- 10 gode råd om netsikkerhed
  1. Brug din sunde fornuft og naturlige skepsis Brug altid din sunde fornuft og din naturlige skepsis, når du færdes på Internettet, og når du sender og modtager e-mails. Læs mere

- Antivirus information
  Maksimal sikkerhed på computeren opnås bedst ved at sørge for, at computerens software er helt opdateret. Det gælder både for alle operativsystemets individuelle komponenter og for de programmer, du bruger. Men mindst lige så afgørende er det, at du installerer og bruger et antivirus program, som løbende opdateres med de nyeste virusopdateringer og signaturer. Kun på denne måde kan du sikre dig, at antivirus programmet fungerer optimalt og at det vil reagere, hvis en ny virus spreder sig til din computer.

- Reducering af risikoen for virus med opdateret antivirussoftware
  En virus er et program, der kan være skadeligt for computeren, og den kan bruge din internetforbindelse til at sprede sig selv til andre computere, f.eks. computere tilhørende kolleger, venner og familie. Du kan undgå mange virus ved kun at åbne vedhæftede filer i e-mails, når du er sikker på, hvem afsenderen af e-mailen er. Samtidig bør du også vide, hvad den vedhæftede fil indeholder. Det er dog ikke altid, at det er nok til at undgå virus. I denne artikel kan du læse mere om, hvordan du kan undgå virus på computeren.

- Sikkerhedskopiering af filer på computeren
  Der findes mange måder, hvorpå du kan miste oplysningerne på en computer ved et uheld. Et barn, der leger med tastaturet som et klaver. En strømafbrydelse. Lynnedslag. Brand. Tyveri. Og nogle gange kan det skyldes fejl på computeren. Hvis du regelmæssigt sikkerhedskopierer dine oplysninger, kan du gen-danne de fleste eller alle oplysninger, hvis der sker noget med de originale filer på computeren. I denne artiklen kan du læse mere om, hvorfor og hvor ofte du bør sikkerhedskopiere filer. Du får også nogle tip til, hvordan du kommer i gang.

- Tip til beskyttelse af børn, når de er online
  På internettet har dine børn adgang til helt nye muligheder for at få oplysninger, spille spil, se film og udforske deres ideer. Sammen med disse fordele følger nogle udfordringer. Du kan gøre dit til at beskytte dine børn, når de er online, og du kan lære dem, hvordan de kan bruge internettet på en måde, der hjælper med at beskytte dem. Selvom software ikke kan erstatte forældrenes engagement og indsigt,

- Fokus på driftsikkerhed
  Det skal være muligt at installere eller ændre routers, switches, web- og databaseservere og storageenheder uden uheldige konsekvenser. Men alting hænger sammen, og forandringerne kan være meget tidskrævende at modne til produktion. Samtidig mangler der ofte klare ansvarsfordelinger og processer for, hvordan miljøer med Microsoft Windows Server skal opbygges, drives, sikres og overvåges.

- Hold øje med falske emails og orme
  Grundreglen bør være, at du aldrig åbner programmer eller vedhæftede filer, som du har fået tilsendt uden at du har bedt om det. Det er almindeligvis ikke risikabelt at læse selve e-mailen, det er vedhæftningerne du skal være opmærksom på. Sørg også for at have opdaterede versioner af dit e-mail program og din Internetbrowser, samt for at have installeret seneste virusdefinitioner til dit antivirusprogram. Har du ikke et antivirusprogram, anbefaler vi at du anskaffer dig et sådant

- Bekæmpelse af uønsket post (spam)
  Hvis du sender eller modtager e-mails, modtager du formentlig spam. Formentlig en masse spam. Har du nogensinde undret dig over, hvorfor du modtager så mange uønskede e-mails? Det er fordi, det er en god forretning. Det er billigt at sende millioner eller endda milliarder af e-mails. Og hvis blot en lille procentdel af 100 millioner mennesker køber noget på baggrund af en e-mail, så bliver det til mange købere!

