcdeff".
- Lad være med at bruge dele af dit navn, din fødselsdato, dit CPR-nummer eller navnene på din kone eller børn.
- Brug ikke almindelige ord, et ord stavet bagfra eller almindelige fejlstavninger. Hackerens ordlister indeholder tusindvis af sådanne kode-forslag.

Brug aldrig den samme kode. På den måde kompromitterer du ikke alle de steder, du anvender koder, hvis blot én af dem er knækket.

Fakta:

Test din kodes sikkerhed	JA	NEJ
1. Består koden både store og små bogstaver?	Gå til punkt 2	Din kode er ikke sikker nok
2. Indgår der tal i koden?	Gå til punkt 3	Din kode er ikke sikker nok
3. Er koden bogstaver hele ord?	Din kode er ikke sikker nok	Gå til punkt 4
4. Bruger du din fødselsdato eller familienavne i koden?	Din kode er ikke sikker nok	Gå til punkt 5
5. Skifter du koden med jævne mellemrum?	Din kode er sikker	Din kode er sikker, men husk at skifte

Børnebørnene er gået online

Kapow! 12-årige Andreas leger soldat i en online skyttegrav, Anders And har fået mobiltelefon, og poesibogen er blevet interaktiv. Internettet er en naturlig del af børnebørnenes dagligdag.

Af Gry Hasselbalch, Medierådet for Børn og Unge



96% af børnene i en ny undersøgelse fra Medierådet for Børn og Unge har adgang til internettet derhjemme. Her søger de informationer, lytter til musik, spiller computerspil eller ser film. Men herudover er det de sociale aktiviteter, der trækker, viser undersøgelsen. Over halvdelen går f.eks. på nettet for at chatte.

"Selvom børn ofte er teknisk længere fremme, så er det stadig forældrene og bedste-forældrene, der har samlet de erfaringer sammen, som gør os i stand til at færdes etisk og socialt mellem andre mennesker. Det er kompetencer, der er lige så vigtige online som i den virkelige verden".

Mød børnebørnene på nettet

Det handler om at have en dialog med børnebørnene om medierne. Her er internetchat en god mulighed for at møde børnebørnene i deres online verden. Og måske vil du også selv drage nytte af dit barnebarns gode fif til at navigere uden om spam, virus og fiduser på nettet?

Fakta:

Børneundersøgelsen 2007:

- 71% spiller onlinespil over internettet
- 54,3% bruger internettet til at chatte
- 57% hører musik
- 37% ser film/video

Medierådet for Børn og Unges hjemmeside:
www.medieraadet.dk

Nettet er en vigtig del af børns hverdag

Tendensen er klar. Børn i dag er vokset op med de digitale medier som en fast del af deres hverdag. Specielt internettet fungerer som en forlængelse af deres hverdagsliv med venskaber, de vedligeholder via chatportaler. Men for bedste-forældre og forældre er internettet et nyt bekendtskab. Mange børn oplever derfor, at de voksne er fraværende i online verdenen. I undersøgelsen angiver en stor del af børnene f.eks., at de ikke taler med deres forældre om en række risici forbundet med deres færden på nettet. Vi voksne bliver dog nødt til at tage børnenes online verden alvorligt, og her kan man som bedsteforælder også være med. Susanne Boe, Sekretariatschef for Medierådet for Børn og Unge og bedstemor til fire, siger:

Farmor chatter på

Messengers

Lise Agger på 87 år bruger Messenger og e-mail. Og hun og barnebarnet Christian har elektronisk kontakt mindst et par gange om ugen, for det er så nemt.

Af Signe Thomsen, Microsoft

"Det er jo fantastisk. I samme øjeblik, jeg trykker på en knap, - gong! - så har han mit brev".

87-årige Lise Agger er vildt begejstret for at sende og modtage elektroniske beskeder. Selv om der står 1920 på fødselsattesten, bruger hun i gennemsnit en halv time om dagen på at skrive e-mails til venner og familie eller være på Messenger med sine børnebørn.

"Den moderne teknologi forenkler tilværelsen utroligt meget. Det er en nem og hurtig måde at være i kontakt med hinanden på", siger Lise Agger.

Hendes hyppigste e-mail- og Messenger-partner er barnebarnet Christian Agger på 31 år. Han lærte for fem år siden sin farmor, hvordan man sikkert og nemt bruger e-mail og chatter med Messenger.

"Vi kan altid komme i kontakt med hinanden via e-mail. Det er sværere på telefonen", siger Christian Agger.

Nu kommer der levende billeder

Lise og Christian Agger skriver sammen på e-mail eller chat mindst et par gange om ugen. Ofte om at ses til koncert i Radiohuset eller til middag hos farmor. Ellers skriver de sammen om løst og fast.

"Messenger er fint til korte beskeder, eller hvis vi lige skal skrive, at vi glæder os til at se hinanden i morgen, men ellers kan jeg bedst lide e-mail.



Lise Agger sammen med Christian, der introducerede hende til internettet.

Så sidder jeg så hyggeligt og skriver i fred og ro", siger Lise Agger, som er pensioneret sekretær.

Måske bliver Messenger snart favoritten. Senere samme aften skal Christian Agger nemlig hjælpe sin farmor med at sætte et web-kamera op, så de fremover kan se hinanden, mens de chatter.

