Sikkerhed på internettet

Sikkerhed på internettet omfatter forskellige tiltag, alt efter hvilken anvendelse, der er tale om.

Adgang til et websted kan begrænses med et **brugernavn** og en **adgangskode**. Anvendelsen af brugernavn og adgangskode kan have til formål at beskytte mod adgang til bestemte oplysninger, eller til at opkræve brugerbetaling for benyttelsen af hjemmesider.

Det **digitale certifikat** er en elektronisk erklæring, der godtgør at f.eks. en software udgiver kan identificeres og at identiteten kan bekræftes, eller at en webside virkelig har den udgiver, som websiden tilkendegiver. Det digitale certifikat (SSL certifikatet) udstedes af en betroet tredjepart, et certificerings center. I Danmark kan man bestille en digital signatur hos TDC.

Et digitalt certifikat er en elektronisk fil, der unikt identificerer enkeltpersoner og servere. Digitale certifikater lader klienten (webbrowseren) autentificere serveren, før SSL-sessionen etableres. Digitale certifikater er typisk underskrevet af en uafhængig og betroet tredjepart for at sikre deres gyldighed. "Underskriveren" af et digitalt certifikat kaldes et certificeringscenter (CA - Certification Authority), såsom VeriSign ellerDanID.

SSL muliggør sikre online transaktioner ved at kombinere følgende tre vigtige elementer:

1. *Autentificering: Et digitalt certifikat er associeret med et specifikt domænenavn. Før der udstedes et digitalt certifikat, har certificeringscentret ansvaret for at udføre en række kontroller (kaldt "autentificerings- og bekræftelseskontroller") til at bekræfte identiteten på den organisation, der anmoder om certifikatet, og hvorvidt det har ret til at bruge det domænenavn, som vil være associeret med det pågældende certifikat. Denne stærke forbindelse mellem certifikat og domænenavn giver brugere forvisning om, at de samvirker med en lovlig organisations website, ikke en bedragers.*
2. *Kryptering: Kryptering er processen med at omdanne oplysninger for at gøre dem uforståelige overfor alle med undtagelse af den tiltænkte modtager. Dette danner grundlaget for dataintegritet og diskretion, som er nødvendig for sikre online transaktioner. Et SSL-certifikat er en særlig slags digitalt certifikat, som binder en identitet til et par elektroniske nøgler, der kan bruges til at kode og underskrive digitale oplysninger, der transmitteres over internettet via "https" protokollen. Når først certificeringscentret bekræfter identiteten på den organisation, der anmoder om certifikatet, og hvorvidt det har ansvaret for det domænenavn, som vil være associeret med det pågældende certifikat, bruger certificeringscentret dets offentlige nøgle til at underskrive certifikatet indeholdende bla. organisationens offentlige nøgle og "udsteder" certifikatet til organisationen.*
3. *Meddelelsesintegritet: Efter en SSL-session er blevet etableret, beskyttes indholdet på al kommunikation imellem klient og server imod forfalskning undervejs. Alle parter til transaktionen ved, at de oplysninger, som de har modtaget, er nøjagtig, hvad der blev skabt fra den anden side af SSL-sessionen.*

Når de tre ovennævnte elementer kombineres, bliver SSL en simpel, men alligevel effektiv sikkerhedsløsning, der giver dig mulighed for at foretage autentificerede og kodede online transaktioner med gæster på din website. Med et VeriSign SSL-certifikat installeret på din website vil gæster være i stand til at afgive kreditkortnumre eller andre følsomme oplysninger til dig med fuldstændig forvisning om, at de virkelig gør forretning med dig (og ikke en bedrager), og at de oplysninger, de sender til dig, ikke kan opfanges eller forfalskes under transmissionen.

Kilde: http://www.symantec.com/da/dk/ssl-certificates/

Anvendelse af kreditkort på til e-handel eller andre former for betalinger, bør kun foretages på sider, der anvender ://https forbindelser. Ved anvendelse af kreditkort til e-handel skal man være opmærksom på flg. risici: at købsbeløbet overføres, men varen ikke leveres, at kortnummer og udløbsdato opsnappes af en tredjepart, og at lovgrundlaget er nøjagtigt det samme, som ved almindelig handel.