- Få mere at vide om firewalls
  Med en god firewall til internettet kan du forhindre andre i at få adgang til din computer via internettet. Firewalls fås i to udgaver som software eller hardware, og de fungerer som en beskyttelsesbarriere, der er med til at forhindre, at andre tiltvinger sig adgang til computeren via internettet.Med en god firewall til internettet kan du forhindre andre i at få adgang til din computer via internettet. Firewalls fås i to

udgaver som software eller hardware, og de fungerer som en beskyttelsesbarriere, der er med til at forhindre, at andre tiltvinger sig adgang til computeren via internettet.

- Hvorfor man bør bruge en firewall på computeren
  Hvis du opretter forbindelse til internettet uden en firewall, svarer det til, at du lader bilnøglerne sidde i tændingen med motoren kørende og undlader at låse bildørene, mens du går ind i en forretning for at handle. Selvom du muligvis kan nå ind og ud, uden at nogen opdager det, er der stor risiko for, at der er nogen, som udnytter situationen. På internettet kan hackere bruge skadelig kode, f.eks. virus, orme og trojanske heste til at finde frem til de ulåste døre, som er den ubeskyttede computer. Ved hjælp af en firewall kan du beskytte computeren mod disse og andre typer sikkerhedsangreb.

- Valg og installation af et kabelnetværk
  Hvis du bruger et DSL- eller kabelmodem, får du en høj hastighed, men

- Derfor er sikkerhed vigtig
  Et af de største problemer inden for computersikkerhed er, at folk har svært ved at tro på, at de kan blive udsat for noget negativt – indtil det rent faktisk sker. Sandheden er, at der sker negative ting, og det sker oftere, end du måske selv tror. Computer Security Institute og Federal Bureau of Investigation (FBI) har foretaget undersøgelser, som anslår, at 90 procent af alle virksomheder og offentlige institutioner i 2002 har registreret brud på it-sikkerheden. Ud af disse virksomheder og offentlige institutioner erkender 80 procent at have lidt et økonomisk tab som følge heraf.

- Aktivering af Firewall til Internetforbindelse
  Du har formentlig hørt om ordet firewall. Enten på nyhederne, på arbejde eller måske endda fra andre familiemedlemmer. Men ved du, hvad det er? En firewall forbedrer kort fortalt sikkerheden på din computer.

- Øget sikkerhed med Internet Explorer
  Korrekt indstilling af Internet Explorer 6.0 forbedrer sikkerheden, når du surfer på Internet. Indbygget flerbrugerfunktionalitet betyder, at flere brugere kan have hver deres brugerprofil på samme computer. Windows XP er således som skabt til den moderne computer.

- Valg af internetudbyder
  Internettet er blevet en del af mange menneskers dagligdag. I denne artikel kan du læse om nogle af de ting, du bør overveje, inden du beslutter, hvordan du opretter forbindelse til internettet, og hvilken internetudbyder du skal benytte. Du får også nogle tip til, hvordan du kan forbedre computerens sikkerhed, mens du er online.

- En introduktion til begreberne kriminel hacking, vira og ondsindede aktiviteter
  ”Tid er værdifuld. Livet for kort til at skulle bekymre sig om computere”. Enig. Men for at forstå de trusler, som findes, og hvordan sådanne trusler skal håndteres, er du nødt til at vide lidt om teknikken. Bare rolig – det bliver holdt på et minimum.

- En computerorms livscyklus: Fra infektion til udryddelse
  På nuværende tidspunkt har du nok allerede hørt utallige advarsler om, at du ikke bør åbne vedhæftede filer i e-mails, medmindre du har tillid til afsenderen og samtidig forventede at modtage den vedhæftede fil. Den mest almindelige måde, som såkaldte orme (små skadelige programmer) spredes på, er, når folk åbner vedhæftede filer, hvis indhold de ikke kender. Hvordan bliver en computerorm egentlig spredt? Svaret på dette spørgsmål hjælper dig med at forstå de forholdsregler, du skal tage for at beskytte dig selv og andre.

