

DATORSÄKERHET FÖR NYBÖRJARE

Om att skydda dig själv och din dator mot attacker, stölder, förstörelse och bedrägerier

En e-bok av

Tommy k Johansson

blogg.tkj.se

(C)2009-2010, TkJ Data & Media

Får ej vidare distribueras utan upphovsmannens tillstånd.

Förord

Har du någon gång drabbats av virus, trojaner, spyware, falska säkerhetsprogram eller andra former av bedrägerier, stölder och dataförstörelse? **Då är du inte ensam.**

Marknaden för datorvirus och liknande hot mot datorer och dess användare, har **exploderat till en miljonbransch** där cyberskurkar tjänar massor av pengar på att utnyttja Internetanvändares rädsla och naivitet.

Det är inte helt omöjligt att du har en dator som redan idag är smittad av en trojan, utan att du vet om det. De arbetar i det tysta och deras syfte är att låta cyberkriminella komma åt din dator för att stjäla information, för att använda den för att sprida virus och skräppost, och för att genomföra attacker mot servrar och företag.

Virus är inte längre någonting som bara drabbar okunniga användare som surfar på suspekta webbsajter och laddar ner piratspel. Det är något vem som helst kan drabbas av, om man inte har rätt skydd och inte känner till hur man ska tänka och agera.

Den här boken riktar sig till **alla som vill veta mer om säkerhet på Internet**, som vill lära sig att installera de bästa skydden och dessutom känna till de smartaste men enklaste tipsen om att effektivt undvika farorna.

Jag hoppas att du får mycket nytta av den här e-boken!

Trevlig läsning!

Tommy k Johansson

Tkj är Sveriges största IT-bloggare och har skrivit om datorer och Internet för en lång rad datortidningar, nyhetsbrev och webbsajter sedan mitten av 90-talet. Du kommer i kontakt med honom via e-post johansson@tkj.se.

Vad är datorvirus, trojaner och spyware?

Datorvirus har blivit ett samlingsnamn för en stor mängd farlig kod. I folkmun brukar vi kalla den mesta farliga kod för datorvirus idag – på engelska *malware*. Egentligen finns det massor av olika typer av virus, där maskar och trojaner är mest kända.

Maskar är virus som försöker sprida sig vidare via exempelvis säkerhetshål i programvaror och operativsystem. **Trojaner** är virus som gömmer sig genom att framstå som ett legitimt program, men i bakgrunden körs farlig kod. Det kan vara elektroniska vykort, småspel och annat.

Ett **spyware** – spionprogram på svenska – är en typ av program som spionerar på användaren. Det försöker ta reda på personliga uppgifter genom att exempelvis lyssna av tangentbordet och skicka vidare datan till virusskaparen.

I samma område som spyware brukar man nämna **adware**, en sorts ”virus” som utsätter dig för olika former av reklam. De vanligaste tecknena på att du har blivit smittad är nya verktygsfält i din webbläsare, suspekta ikoner på skrivbordet, att din startsida ändras och att du får nya länkar i dina bokmärken (vanligtvis till kasinosajter). Du lär också utsättas för mängder av popuper med reklam.

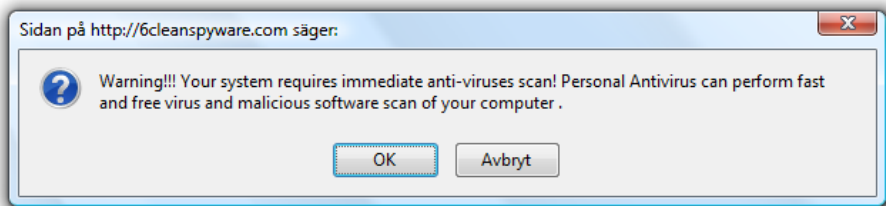
Men det här är en massa tekniska termer du inte behöver känna till. **Du kan kalla allt för datorvirus eller farlig kod.** Dess syfte är idag alla desamma – att på något sätt försöka tjäna pengar på den smittade användaren.

Cyberkriminaliteten ökar för varje dag som går, och de sysslar med alla möjliga former av bedrägerier för att **lura användare på pengar och personliga uppgifter**. De senare säljs vidare på den svarta marknaden. Inloggningsuppgifter och kontokortsnummer är saker som lätt säljs dyrt.

En **vanlig missuppfattning** är att man bara drabbas av virus om man laddar ner piratkopierade program och spel, och om man surfar runt på väldigt

suspekta sajter med så kallade cracks och dylikt. Det är sant att denna typ av aktivitet onekligen ökar riskerna att drabbas, men det är inte alls sant att du är säker bara du undviker dem.

En dag under slutet av 2009 började besökare av **New York Times** hemsida få upp ett fönster som varnade dem för att deras datorer blivit infekterade av hemska virus. För att lösa problemet ombads man att ladda ner ett antivirusprogram, som sedan krävde registrering för hundralappar för att rensa datorn. **Allt det här var rent bedrägeri.** Annonserna kom från en tredjepartsleverantör av webbannonser, där man inte varit tillräckligt uppmärksam på sina kunder.



Figur 1: Typisk dialogruta som försöker lura användaren att ladda ner ett falskt antivirusprogram – i det här fallet Personal Antivirus.