"Det bliver sjovt, at vi også kan se hinanden. Men så må jeg jo ordne håret pænt, hver gang jeg sætter mig ved computeren", siger Lise Agger med smil i stemmen. Hun forsøger også at overtale nogle af sine jævnaldrende til at komme online, så de kan chatte med hinanden.

Messenger og Hotmail giver adgang til nem og sikker kommunikation

Windows Live Messenger er et gratis program, hvor du kan chatte, altså sludre, med én eller flere personer ad gangen. Du kan kun komme i kontakt med dem, som du selv har tilføjet som dine kontaktpersoner. Når du vil chatte med dine venner eller familie, kan du skrive korte sætninger til dem. Så kan de med det samme se, at du har skrevet en besked til dem. Du kan også tilføje et webkamera til din computer og se den eller dem, som du chatter med.

For at kunne chatte skal du først hente programmet "Messenger" på www.windowslive.dk Så skal du vælge

"Live Messenger" i oversigten og vælge "download", hvorefter programmet er installeret, skal du oprette en "Messengerkonto", hvilket sker ved at trykke på "Tilmeld dig et Windows Live-ID".

Når Messenger er installeret, skal du selv invitere dine venner/familie ved at gå under punktet "kontaktpersoner" og vælge "tilføj en kontaktperson".

For at oprette en "Messengerkonto" skal man have en e-mail-adresse. Hvis du ikke har sådan en, kan du gratis oprette den på www.windowslive.dk under "Live Hotmail".

Fakta:

Kom godt i gang med at chatte

- Tilføj ikke personer på din Messenger, som du ikke kender.
- Opgiv aldrig personlige oplysninger som konto- eller CPR-nummer.
- Brug smileys, hvis du gerne vil udtrykke følelser.
- Du kan sende billeder igennem Messenger for at gøre din historie mere spændende.
- Indsæt et billede af dig selv for at gøre din profil mere personlig.
- Tilføj et web-kamera og tal igennem Messenger - helt gratis.
- Vær opmærksom på, at kommunikation gennem korte beskeder nemt kan misforstås.

Test dig selv

Færdes du sikkert på nettet? Se hvor mange spørgsmål, du kan svare rigtigt på.

1.
Skal du oplyse din firecifrede pinkode ved online handel?

- a** Du skal altid oplyse din firecifrede pinkode
- b** Du skal kun oplyse din firecifrede pinkode til din bank
- c** Du skal aldrig oplyse din firecifrede pinkode

2.
En af nettets største farer er?

- a** E-mails fra folk, der vil sælge dig noget
- b** Falske e-mails, der lokker oplysninger ud af dig
- c** Museskader og trætte øjne

3.
Hvad kan du i Ældremobiliseringens datastuer?

- a** Lære at bruge en pc og være på internettet
- b** Lære om data og statistiske tabeller
- c** Lære hvordan du installere en trojansk hest

4.
Hvis du er et "muldyr" på nettet, er du?

- a** En, som er langsom på nettet
- b** En, som mod betaling hjælper kriminelle med at overføre stjålne penge til andres konti
- c** En, som lokker andre til at begå kriminelle handlinger på nettet

5.
Hvad bør du gøre, når du modtager spam?

- a** Slette e-mailen med det samme
- b** Sende den videre, hvis det er en sjov e-mail
- c** Forsøge at afmelde den ved klik på eventuelle links

6.
Hvad er en god adgangskode?

- a** En, som du altid kan huske eller kan gætte dig til
- b** En, med flere specialtegn og på mindst 8 tegn
- c** En, der er så kort som muligt

7.
Hvad er en Digital Signatur?

- a** En sikker og personligt identifikation på nettet
- b** Min underskrift ved køb af en computer
- c** Mit navn, der står i bunden af en e-mail

8.
Hvordan kan du undgå virus?

- a** Ved at spise vitaminpiller hver dag
- b** Ved kun at læse e-mails fra folk du kender
- c** Ved at installere og huske at opdatere dit antivirus-program

9.
Hvad er en chat på nettet?

- a** En elektronisk slåskamp
- b** En "samtale" bestående af små elektroniske beskeder over nettet
- c** En internettelefon

10.
Hvad er det bedste middel mod phishing?

- a** Sund skepsis og et spamfilter
- b** Et fisketegn
- c** En forsikring mod phishing

11.
Hvordan kan du gøre dit netværk sikkert?

- a** Gem netværket i et skab så indbrudstyre ikke kan se det
- b** Du behøver ikke at foretage dig noget
- c** Skjul og omdøb dit netværks navn

12.
Hvor tit bør et antivirusprogram opdateres?

- a** Mindst en gang om dagen
- b** Mindst en gang om ugen
- c** Mindst en gang om måneden

13.
Hvad er spyware?

- a** Skæg og briller til at forklæde dig med
- b** Program, der ændrer din pc's opsætning mod din vilje
- c** Et program til at hjælpe detektiver

1.c, 2.b, 3.a, 4.b, 5.a, 6.b, 7.a, 8.c, 9.b, 10.a, 11.c, 12.a, 13.b

Hvor mange rigtige havde du?

0-3: Gå omgående hen til din computer og træk internetstikket ud. Hvis du stadig har returret på computeren, så benyt den. Eller få styr på internet-sikkerheden. Nu.

4-7: Brug hellere telefonen. E-mail-kontakt er ikke sikker for dig. Læg nettet på hylden indtil du har styr på sikkerheden. 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

