Säkrare Internetsurfning

Det finns bättre sätt än att sluta använda Internet.

Riktigt säker kan du aldrig bli, men med lite förståelse för hur Internet fungerar och med ganska enkla medel kan du göra din egen och andras tillvaro tillräckligt säker för att Internet med webb och e-post ska kunna vara en tillgång istället för en belastning.

Bengt-Göran Carlzon
Faktorivägen 8B
691 33 Karlskoga
Tel: 0586-690 27
Mobil: 070-585 24 44
E-post: cosmos.data@telia.com
Hemsida: http://www.cdik.se

Några enkla tips för att "surfa" säkrare:

1. Öppna inte bifogade filer från okända personer!
   Sådana filer kan medföra obehagliga överraskningar
   Små program kan innehålla så kallade ”hacker-verktyg”
   När du kör ett sådant program installeras en öppen "bakdörr" i systemet.
   På detta sätt kan obehöriga personer få tillgång till din information.
   Virus installeras också vanligtvis när du kör ett sånt här program. Det finns ännu inga virus som kan överföras med vanlig text.

2. Svara inte på skräppost!
   Om du returnerar skräppost (s.k. spam) riskerar du att ditt epostsystem översvämmas av epostmeddelanden, som kan blockera systemet.

3. Använd "starka" lösenord samt håll dem hemliga!
   Använd både versaler och gemener, samt tecken och siffror.
   Håll lösenordet hemligt.
   Genom att ändra lösenord ofta förhindrar du att obehöriga personer får tillgång till ditt Internetkonto och dina epostmeddelanden hos Internetleverantören.

4. Logga ut från Internetkontot när du inte använder det!
   Genom att logga ut stänger du din anslutning och skadliga program kan inte överföras.

5. Med en öppen anslutning ökar risken för att obehöriga personer ska få tillgång till din information - ju längre tid Du är uppkopplad mot Internet och ju fler Internet-program Du har igång samtidigt desto större är risken att bli utsatt av angrepp!

6. Håll ditt operativsystem uppdaterat!
   För att åtgärda problem som kan göra datorn sårbar för virus eller maskar släpper Microsoft då och då kritiska uppdateringar till Windows och Office.
   Det är därför en bra idé att besöka webbplatsen Windows Update/Office Update regelbundet för att få information om uppdateringar och förbättringar.

7. Använd antivirusprogram!
   Genom att använda antivirusprogramvara minimerar du risken för att din dator ska utsättas för virus. Tänk på att uppdatera din antivirusprogramvara regelbundet.

8. Kör inte program direkt från Internet!
   Om du vill använda ett program hämtar du det först till din hårddisk. Därefter kan du kontrollera programmet med ett antivirusprogram.
   Hämta bara program från webbplatser som du anser vara säkra.

Ladda ner aktuella säkerhetsuppdateringar!

Nya uppdateringar till operativsystem, webbläsare, och e-postprogram och säkerhetsprogram släpps efterhand som det upptäcks säkerhetshål.
Säkerhetsbrister finns i alla Windows-versioner, men uppdateringarna finns nästan endast till Windows NT-versioner (NT, 2000 och XP).
Låt dig dock inte förledas att tro att du skulle vara säker med Windows 95, 98, 98SE eller ME som bygger på en mer osäker arkitektur.

Dela inte ut filer!

Om Du delar ut filer och/eller mappar så är Din dator på detta sätt vidöppen för angrepp!

Installera ett antivirusprogram!

Uppdatera med jämn intervall.
Använd gärna antivirusprogrammets funktioner för att skanna inkommande mail och sätta en certifieringsstämpel på utgående!

Virus
Den första typen kallas virus och har gett det något missvisande samlingsnamnet till all skadlig kod.
Virus kännetecknas av att de kopierar sig själva från fil till fil och därmed infekteras mer och mer av den drabbade datorn.
Ordet datorvirus började användas år 1983 av den amerikanske forskaren Fred Cohen.

Mask (engelska worm)
är den andra typen kopierar sig vidare mellan datorer (ofta med hjälp av e-post) för att spridas och infektera så många datorer som möjligt.

Trojan
är den tredje typen där den skadliga koden finns i ett program eller en bit kod som i sig verkar ofarlig.
Uttrycket kommer från Homeros bok Iliaden där det beskrivs hur grekerna tog sig in i staden Troja genom att gömma sig en stor trähäst som stadens invånare inte trodde var farlig och därför släppte in i staden.
En trojan i IT-sammanhang inväntar en förutbestämd tidpunkt, instruktioner utifrån eller lämpligt tekniskt tillfälle för att utföra sitt uppdrag.

Ett "e-postvirus" fungerar vanligen så här:
1) En dator blir virusangripen.
2) Virusprogrammet går igenom datorns e-postprogram i jakt på användbara adresser, väljer en adress på måfå som avsändare och skickar post till resten med denna slumpmässigt valda adress som avsändare.

Installera en brandvägg!

Skydda datorn mot intrång.

E-postsäkerhet!

Klicka ALDRIG! på bilagor som inte avsändaren begripligt beskriver innehållet i.
Detta gäller alltid och utan undantag - att posten kommer från någon som är bekant spelar igen roll.
Du kan alltid e-posta tillbaka och fråga vad det är i stället för att direkt klicka på bilagan.

Ställ in Windows så att systemet visar filändelser.
Om en bilaga har dubbla filändelser, ex.: Humor.doc.as, öppna den inte!
Virusscanna gärna .exe-, .vbs-, .doc-filer innan de öppnas.