- Microsoft konsulentydelser
  Vælg blandt en række konsulentydelser, som er baseret på Microsofts standardiserede arkitekturer og gennemprøvede ”best practices”. Ydelserne tilbydes af Microsoft og vores partnere.

- Oprettelse af et sikrere hjemmenetværk
  Hvis du bor i en husstand med to, tre eller flere computere, er du ikke den eneste. Og det er blevet lettere end nogensinde før at oprette forbindelse mellem flere computere, så du kan dele filer, printere og spil, eller så du kan surfe på internettet fra alle computerne i huset. I denne artikel kan du læse, hvordan du kommer i gang med at vælge et netværk, du kan bruge vores retningslinjer til at forbedre sikkerheden på dit nye (eller eksisterende) netværk

- Få øjeblikkelig besked om vigtige sikkerhedsopdateringer
  Microsoft tilbyder at sende dig en e-mail, som vil give dig besked, når vi offentliggør en vigtig sikkerhedsbulletin, eller når du fx får brug for at træffe dine forholdsregler mod en verserende trussel. På den måde hjælper Microsoft dig til at opretholde et sikkert computermiljø.

- Brug af sikkerhedsfunktioner i Office
  Mange bruger Microsoft Office-produkterne hver dag på deres arbejde og hjemme. Microsoft Office 2003 indeholder indbyggede sikkerhedsfunktioner, som er med til at beskytte dine oplysninger. I denne artikel kan du læse mere om, hvordan du kan udnytte disse funktioner til at forbedre forsvaret mod ubudne gæster. Selvom der ikke kan gives nogen garantier, så vil disse funktioner være med til at øge sikkerheden for dine personlige oplysninger.

- Tip til at være sikker, når du spiller online
  Onlinespil er ikke designet til mindre børn, men at spille videospil kan være en både sjov og lærerig aktivitet for de lidt ældre børn. Hvis du fastlægger nogle regler sammen med dit barn, og du sætter dig ind i de ressourcer og værktøjer, der er tilgængelige for forældre, kan du hjælpe med at sikre dit barn,

- Opdatering af Microsoft
  Windows Update er en onlinetjeneste, som du kan bruge til gratis at hente opdateringer til Microsoft-software. I denne artikel kan du læse, hvordan du kan hente de gratis opdateringer fra Windows Update. Artiklen omhandler også Windows Automatiske opdateringer, som du kan bruge til at hente opdateringerne automatisk. (Ikke tilgængelig i alle versioner af Windows). Men først en beskrivelse af brugen af Windows Update.

- Hvis du har ansvar for en stor Windows installation, så stil dig selv tre spørgsmål om driften: Fokus på Microsoft Operations Manager
  MOM står for Microsoft Operations Manager. Løsningen centraliserer alle driftsdata fra dine Windows servere. Det giver dig den centrale kontrol og overblik. MOM er skalerbart og understøtter fra én til tusindvis af servere.

- Bestået – og plads til endnu flere forbedringer
  I marts og april 2003 har vi kørt en spørgeskemaundersøgelse blandt vore partnere omkring branchens aktuelle sikkerhedsudfordringer. Resultatet er nu indløbet, og bedømmelsen af sikkerhedsniveauet er god, og vi kan kun være tilfredse med tilbagemeldingerne. Ikke mindst fordi vi i besvarelserne har fået mange gode ideer til, hvordan vi kan gøre det endnu bedre i fremtiden.Tak for det.

- Oprettelse af sikre adgangskoder
  Hvis du har mistet din pengepung, ved du, at det medfører problemer. Der kan f.eks. være nogen, der bruger dine identitetskort og dermed udgiver sig for at være dig. Hvis der er nogen, der har stjålet dine adgangskoder, kan de gøre nøjagtigt det samme online. En hacker kan f.eks. åbne nye konti, optage lån eller chatte online forklædt som dig. Og du finder først ud af det, når det er for sent.