Vad det här visar är att farliga länkar och annonser kan dyka upp var som helst. Kan självaste NY Times drabbas, är du inte säker någonstans. Du skulle bara veta hur många farliga annonser det visas i annonssystem där kunderna sköter allt själva – såsom Google AdWords, som finns på miljontals sajter och framför allt hos Google själva!

Jag lägger absolut inte skulden på Google. Det är helt omöjligt för dem att kontrollera alla annonser. Men det är viktigt att poängtera att du inte är säker, var du än befinner dig på Internet. **Kunskap och rätt säkerhetsapplikationer är ett måste** för att du ska kunna skydda dig och din dator.

Det är detta du lär dig i den här e-boken!

Botnäten som kontrollerar din dator

En av den vanligaste formen av virus (trojaner) som finns idag, infekterar datorn utan att ge något väsen av sig. När datorn är infekterad kommer den att koppla upp sig mot ett nätverk som kallas för **botnät** (engelska *botnet*).

Man brukar kalla en dator som blivit infekterad av en botnät-trojan för en **zombie**, eftersom det inte längre än användaren som har kontroll över PC:n, utan de cyberskurkar som kontrollerar botnätet.

Det finns idag miljontals datorer som är zombies, och det finns botnät som kontrollerar hundratusentals datorer. Dessa nätverk erbjuder datorkraft som är betydligt mer omfattande än de mest avancerade stordatorer. Och prestandan används inte till goda gärningar.

Botnäten används för att skicka ut skräppost (*spam*) och virus, för att genomföra olika former av attacker, och mycket annat. Många sådana här virus söker även igenom hela den infekterade datorn, och alla lagringsmedier som kan komma åt, efter personlig information, för att sedan skicka vidare denna till cyberskurkarna.

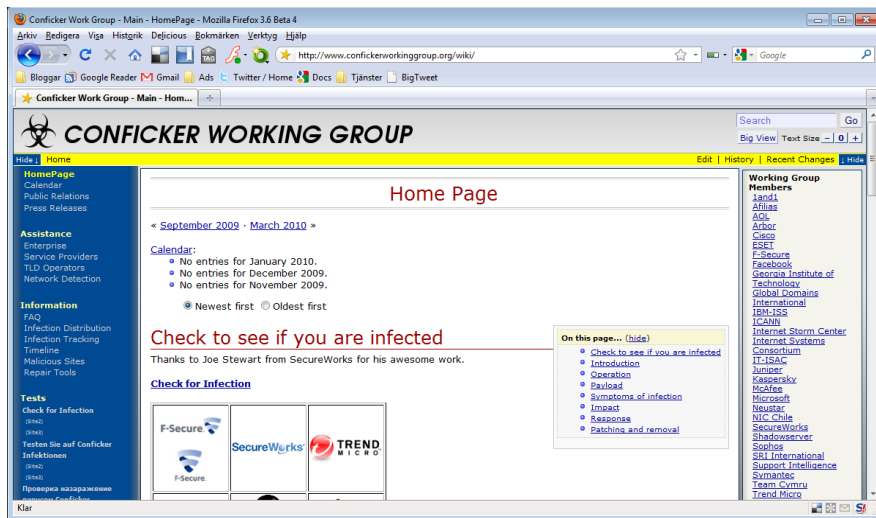
Viruset arbetar i det tysta. De har väldigt sofistikerad teknik som gör sitt yttersta för att inte märkas på något sätt. Många gör framgångsrika försök att stänga av antivirus, brandvägg och andra säkerhetsprogram. De syns inte i *Aktivitetshanteraren* eller andra vanliga verktyg för att visa aktiva applikationer.

Därför kan de arbeta i bakgrunden utan att datorns användare vet om att han **varje dag skickar iväg tiotusentals skräppost** med reklam för potenspiller och suspekta lån, eller hjälper till att attackera ett företags servrar för utpressning. Det händer att Internetleverantörer stänger av kunder som har smittats av sådana här former av virus eftersom Internettrafiken från datorn är rätt omfattande.

De som driver botnäten hyr ut sin kapacitet till andra skurkar som vill distribuera ut skräppost eller farlig kod. Man har till och med speciella provisionsavtal där botnätsens ägare får betalt per tusen datorer som installerar en programvara som sprids via botnätets datorer.

Botnäten anses av många säkerhetsexperter vara den största faran på Internet idag.

En av de mest kända trojanerna som skapar botnät är **Conficker**, som fick enormt stor uppmärksamhet under början av 2009. Flera antivirusföretag gick samman för att slå bort Conficker och man lyckades rätt bra. Men Conficker har fortfarande stor kontroll över datorer på Internet.



Figur 2: Viruset Conficker var så omfattande att säkerhetsföretagen gick samman och bildade Conficker Working Group.

Skydda din dator med säkerhetsprogram

Det finns två sätt du måste skydda dig själv och din dator på. Det ena är **kunskap om hur du använder Internet på ett säkert sätt**, och det andra är att **installera och köra bra säkerhetsprogram** som försöker hindra farlig kod från att komma in i din dator.

Tre typer av programvara är grundläggande för att ge ett bra skydd av din dator; **antivirus**, **antispysware** och **brandvägg**. Marknaden är full av olika alternativ för dessa program, och ofta brukar man dela in dem i kommersiella säkerhetspaket och gratisprogram.