Det förekommer med jämna mellanrum utskick som ser ut att komma från t.ex. Microsoft (s.k. spoofing) ang. säkerhetsuppdatering.
Seriösa företag sänder ALDRIG ut e-post med denna uppmaning!
Detta är endast ett försök att få dig att besöka webbsidor och/eller ladda hem skadlig kod.

På senaste tiden har det också börjat komma e-post som ser ut att vara från banker, kreditkortsföretag m.fl.
I denna e-post uppmanas Du att skriva in kontonummer och lösenord i ett formulär - för att företagen skall uppdatera sina register.

Seriösa företag ber ALDRIG om kundernas kontouppgifter - detta är endast försök att komma åt dem (s.k. phishing) för att tömma Dina konton!

KASTA BORT DENNA E-POST!!

Modemkapning!

Modem kapas genom att ett program laddas ner från Internet - oftast utan att Du vet om det. Programmet bryter Din anslutning till Internet och ringer sedan upp ett betalnummer som resulterar i en hög telefonräkning. Om Du har modemljudet på så hör Du om det kopplar ner och ringer upp ett annat nummer. Du är ändå inte helt säker, eftersom det finns vissa program som även kan stänga av ljudet på ditt modem. För att undvika dyra telefonkostnader om modemet ”kapas” kan du spärra din telefon för betalsamtal hos din teleoperatör. Om du skulle råka få fakturor för tjänster som du inte avtalat om bör du alltid tillbakavisa dessa.

Töm mappar regelbundet!

Det samlas massor av "skräpfiler" på datorns hårddisk. Dina internetvanor kan kartläggas med hjälp av dessa filer. Öppna Kontrollpanelen och klicka på Internetalternativ. Under fliken Allmänt kan Du sedan klicka på Ta bort cookies, Ta bort filer, Rensa tidigare. Mapparna töms dock ej hundraprocentigt.
Vill Du tömma mapparna helt så får Du leta upp och tömma dem manuellt i utforskaren.

Det finns en hel del s.k. "clean"-program som hjälper till med utrensningen.
Det är dock på plats med en varning för att dessa program ibland tar bort för mycket. Så man skall verkligen veta vad man gör (och vad programvaran gör)!

Spyware!

samlar data om vilka webbplatser Du besöker och skickar detta vidare till programtillverkare. Skaffa program som genomsöker hårddisken efter Spyware och tar bort dessa.

Förslagsvis:

Ad-Aware
http://www.snabbstart.com/download/ad-aware

Spybot - Search & Destroy
http://www.safer-networking.org/sv/download/index.html

Spam!

Oönskad skräppost – SPAM – är oftast mer besvärande än det är en säkerhetsrisk, men virus kan spridas med hjälp av spam.
Från och med första april 2004 är det förbjudet att skicka e-postreklam som inte är beställd.
Lagen gäller inte all "SPAM" utan bara meddelanden med ett kommersiellt syfte. Opinionsbildning, upplysningar och liknande budskap får man däremot skicka.

Varför oönskad e-post kallas SPAM är inte helt klarlagt.
Mycket tyder på att det har sitt ursprung i en Monty Python-sketch där ordet SPAM upprepas så ofta att det dränker alla samtal.
SPAM är ett varumärke för en billig grisköttskonserv som lanserades av amerikanska Hormel Foods 1937.
Det finns ett par typer av skräppost som du bör vara extra uppmärksam på - falska virusvarningar (HOAX) och investeringsbedrägerier.

Falska virusvarningar – HOAX.

I dessa så påstår man sig ha upptäckt mycket farliga virus som antivirusföretagen inte har kunnat ta fram motmedel mot och Du uppmanas att skicka varningen vidare.
Just att man skickar många varningsmail kan ju i och för sig betraktas som ett virus.
Säkerhets- och Antivirusföretaget F-Secure har en sida där Du kan söka efter kända hoax.

Hoax som fått stor spridning är uppmaningar att ta bort vissa filer – ex.:
sulfnbk.exe och jdbgmgr.exe.
Dessa filer ingår normalt i Windows.
sulfnbk.exe hanterar långa filnamn
jdbgmgr.exe är en felsökningshanterare.
Ta inte bort dessa filer från datorn!

Investeringsbedrägerier, ofta i form av så kallade Nigeriabrev, utlovar snabba pengar utan någon större insats från dig. Ytterligare en form av massbrev är dessa fantastiska erbjudanden om mobiltelefoner, datorer m.m. Vidarebefordrar Du meddelandet till ett antal personer och sedan redovisar till ett stort företag påstås Du få olika varor gratis. Dessa erbjudanden har endast ett syfte: Att fylla Din postbox!

Slutord!

Tänk dig för innan du lämnar ut information om dig själv såsom namn, adress eller personnummer.
Om en webbplats kräver mycket information om dig bör du ifrågasätta detta och vara försiktig om det inte framgår tydligt hur uppgifterna kommer att användas.

Ladda aldrig ned program eller filer om Du inte känner igen dem eller inte litar på avsändaren.
Var skeptisk mot program som kommer via e-post eller erbjuds på en chatt.
Var också försiktig med att kryssa i så kallade popupfönster, som ibland dyker upp på din skärm, där du ombeds att ladda ned en fil från en webbplats.
Ta för vana att först spara filen på din hårddisk och sedan kontrollera den med ditt antivirusprogram.

Välkommen in i cybervärlden!