- Fokus på sikkerhed og privatliv
  Men det nytter ikke noget, hvis man glemmer at låse hoveddøren. Og det samme gælder i den digitale verden: Bare fordi man kan dele data, er der ingen grund til at forære det hele væk.

- Sådan bekræftes det at en sikkerhedsrelateret meddelelse fra Microsoft er ægte
  Microsoft sender med jævne mellemrum en e-mail til abonnenterne på vores sikkerhedsbulletiner. Desværre har vi måttet konstatere, at ondsindede personer har udsendt falske bulletiner, som ser ud som om, de kommer fra Microsoft. Det kaldes i øvrigt for spoofing. Nogle af disse meddelelser lokker modtagerne ind på ondsindede websteder, hvor de risikerer at få overført ondsindet kode, mens andre indeholder en vedhæftet fil med en virus.

- Sikkerhed i Windows 2003 server
  Effektive og sikre netværk er gennem de seneste år blevet vigtigere, da mange virksomheder integrerer Intranet, Extranet og Internet. Windows 2003 server tilbyder et mere sikkert miljø til virksomheder. Det er bl.a. blevet nemt at kryptere filer og styring af softwaren kan sikre mod trojanske heste og virus.

- Sikkerhed anno 2003
  Microsoft har nu gennemført en omfattende opdatering af stort set hele Server familien, med de fire

Windows Server 2003 varianter i spidsen. Et kort kig ned over listen med nye funktioner og opdateringer illustrerer, at Microsofts udviklere denne gang har fokuseret på sikkerhed og pålidelighed, og derfor har man valgt at bygge videre på arkitekturen fra Windows Server 2000. Det skyldes, at denne arkitektur performer fantastisk og udgør et meget stabilt serverfundament. Desuden har dette valg givet Microsofts udviklere plads til at fokusere på optimering af sikkerheden i Windows Server 2003.

- Sikker onlineshopping
  Det kan være sjovt og nemt at handle i en veldesignet onlinebutik, der er åben 24 timer i døgnet og syv dage om ugen. Nogle gange måske lidt for sjovt og nemt!

- Sikkerhed på web og netværk
  Sikkerhed omkring netværksløsninger og webservere er den helt store udfordring for alle. Ved at være åben omkring problemstillingerne, melde ærligt ud og initiere en proaktiv politik på området fremstår en virksomhed dynamisk og troværdig i dag. Alle aktører gør sig de samme overvejelser og står overfor de samme sikkerhedsudfordringer. Derfor er der ingen grund til at skjule sikkerhedsspørgsmålet i form af en kommunikationsstrategi som ovenstående.

- Sikkerhedsindsats på rette vej – en statusrapport
  Ondsindet kode har været en fast følgesvend for alle, der har arbejdet med IT de sidste årtier. Men det er først inden for de seneste år, at internettet, lynhurtige bredbåndsforbindelser og millioner af nye enheder og netværk for alvor har skabt et globalt forum, der gør vira og orme i stand til at sprede sig til hele kloden på ganske få minutter.

- Øg sikkerheden ved surfing og brug af email
  Her er 4 trin, som hjælper dig med at afvise hackere og andre angribere. Ondsindede hackere og virusskribenter kan udnytte eventuelt lave sikkerhedsindstillinger i e-mail- og browsersoftware til at inficere din computer. Det kan de gøre ved at sende dig ondsindede e-mails eller lokke dig til at gå ind på et ondsindet websted. Hvis du forbedrer dine sikkerhedsindstillinger i Microsoft Internet Explorer, Microsoft Outlook og Microsoft Outlook Express, kan du selv være med til at begrænse din risiko for at blive ramt.