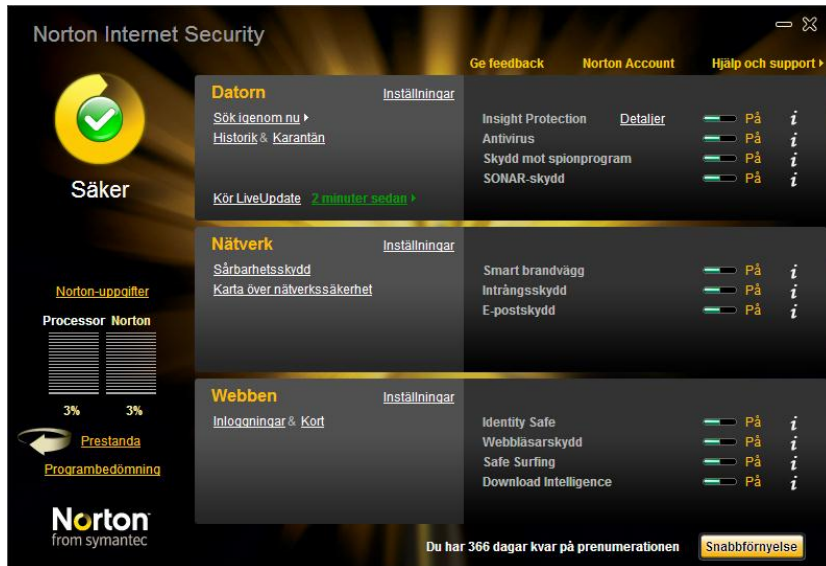
Några välkända kommersiella säkerhetspaket är:

- [Symantec Norton Internet Security](#)
- [F-Secure Internet Security](#)
- [Kaspersky Internet Security](#)
- [McAfee Internet Security](#)
- [Panda Internet Security](#)

Dessa är alla **kompleta programpaket** som ger dig ett riktigt bra skydd. De innefattar såväl antivirus som antispysware och brandvägg, och dessutom har de många andra smarta säkerhetsfunktioner för att hindra bedrägerier, hjälpa föräldrar att kontrollera var deras barn surfar någonstans, varna för farliga webbsidor och så vidare.

Under de senaste två åren har samtliga utvecklare av säkerhetspaket inriktat sig mycket på att göra sina program **enklare att använda och framför allt mindre krävande av datorn**. Tidigare har programmen slöat ner datorn eftersom de varit så fullproppade av onödiga funktioner.

Sedan versionerna som kom 2008 har man trimmat verktygen ordentligt, och det blev ännu bättre under 2009 (de versioner som kallas för 2010 av utvecklarna). **Dessa är väldigt snåla på prestandan.** Symantec Norton tar bara några få MB av internminnet och knappt märkbart av processorn. Syftet är att programmen ska köras i bakgrunden utan att störa användaren.



Figur 3: Symantec Norton Internet Security är ett riktigt bra säkerhetspaket.

Fördelarna i att investera i ett kommersiellt säkerhetspaket är att **du får en komplett lösning**. De innehåller allt du behöver och de är integrerade under ett tak, vilket gör att du inte behöver köra en massa olika applikationer. **Dessutom kommer de med support** – flera av dem har svensk supporttelefon för dig som vill ha hjälp av proffs.

I de flesta tester brukar [Symantec Norton](#) gå ut som vinnare, och jag kan själv rekommendera programmet efter att ha testat flera av de aktuella säkerhetsprogrammen. De övriga är också väldigt bra, men Norton Internet Security är så enkelt att använda och tar så lite kraft av datorn, att det enligt

mig numera är det bästa valet. Kritiken som historiskt sett finns mot att Symantecs program har varit sega och resurskrävande är inte längre gällande.

Gratis antivirusprogram

De gratis antivirusprogrammen är ett bra alternativ för dig som inte vill betala för säkerhetspaket. **Istället för att strunta i det helt, skaffa ett gratisprogram.** Dessa kostnadsfria programmen ger ett bra grundläggande skydd, fast de har inte så många funktioner som de kommersiella.

Bakom gratisprogrammen står företag som även utvecklar mer avancerade kommersiella versioner av sina program. Gratisversionerna kommer oftast bara med de vanligaste finesserna, och dessutom kan det vara så att man prioriterar uppdateringar till betalande användare.

Om du vill satsa på gratis säkerhetsprogram behöver du ett antivirus och ett antispyware. En del gratis antivirus har även antispywareprogram, men jag anser att det är bra att komplettera detta med ett bättre sådant.

Här är värt att anmärka att du **aldrig får installera två antivirus samtidigt** på din dator. De kommer nämligen att krocka med varandra. Däremot går det bra att köra fler än ett antispyware, även om det är rätt onödigt att belasta datorn med det.