Computervirus er programmer, der er designet til at multiplicere sig selv, når den inficerede computer anvendes. Hensigten er destruktiv, idet infektionen i mildeste fald fylder harddisken op, og i værste fald destruerer programmer eller dokumenter, eller anvender mail systemet og adressekartoteket til at sende mails i dit navn. Mailen vil typisk indeholde et "uskyldigt" emne og en vedhæftning, der inficerer modtagerens computer.

Typiske tegn på at en computer er blevet inficeret med virus er forringet arbejdshastighed, filer der skifter navn og / eller størrelse, ikoner der forandrer udseende, eller mere generelt – at computeren arbejder anderledes end normalt.

Beskyttelsen mod computervirus er **opdaterede antivirus programmer**, som automatisk kontrollerer indkommende mails og vedhæftede filer, downloads, CD´er, USB-enheder, eksterne diske mm.. Antivirus programmerne kontrollerer for kendte vira – og gør opmærksom på filer med mistænkeligt indhold.

Der bør altid arbejdes med automatisk kontrol af filer, der hentes, ændres eller udføres. Programmer, der downloades bør altid scannes for virus inden de pakkes ud og installeres.

Mails med vedhæftninger bør ikke uhildet åbnes, medmindre man er sikker på afsender identiteten.

Microsoft integrerer antivirus og firewall i Windows 7, Vista og 8. Microsoft Security Essentials kan downloades fra: http://windows.microsoft.com/da-dk/windows/security-essentials-download

Der findes flere forskellige producenter af antivirus programmer.

McAfee - www.mcafee.com
Download: http://home.mcafee.com/?CID=MFEen-usMHP001

Symantec (F-secure) - https://www.f-secure.com/da_DK/web/home_dk/downloads
Download: https://www.f-secure.com/en/web/home_global/home

Panda Software - http://www.pandasecurity.com/denmark/
Download: http://www.pandasecurity.com/denmark/

AVG - http://www.avg.com/dk-en/homepage
Download: http://www.avg.com/dk-en/free-antivirus-download

Avasti - https://www.avast.com/da-dk/index

Download: https://www.avast.com/da-dk/index

Programmerne opdateres løbende, således at der hele tiden tages højde for nye vira.

Antivirus producenterne publicerer jævnligt beskrivelser af de forskellige vira, deres virkemåde og bekæmpelsen af disse.

Hacking er betegnelsen for at trænge ind på en computer eller et netværk, som man ingen legal adgang har til. Hacking omfatter illegal anvendelse brugernavn og adgangskode (evt. at knække en kode) for at tiltvinge sig adgang til at kunne udføre forskellige handlinger, eksempelvis industrispionage eller økonomisk kriminalitet.

Beskyttelsen mod hacking er anvendelse af en **Firewall**. Firewall kan bestå af hardware eller software, der registrerer og afviser uautoriseret adgang til en computer eller et lokalt netværk.

Firewalls i software udgave produceres af de samme producenter, som udgiver antivirus programmer. Software firewalls installeres på de(n) enkelte maskine(r).

Hardware firewalls er selvstændige maskiner, der med eget software beskytter et netværk mod hacking.

Både software og hardware firewalls skal passes og opdateres, da hackingen typisk vil foregå mod forskellige porte (stik / forbindelser)

Phishing er et relativt nyt internetfænomen (2005), hvor svindlere forsøger at franarre godtroende internetbrugere deres kreditkort- eller netbankoplysninger. Det sker typisk ved at brugeren får tilsendt en e-mail, hvis indhold forsøger at få brugeren til at indsende sine oplysninger pr. e-mail eller logge ind på en falsk internetside, der ligner f.eks. bankens.

Siden har der udviklet sig et lignende fænomen omkring indholdstakserede sms-beskeder kaldet **smishing**: Personer lokkes til at købe f.eks. billeder af letpåklædte kvinder og betaler for dette, men modtager i bedste fald noget helt andet.

Betegnelsen **spyware** eller **spionprogrammer** bruges om computerprogrammer, der installerer sig selv hos en klient, som regel uden at klienten ved noget om dette. Man kan beskytte sin computer mod spyware med programmer, men disse skal typisk opdateres tit, for at kunne følge med fremvæksten af nye spyware-programmer.