- Når slemme ting sker for gode virksomheder
  Din virksomhed er måske udsat for trusler hver eneste dag. Vira, angribere og selv brugerfejl, som sker ved et uheld, er alvorlige trusler, som kan få drastiske følger. De følgende historier illustrerer truslerne om ondsindede aktiviteter og resultatet af dem med eksempler hentet fra den virkelige verden. Historierne understreger betydningen af at tage forholdsregler, fordi hver enkelt trussel kan minimeres eller helt undgås. Dog er der ingen grund til panik. Denne vejledning forklarer, hvordan trusler skal vurderes, og hvordan din virksomhed tager de bedste forholdsregler. Det er altid bedre og billigere at lære af fejltagelser, som andre har begået, i stedet for ens egne. I denne vejledning kan du i afsnittet Introduktion til kriminel hacking, vira og ondsindede aktiviteter. læse om, hvordan internettet fungerer, og hvordan angriberne opererer.

- Valg af en softwarefirewall
  Der er konstant hackere, der forsøger at angribe computere, der har forbindelse til internettet. En firewall hjælper med at skjule din computer, når du er online, hvilket hjælper med til at beskytte computeren (og dine fortrolige oplysninger).

- Spam og junk
  I takt med, at flere og flere mennesker er kommet på Internet, er der helt naturligt opstået et enormt potentiale for reklame og salg på det globale medie. Den mest generende form for reklame er kendt som spam eller junk-email. Spam er en ulovlig form for markedsføring inden for EU. Desværre lader det ikke til, at det holder de fleste ”spammere” tilbage, og spam er da også langt fra et ukendt problem for private såvel som virksomheder i dag.

- Guide til, hvordan du udnytter det indbyggede spamfilter i Microsofts produkter
  Klik på knappen Organiser. Vælg Junk E-mail. Nu kan du vælge at sortere spam og emails med indhold, som du vurderer er uegnet for børn, fra. Slå spam-filtret til ved at klikke på knappen ud for Junk E-mail. Klik på linket nedenfor og tilføj emailadresserne eller domænenavnet på de kendte spammere, du bliver generet af...

- Håndtering af uønsket post (spam)
  Uanset hvor meget du har prøvet at undgå det, så har du modtaget en e-mail, som du ikke har bedt om. Og som du slet ikke ønsker. Hvad kan du gøre ved det? Først og fremmest skal du ignorere e-mailen. Hvis du besvarer den, vil du sandsynligvis modtage endnu mere spam. For det andet bør du melde den eller de personer, der har sendt e-mailen. I denne artikel kan du læse, hvad du kan gøre for at undgå uønsket post i fremtiden.

- Tag dine forholdsregler, og undgå at blive narret af falske websteder
  Julesæsonen er en hektisk periode, og mange forbrugere er derfor afhængige af, at det er nemt og hurtigt at købe ind online. Hører du til denne gruppe, skal du sikre dig, at du er lige så forsigtig på internettet som i et overfyldt indkøbscenter eller en gavebutik. Ellers risikerer du at blive udnyttet af folk, som ikke har reelle hensigter. I år er det uheldigvis sådan, at sæsonen for juleindkøb falder sammen med en stigning i antallet af falske websteder på internettet.

- Trin 10: Beskyt serverne
  Hvis du betragter dine servere som kommandocentret i netværket, er det indlysende, hvorfor det er kritisk at sikre dem mod angreb. Når dine servere først er ramt, vil hele dit netværk være i fare. Nogle angreb mod servere virker blot som et irritationsmoment, mens andre kan medføre alvorlige skader. Hvis du vil beskytte din forretning, skal du beskytte dine servere.

- Trin 11: Beskyt klienter
  Og når du så tror, at du overholder alle sikkerhedsregler til beskyttelse af aktiverne i din virksomhed mod vira og indbrudstyve, så kommer en medarbejder med en bedre ide. Eller rettere, det er den måske ikke – og den kan sætte alle de smarte sikkerhedsforanstaltninger, du har iværksat indtil videre, over styr.