De tre gratis antivirus jag rekommenderar idag är:

- [Panda Cloud Antivirus](#)
- [Avast! Free Anti-Virus](#)
- [Microsoft Security Essentials](#)

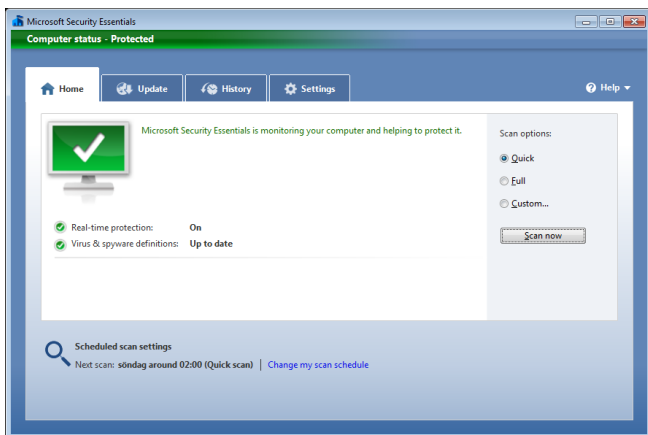
Dessa program har alla sina för- och nackdelar. Avast! är ett klassiskt antivirusprogram utan några större konstigheter. Gränssnittet är aningen konstigt, men det fungerar bra och får goda recensioner i tester.

Panda Cloud Antivirus är i skrivande stund min personliga favorit. Det är resurssnålt och det är väldigt enkelt att använda. Gränssnittet i programmet är extremt sparsmakat och dess syfte är att så tyst som möjligt skydda dig mot virusangrepp. Det lyckas det bra med.

Pandas gratis antivirusprogram arbetar inte med så kallade virusdefinitioner, som är listor över viruskod som antivirusprogram använder sig av för att identifiera virus. Istället arbetar Panda Cloud Antivirus i molnet (*cloud computing*), vilket betyder att det kommunicerar med Pandas säkerhetsservrar över Internet för att kontrollera filer som laddas ner och kopieras till datorn.

Den här tekniken har de flesta säkerhetsföretag börjat använda i sina programvaror, eftersom det ger ett **väldigt effektivt och uppdaterat skydd**. Istället för att försöka få alla miljontals användare världen över att ladda ner nya uppdateringar till sina antivirus, räcker det att uppdatera datan på sina egna servrar.

Som användare kan du med Panda Cloud Antivirus glömma all form av vanlig uppdatering som antivirusprogram annars brukar kräva flera gånger om dagen.



Figur 4: Microsoft Security Essentials är ett bra gratis antivirusprogram.

Microsoft Security Essentials har fått väldigt bra testresultat. Det arbetar med klassiska uppdateringar och skyddar förutom mot virus även mot spyware. Det har visat sig vara effektivt och kan rekommenderas.

Att använda ditt antivirus

Ett antivirusprogram som arbetar med **signaturfiler**, eller definitionslistor, fyller föga nytta om det inte är uppdaterat. Virus sprids otroligt snabbt idag och det gäller att uppdatera programvaran kontinuerligt. Flera av de kommersiella programmen uppdateras så snabbt som var femte minut. En del gratisprogram uppdaterar sig bara en eller två gånger per dag. Se till att du håller den här rutinen så kontinuerlig som möjligt.

Med Panda Cloud Antivirus behöver du inte bry dig om uppdateringar, eftersom det inte använder några definitionslistor. Däremot bör understrykas att själva programvaran ibland kommer i en ny version och då behöver du uppdatera. Det är dock inte samma sak, och det händer inte speciellt ofta.

Du bör också **kontinuerligt genomföra en komplett skanning av din dators lagringsenheter**. Även om antivirus skyddar mot att virus installeras, finns det möjlighet att farlig kod slinker igenom och ligger på din hårddisk. En ordentligt skanning tar hand om det här.

Gratis antispywareprogram

Spyware och virus är inte samma sak. Faktum är att spyware och adware kan vara legala och en del gratisprogram som du laddar ner och installerar från Internet kommer med spyware. Detta står i licensavtalet, men ärligt talat, hur många läser igenom licensavtalen? De flesta klickar bara *Godkänn* och kör på.

Det finns många gratis antispyware, varav två jag fastnat för: [Lavasoft Ad-Aware](#) samt [Spybot Search&Destroy](#). Ad-Aware har funnits på marknaden i över tio år, och utvecklas faktiskt i Göteborg.

Det är väldigt effektivt och de nya versionerna av gratisalternativet (programmet finns även i kommersiell version) har även **realtidsskydd** – det vill säga att det skyddar dig från att spyware installeras. Tidigare har Ad-Aware Free bara låtit dig söka igenom datorn efter spyware och adware som redan installerats.

Spybot är också mycket effektivt, och enligt min erfarenhet ger ofta Spybot ett bättre skydd än Ad-Aware. Det här är inget jag baserar på omfattande tester, utan en uppfattning jag har fått under mina år som IT-skribent.