Spyware er en almen form for malware, som ligger spredt ud på din computer, og ser efter hvad du laver. Den minder en del om en keylogger, og man kan beskytte sig mod spyware med programmer som bl.a. *Spyware Blaster*, som kan hentes via mange hjemmesider. Der opstår dog konstant nyere versioner af spyware, og derfor er de altid svære at finde.

Malware er en sammentrækning af de engelske ord malicious software (på dansk: "ondsindet programkode"). Det bruges som en fællesbetegnelse for en række kategorier af computerprogrammer, der gør skadelige eller uønskede ting på de computere, de kører på.

Forskellige kategorier af malware

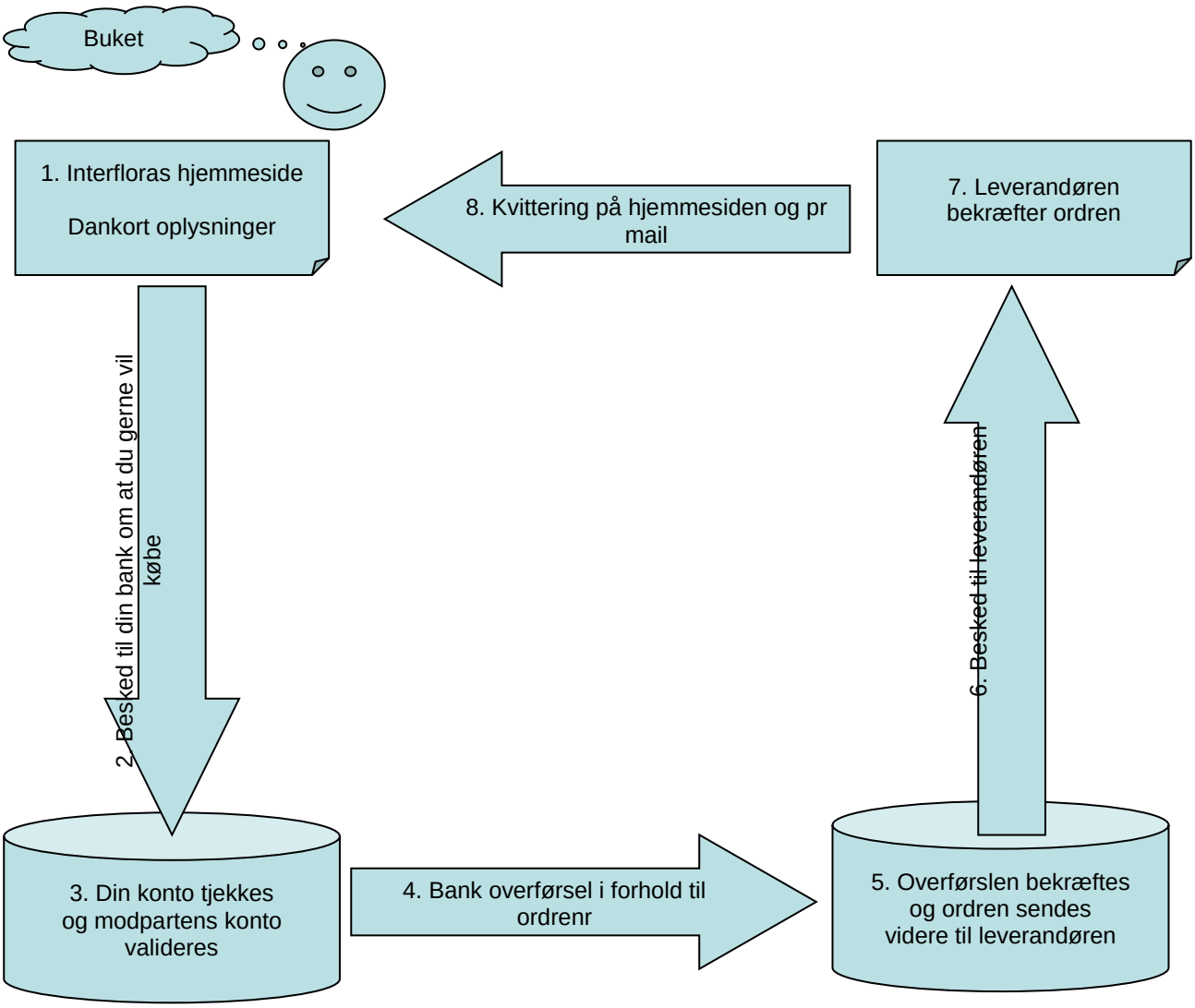
- En computervirus er et lille program, som forsøger at inficere andre programmer. Det er ofte skjult i et tilsyneladende harmløst program, da denne type malware skal aktiveres manuelt for at kunne indlede spredningen. Virusprogrammer kan være meget skadelige, f.eks. ved at slette vigtige data og/eller programfiler fra den inficerede computer.
- En makrovirus er et program, der udnytter det programmeringsmiljø, der findes i mange programmer til kontorarbejde: Et tekstbehandlings- eller regnearks-dokument kan på den måde udgøre en trussel mod computersystemet.
- En orm er omtrent det samme som en computervirus, blot med den væsentlige forskel, at en orm kan sprede sig selv fra maskine til maskine uden at blive aktiveret manuelt. Det foregår ofte ved at udnytte sikkerhedsbrister i operativsystemet eller browseren. En orm vil ofte medbringe en skadelig "last", på engelsk: payload(en), i form af et eller flere programmer, f.eks. en trojansk hest eller en computervirus. Flere orme, f.eks. Nimda-ormen, har i deres payload en mailserver, der benyttes til at videresende ormen til eksempelvis de kontaktpersoner, som offeret har registreret i sit e-mail-programs adressebog.
- Adware er programmer, hvori div. reklamer vises mens programmet afvikles.
- Spyware undersøger typisk hvilke hjemmesider brugeren besøger, og hvilke søgeord han/hun bruger på world wide web, hvorefter det rapporterer tilbage til skaberen af programmet via internettet. Det er ofte nært belægtet med adware, og de indsamlede oplysninger bruges så til at målrette de reklamer, der vises for den pågældende bruger.