- Trin 1: Opdater din software
  Windows Update er en onlinetjeneste, som du kan bruge til gratis at hente opdateringer til Microsoft-software. I denne artikel kan du læse, hvordan du kan hente de gratis opdateringer fra Windows Update. Artiklen omhandler også Windows Automatiske opdateringer, som du kan bruge til at hente opdateringerne automatisk. (Ikke tilgængelig i alle versioner af Windows). Men først en beskrivelse af brugen af Windows Update.

- Trin 2: Beskyt din computer mod vira
  Mange virksomheder opfordrer deres medarbejdere til at få influenza-vaccinationer, når sæsonen for influenza begynder. Nogle virksomheder betaler endda for det. Det kan være et smart træk! Hvis man i øvrigt ser bort fra omsorgen for medarbejderen, svarer en syg medarbejder til en ikke-produktiv medarbejder. Og hvis denne medarbejder smitter andre i kontoret, mangedobles dit problem ... Den samme holdning burde gælde dine computersystemer.

- Trin 3: opsætning af en firewall
  En telefon er en nødvendighed i de fleste virksomheder, også selv om du en gang imellem får uønskede opkald. Internettet er i dag en nødvendighed for mange virksomheder, men det åbner også døren op for uønsket kommunikation. Desværre kan uønsket internettrafik være et langt større problem end en irriterende telefonsælger. Det er grunden til, at du bør en betragte en firewall som en nødvendighed for din virksomhed, da den udgør den første forsvarslinje.

- Trin 4: Stram op på den interne sikkerhed
  Teknologi og internettet betød, at virksomhederne stod over for nogle helt nye sikkerhedsrisici. Men de betød ikke samtidig, at de gamle forsvandt! Sikring af dit fysiske miljø og gennemførelsen af en politik, som beskytter dine forretningsdata og aktiver er stadig af helt afgørende betydning. Et tilfældigt indbrud kan potentielt set medføre større skade, end hvis en ukendt og ubuden gæst angreb via internettet.

- Trin 5: Brug stærke adgangskoder
  Kraftige låse og tyverialarmer hjælper med til at holde ubudne gæster ude fra dit forretningssted. Brugen af stærke adgangskoder til computerne hjælper med til at holde ubudne gæster fra at kende til din forretning. Begge metoder er særdeles vigtige. Alligevel sker det alt for tit, at virksomheder investerer i det allernyeste inden for tyverialarmer til sikre de fysiske rum – og samtidig bruger de adgangskoder, som selv et barn kan knække, til at beskytte følsomme forretningsdokumenter.

- Trin 6: Lav sikkerhedskopiering af kritiske data
  Mange af de katastrofer, som rammer små virksomheder, skyldes udefrakommende kræfter – det kan være en dårlig økonomi, en naturkatastrofe eller en strømafbrydelse. Det kan ikke overraske nogen, at de, som overlever nedetiderne, typisk vil være dem, som har minimeret risikoen ved at træffe nogle grundlæggende forholdsregler. En af de mest grundlæggende forholdsregler er at sikkerhedskopiere alle kritiske forretningsdata.

- Trin 7: Tag intelligent webbrowsing til dig
  Hvis din virksomhed ikke har politik vedrørende brug af internettet, så er det på tide, at den får det. Selv om internettet kan være et utroligt godt værktøj på arbejdspladsen, kan det også øve en betydelig skade på arbejdspladsen og herunder medføre tab af produktivitet. Hvis du laver nogle regler, beskytter du din virksomhed ... og dine medarbejdere.

- Trin 8: Beskyt trådløse netværk
  Ingen bryder sig om at tænke på det værst tænkelige scenarium ... at der er nogen lige om hjørnet, som spionerer i dine forretningsaffærer eller tager sig en fritur på din regning. Men hvis din virksomhed har et trådløst netværk – og oplysninger, som du ønsker at hemmeligholde – kan lidt paranoia vise sig at være en fornuftig indgangsvinkel.