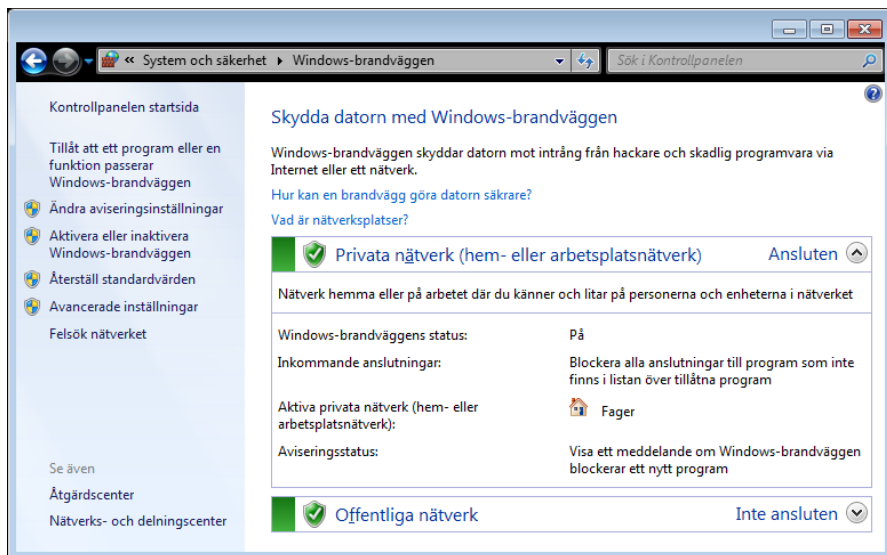
I likhet med Ad-Aware erbjuder även Spybot realtidsskydd. Det ligger resident i minnet och försöker hindra installationer av skräpprogram. Det har även andra skydd mot exempelvis oönskade ändringar i Windowsregistret, vilket är bra.

Windowsregistret är en databas som innehåller alla inställningar i Windows och de program du har installerat. De flesta spyware och adware lägger in sig som autostartande program som kör igång i bakgrunden när Windows startar, och detta görs genom ändringar i registret. Stoppas du dessa, kommer du långt.

Gratis brandvägg

En brandvägg är en programvara som hindrar oönskad trafik till och från din dator. Det här är väldigt viktigt. Många virus utnyttjar säkerhetshål i program och operativsystem och genomför attacker via nätverket (och därmed Internet). En brandvägg sätter stopp för den mesta trafiken av denna typ.

Som exempel kan nämnas viruset **Blaster**, som utnyttjade ett säkerhetshål i Windows XP. En infekterad dator sökte efter öppna datorer på Internet och försökte infektera dem. När Blaster var som mest aktivt räckte det, för en dator med ett ouppdaterat Windows och utan brandvägg, att vara ansluten till Internet i genomsnitt ett par sekunder innan datorn infekterats.



Figur 5: Windowsbrandväggen som medföljer Windows 7 fungerar fint.

Om du har Windows XP Service Pack 2, eller senare (Vista eller Windows 7), har **Windows en egen brandvägg** som fungerar bra. Den heter Windowsbrandväggen och finns i Kontrollpanelen. Windowsbrandväggen är påslagen som standard, så som regel har du ett rätt bra skydd.

Kommersiella säkerhetspaket har brandvägg som en av funktionerna och dessa ger ofta fler funktioner än Windowsbrandväggen. Om du vill ha ett bättre alternativ än Windows egna, finns det så klart gratisprogram att dra nytta av. En klassiker är [Zone Alarm](#).

I de kommande två kapitlena ska jag förklara hur du snabbt kommer igång med Panda Cloud Antivirus respektive Spybot Search&Destroy.

Installera Panda Cloud Antivirus

[Panda Cloud Antivirus](#) finns i svensk version, och på hemsidan väljer du *Svenska* uppe i menyn *Language*. Därefter klickar du *Hämta det nu* för att ladda ner programmet. Installationsfilen är på cirka 22 MB.

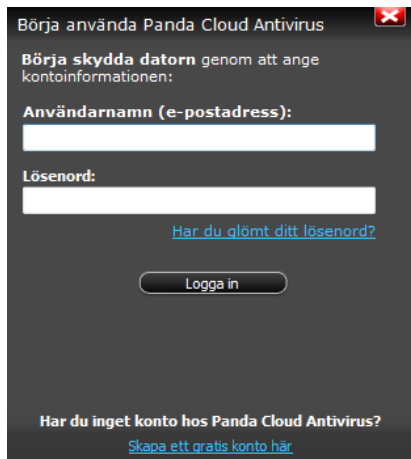
När du laddat ner den klickar du igång programmet, efter att du noggrant **avinstallerat ditt tidigare antivirus**. Det är en god idé att koppla ifrån dig från Internet under tiden du avinstallerar ditt aktuella antivirus och installerar Panda Cloud Antivirus, så att du inte råkar bli infekterad under tiden du är utan viruskydd.

Om du har problem att avinstallera ett antivirus, kan du söka efter removal-verktyg, då de flesta utvecklare erbjuder ett sådant. Du kan även prova verktyget [AppRemover](#) som är till för att ta bort säkerhetsprogram och som är gratis att använda.



Själva installationen är inte mycket att orda om. Det ser ut ungefär som när du installerar vilket program som helst. Inledningsvis får du en fråga om att acceptera licensavtalet och installera, och här finns även en kryssruta om att förse Panda med information om potentiellt farliga filer. Jag rekommenderar att du har denna ikryssad för bästa skydd.

Panda Cloud Antivirus kräver att du registrerar dig som medlem, vilket är helt gratis och det tar bara någon minut. Det är inte mycket mer än e-postadress och lösenord som behövs för att du ska komma igång. Har du inget konto klickar du *Skapa ett gratis konto här*.