- Jokeware er programmer, som prøver at irritere brugerne på forskellige måder. For eksempel ved at styre en enkel brugers markør.
- En keylogger er et program, der registrerer, hvad der skrives på tastaturet. Det bruges til at spionere mod den bruger, hvis computer er inficeret med keylogger-programmet, oftest med henblik på at aflure passwords, kontonumre og andre følsomme oplysninger, når brugeren handler eller ordner bankforretninger via nettet. Oplysningerne kan blive gemt i en logfil på offerets computer og/eller automatisk blive sendt til en forudbestemt e-mail-adresse. Visse programmer til "forældrekontrol" indeholder reelt også en keylogger beregnet på at overvåge børns brug af chatprogrammer mv..
- Ransomware er et relativt nyt fænomen (2005). Det er en art virus, hvis skadevirkning består i at kryptere brugerens data, hvorefter man præsenteres for en besked om, at man kan få "nøglen" til at afkode sine data mod at betale en løsesum.
- En dialer er et program rettet imod folk, der bruger et modem til at etablere forbindelse til internettet. Det ændrer i computerens indstillinger for brug af modemmet, så det i stedet for den vante internetudbyder ringer op til et andet telefonnummer ofte med store telefonregninger til følge.
- En trojansk hest er malware forklædt som noget harmløst. Den har fået sit navn fra Homers skildring af Odysseus' krigslist mod byen Troja. I it-sammenhænge er den indsmuglede "trojaner" eller payload ofte et serverprogram, som gør det muligt for andre at fjernstyre offerets computer. Det kalder man også at installere en bagdør. Adgangen kan f.eks. misbruges til at foretage denial-of-service-angreb mod andre systemer på nettet. Fjernstyringsprogrammet Back Orifice(en) er et af de mest kendte payload-programmer i trojanske heste, selv om programmet i sig selv er lavet til legale formål.
- Et hoax (engelsk for "fupnummer") er en advarsel om en fiktiv virus eller anden malware, som sendes rundt, typisk via en kædebrevslignende e-mail, med det formål at få forskrækkede, ukyndige brugere til at slette en ellers nyttig fil fra deres computersystem - eller ganske enkelt for at drille.