- Trin 9: Sikker tilslutning af fjernbrugere
  Muligheden for at forbinde fjernbrugere til virksomhedens netværk via internettet kan være en fantastisk styrkelse i forhold til virksomhedens effektivitet – og dermed din bundlinje. Men der er også en negativ side: Hvis dine medarbejdere kan tilslutte sig netværket, vil andre også kunne gøre det. Det er grunden til, at sikkerhed – herunder krypteringen og godkendelse – skal prioriteres.

- Microsofts initiativ – Trustworthy Computing
  Microsoft har som verdens største softwareudvikler et enormt ansvar for at beskytte vores kunders forretning mod ondsindet cyberkriminalitet, og imødekomme deres krav om optimal beskyttelse af personlige og følsomme oplysninger. Microsofts strategi hedder "Trustworthy Computing" og dækker blandt over følgende 7 tiltag, der allerede er sat i gang

- Sikkerhed – den største udfordring
  Der er nok ingen som har kunnet undgå at bemærke, hvor intenst der tales om virus, hackerangreb, beskyttelse af privatlivets fred, digitale signaturer og mange andre emner der vedrører IT-sikkerhed. Beskyttelse af vores teknologiske infrastruktur er på rekordtid er blevet en hel industri for sig selv. Microsoft ligger helt i front af denne udvikling, og bruger enorme ressourcer for at holde en position som markedsledende, når det gælder om at lave verdens mest sikre software.

- Tip til vedligeholdelse af computeren
  Du er måske ikke klar over det, men der er en ting, som din computer og din bil har til fælles: begge kræver regelmæssig vedligeholdelse. Det betyder ikke, at du skal skifte olie på computeren. Men du skal sørge for at opdatere softwaren, opretholde et abonnement på et antivirusprogram og kontrollere, at der ikke er installeret spyware. I denne artikel kan du læse mere om, hvordan du forbedrer sikkerheden på computeren.

- Tips til bekæmpelse af computer virus
  Når du hører om en computervirus, der er aktiv, er det på tide at dobbelttjekke, at din computer ikke er sårbar over for - eller spreder - virusen. Udover de forebyggende foranstaltninger, du kan træffe, er der nogle ting, du skal gøre, hvis du tror, du har virus, for at fjerne problemet fra computeren.

- Introduktion til virus, orme og trojanske heste
  Virus, orme og trojanske heste er ondsindede programmer, der kan skade din computer og dine oplysninger på computeren, nedsætte hastigheden på internettet og bruge din computer til at sprede sig til dine venner, familie, kolleger og resten af internettet. Det positive er, at du med lidt forebyggende arbejde og lidt sund fornuft kan undgå en stor del af disse trusler.

- Sådan bekæmper du virusangreb på computeren
  Når du hører om en computervirus, der florerer på Internettet, skal du sikre dig, at din computer ikke er modtagelig over for et angreb eller kan risikere at videresende inficerede e-mails eller filer. Ud over de forebyggende forholdsregler du kan træffe, er der en række ting, du skal gøre for at fjerne en virus, hvis din computer er inficeret.

- Fokus på virus og hackere: Kører du på en Windows platform, så stil dig selv tre enkle spørgsmål om sikkerheden i din virksomhed
  1. Er min pc installation sikret bedst muligt mod angreb? 2. Har jeg implementeret metoder og værktøjer som holder sikkerheden ved lige? 3. Har jeg installeret sikkerhedsopdateringer fra Microsoft? - Hvis du kan svare ja til alle tre spørgsmål, kan du sove roligt om natten. Svarer du derimod nej eller ved ikke, er der hjælp at hente:

- Valg af trådløst netværk
  Hvis du har mere end én computer hjemme, har du muligvis et netværk. Et netværk er ganske enkelt to eller flere computere, der har forbindelse til hinanden. Mange netværk bruger en masse kabler, som ligger og roder. Og alt efter hvor dine computere står, risikerer du også at falde i kablerne. Men ved hjælp af den trådløse teknologi kan du slippe for alt dette. Du kan bruge et stykke hardware, der hedder en trådløs router, til at oprette forbindelse mellem computerne og til internettet.