Börja använda Panda Cloud Antivirus

Börja skydda datorn genom att ange kontoinformationen:

Användarnamn (e-postadress):

Lösenord:

[Har du glömt ditt lösenord?](#)

Logga in

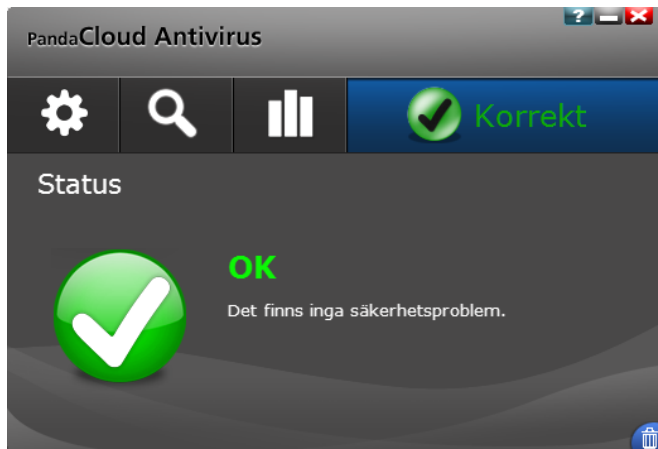
Har du inget konto hos Panda Cloud Antivirus?
[Skapa ett gratis konto här](#)

Om du installerar Panda Cloud Antivirus under Vista eller Windows 7 är det troligt att Windows frågar dig om du verkligen vill köra programmet. Det här är Windows egna säkerhetsfunktion, och här väljer du att lita på utgivaren och köra programmet.



Efter detta kommer Panda Cloud Antivirus vara installerat och igång för att skydda din dator. Då det arbetar i molnet behöver du som sagt inte bry dig om de ordinära uppdateringarna av signaturfiler, då det fungerar annorlunda.

För att komma åt gränssnittet till Panda Cloud Antivirus klickar du på dess ikon nere i systemfältet. Ikonen ser ut som en panda. Programmets utseende är som redan påpekat väldigt sparsmakat.



För att genomföra en **skanning av datorns lagringsenheter**, något jag som sagt rekommenderar att du gör i alla fall en gång i veckan, klickar du på förstoringsglasat. Följ därefter instruktionerna för att påbörja en skanning.

Om du klickar på ikonen för **statistik** får du reda på vad det är för typ av farlig kod som Panda Cloud Antivirus har hindrat att installeras på din dator. Det finns även en karantän där virus och annat sparas tills du själv väljer att radera det. Du kommer åt dessa filer genom att klicka på soptunnan nere i högra hörnet.

Installera Spybot Search&Destroy

Antispywareprogrammet **Spybot Search&Destroy** är gratis och kan laddas ner i svensk översättning från [hemsidan](#). Programmet är cirka 16 MB stort och själva installationen kan du klicka dig igenom precis som vanligt.

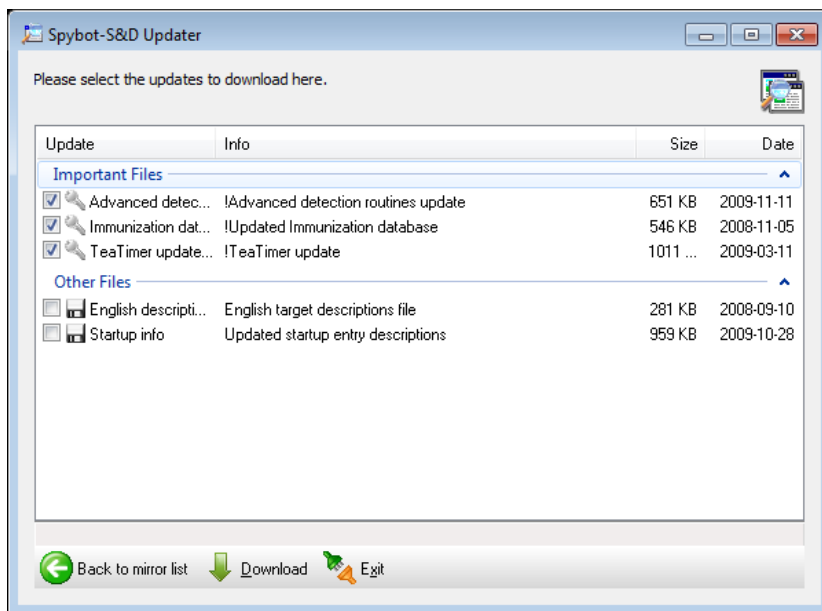
När du startar programmet för första gången får du stega igenom en guide som heter Spybot-S&D Wizard.



Guiden låter dig skapa en backup av ditt Windowsregister, söka efter uppdateringar och **immunisera systemet**. Det sistnämnda aktiverar möjligheten att låta Spybot ha koll på vad som händer i din webbläsare. Immuniseringen gör att Spybot hindrar vissa farliga saker att köras när du surfar på webben. Det rekommenderas varmt att du kör *Immunisera*.

Spybot brukar uppdatera sig automatiskt och ladda ner nya definitionslistor av spyware och adware. När du har installerat programmet för första gången bör du göra detta manuellt så att programmet verkligen innehåller de senaste filerna.