Ofte bruges ordet "computervirus" i flæng om flere af de andre former for malware, fordi dette var den første type af malware. Derfor er antivirus-programmer sjældent begrænset til alene at bekæmpe vira, men sikrer også mod flere andre malware-kategorier.

Forvirringen bliver ikke mindre af, at malware ofte optræder som en kombination af flere af ovennævnte typer. F.eks. kan en orm laves, så den automatisk spreder sig til en computer, hvor den dropper en payload bestående af en keylogger og en trojansk hest med et fjernstyringsprogram. Når den trojanske hests payload bliver aktiveret, kan ormens ophavsmand så skaffe sig fjernadgang til offerets computer for at aflæse keyloggerens logfil

Handel på Internettet

Når ordren er afsendt, sendes der besked til det finansinstitut, som dit betalingskort er udstedt af. Beskeden indeholder dine data, samt modtagerens finansinstituts data, ordrenummer og transaktions beløb. Når dit finansinstitut har godkendt handlen, debiteres din konto for ordrebeløbet, som via dit finansinstitut overføres til sælgerens konto. Forløbet kan skildres som i figuren herunder.



http://www.forbrugerraadet.dk/
Forbrugerrådet har opstillet en række gode råd for nethandel:
2. maj 2006

Nethandel er nemt, men der er nogle ting du skal være opmærksom på
Tjek virksomheden før du handler
Kan du komme i kontakt med butikken, hvis du vil spørge om noget?

Hvem handler du egentlig med? Fremgår butikkens navn, fysiske adresse, e-mail , evt. telefonnummer og virksomhedens registreringsnummer eller navnet på den ansvarlige indehaver?

Kig efter e-mærket, som kontrollerer at netbutikkerne overholder love og retningslinier. Se hvilke butikker der har e-mærket på www.e-maerket.dk

Tjek betingelserne
Inden du gennemfører købet skal du tjekke prisen. Er alt inkluderet - også forsendelsesomkostninger?
Når du handler i udenlandske e-butikker, skal du være opmærksom på, at du i nogle tilfælde også skal betale moms og told.

Får du alle oplysninger om varen. Altså, ved du præcis, hvad du har købt ud fra beskrivelsen på hjemmesiden?

Får du oplysninger om leveringsbetingelser og dine rettigheder f.eks. fortrydelsesret?

Afgivelse af personoplysninger
Har butikken en persondatapolitik? Hvis du skal afgive en masse oplysninger om dig selv for at kunne gennemføre købet, så overvej om du vil handle der. Butikken har pligt til at informere om hvilke oplysninger, der registreres og hvad de skal bruges til.

Hvis der er mangler ved varen - så klag
Kontakt virksomheden hvis du modtager den forkerte vare eller der er mangler ved varen. Det er virksomheden, der skal dække alle omkostninger.

Hvis butikken ikke makker ret, kan du klage til Forbrugerklagenævnet

Hvis varen ikke kommer
Kontakt virksomheden. Skriv, gerne e-mail. Giv dem en rimelig frist for levering, hvorefter du anser købet for annulleret. Har du betalt med kort skal skal din bank tilbageføre beløbet til din konto, hvis butikken ikke selv gør det.

Betal med kort
Der er mange fordele ved at betale med kort, når man handler på nettet. Hvis du har betalt med kort, kan du få pengene tilbage af banken hvis butikken skylder dig penge:
- hvis varen ikke leveres
- hvis du ved at udnytte din fortrydelsesret nægter at modtage varen
- hvis der er hævet penge på din konto udelukkende ved brug af dit kortnummer, uden du har givet lov.

Det er din ret, og det er dem der har udstedt dit kort (oftest din bank), der skal give dig pengene senest to dage efter, at de har modtaget din indsigelse. Klag først skriftlig til butikken med kopi af brev til eget brug.

Udskriv, gem og tjek
Udskriv både din ordre og ordrebekræftelse og gem dem.
Tjek altid dit kontoudskrift for at se om der er nogle virksomheder, der kommer til at trække dig for beløbet to gange eller at nogle uretmæssigt har handlet med dit kortnummer.