Du kan när som helst söka efter nya uppdateringar genom att klicka på knappen *Sök efter uppdateringar* från Spybots huvudfönster. Programmets gränssnitt kommer du åt genom att klicka på Spybots ikon i systemfältet.



Figur 6: Se till att uppdatera Spybot med jämna mellanrum så att det skyddar mot de senaste spionprogrammen.

Till skillnad mot virus, går det som regel att **rensa bort installerade spyware och adware** från din dator. Använd Spybot och klicka på *Sök & rensa bort* för att göra en komplett skanning av systemet efter infektioner.

När sökningen är genomförd kommer du att presenteras en lista över hittat skräp. Mycket av dessa är förmodligen *cookies* som i praktiken sällan är farliga, men anses av många vara integritetskränkande, varför de räknas som spyware.

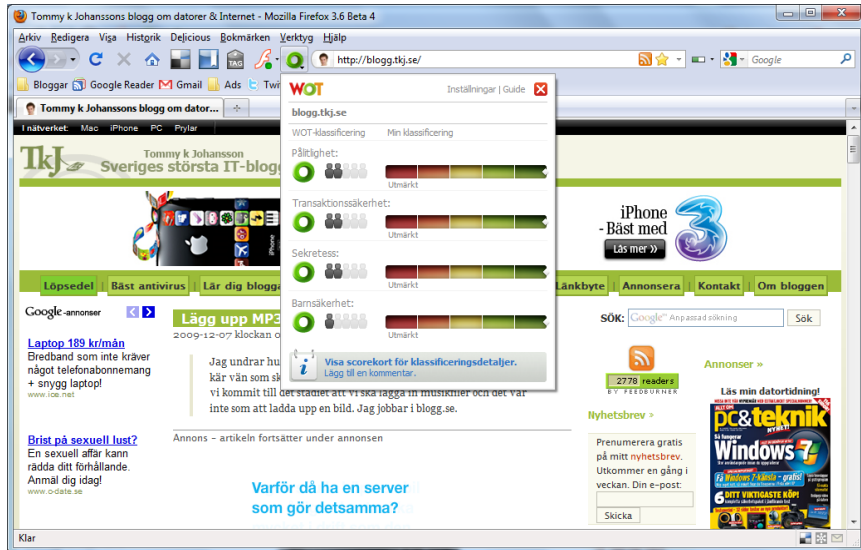
De viktigaste sakerna att radera är riktiga spyware. Enligt min erfarenhet är Spybot imponerande effektivt på att ta bort dessa smittor på ett bra sätt, så att du återfår kontrollen över din dator.

Nyttiga säkerhetsverktyg som skyddar mer

Förutom antivirus, antispysware och brandvägg finns det flera andra verktyg som hjälper dig att bli säkrare när du använder din dator och Internet. Något jag rekommenderar att du installerar är ett av de program som **klassificerar webbsidor**.

Dessa verktyg implementeras i webbläsaren och meddelar dig om du befinner dig på en farlig webbsida, eller om du är på väg till en. De kan baka in sig i sökresultaten hos exempelvis Google, så att varje sökträff markeras med en färgkod för att tala om utifall sidan är klassad som olämplig eller rent farlig.

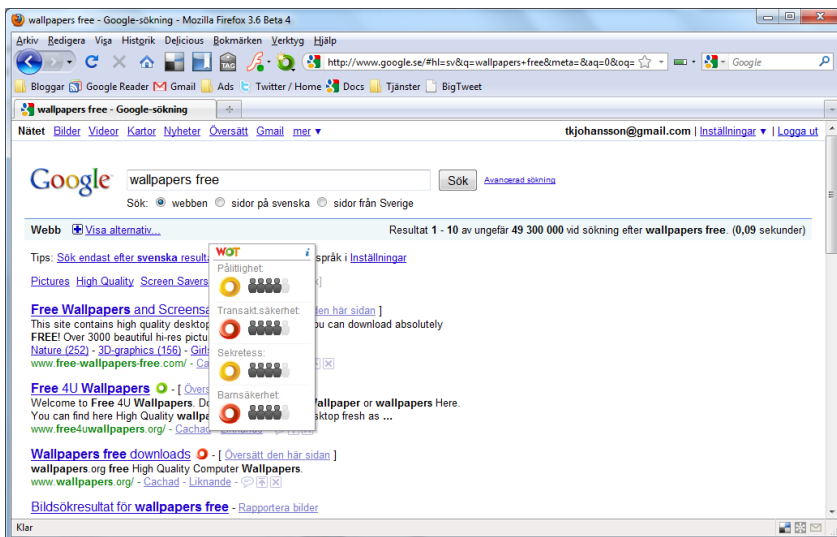
Många kommersiella säkerhetspaket har sådana här funktioner inbyggda. Det finns dock gratis alternativ. Jag brukar rekommendera [McAfee SiteAdvisor](#) eller [WOT – Web of Trust](#). I dagsläget tycker jag att WOT har en stor fördel i och med att det tar upp så lite plats i webbläsaren.



Figur 7: WOT är ett tillägg i webbläsaren som ger dig information om sajtens lämplighet.

WOT finns för såväl Internet Explorer som Firefox, och du installerar det enkelt genom att klicka dig fram på programmets hemsida. Efter en installation behöver du starta om din webbläsare. Därefter finns det en ikon som med färgkod beskriver sidans status – **grön** är positivt, **orange** inte bra och **rött** rent olämpligt. Klickar du på ikonen får du fram mer information.

När du gör en sökning på Google, eller någon annan sökmotor, kommer en liten **färgad ikon** att visas bredvid sökträffarna. På så sätt ser du om en sida är olämplig redan innan du klickar dig vidare. Då kan du undvika att gå in på sajter som är orange- och rödmarkerade.



Figur 8: Sökträffar markeras med färgade ikoner, när du installerat WOT.

Skulle du tröttna på något av programmen kan du enkelt avinstallera dem via *Kontrollpanelen* -> *Avinstallera program*.

Stoppa skript i Firefox

Med hjälp av skript försöker cyberkriminella **installera trojaner och annan bråte på din dator bara genom att du besöker en webbsida**. Man försöker infektera alla möjliga sajter med denna typ av virusspridande skript. Bland

annat använder man tredjepartsleverantörer av annonser, då dessa ibland är dåligt kontrollerade.

Med det gratis tillägget **NoScript** för webbläsaren **Firefox** kan du se till att alla skript stoppas tills du har godkänt domänerna som levererar skript. Efter en installation av NoScript kommer du att få många förfrågningar på de sajter du brukar besöka, men efter att du har lärt tillägget att släppa igenom legitima skript kommer surfandet att bli lugnare och de eventuella oönskade skript som kommer att försöka köras på sajter du inte tidigare besökt stoppas, vilket gör dig väldigt säker mot denna typ av attacker.



Figur 9: Med NoScript installerat stoppas alla skript i Firefox tills du godkänner sajterna.

När du besöker en ny sida visas meddelanden från NoScript. Klicka på ikonen nere i högra hörnet för att få fram en meny där du kan tillåta legitima sajter.

Att tänka på när du använder Internet

Som jag tidigare påpekat är säkerhetsprogram bara en del av ditt skydd på Internet. Ett **lika viktigt skydd är kunskap**, att veta hur du undviker de farliga fallgroparna när du använder Internet.

I det här sista kapitlet ger jag dig grundläggande tips om olika saker du bör tänka på när du surfar på webben och använder Internet i övrigt.

Ladda ner filer och program

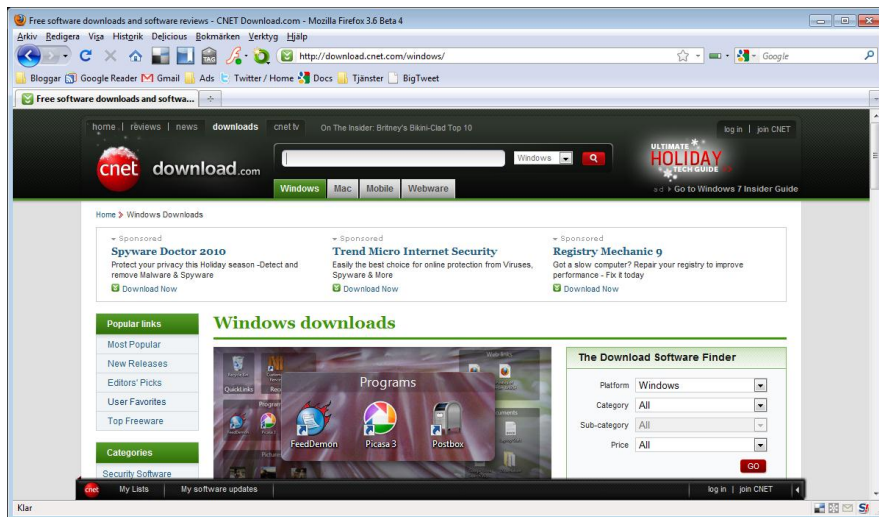
De flesta av oss laddar ner programvaror, spel, filmer, musik och mycket annat. Om man ska sammanfatta det här är rekommendationen att bara **ladda ner från sajter som du har förtroende för**. Det finns gott om nerladdningssajter, men inte alla är pålitliga.

En opålitlig sajt kan antingen ha program som är smittade av virus och spyware. Jag har även sett webbplatser som säger sig erbjuda kända gratisprogram som under installationen ber användaren att registrera programmet genom att beställa en kod via SMS.

När jag en gång skrev om det utmärkta gratisprogrammet PDFCreator fick jag många brev från personer som sade sig laddat net programmet men krävts på en registrering via SMS. De hade betalat 20 kronor per SMS, och fått skicka både två och tre gånger innan de givit upp.

Vad som har hänt är att någon gjort om installationsprogrammet för PDFCreator, som i vanliga fall är helt gratis, och lagt in SMS-betalningen. Sedan har de köpt Google AdWords-annonser för PDFCreator och använt rubriken "Ladda hem PDFCreator". Eftersom den legitima webbplatsen för nerladdning av PDFCreator hade Google AdWords-annonser, visades den här annonsen, och det var många som lurades till att klickade på den istället för den riktiga nerladdningslänken.

Så var uppmärksam på **vad och var när du laddar ner filer**. Download.com är ett exempel på en stor och trovärdig sajt där man är noggrann med att kontrollera alla filer. Letar du efter freeware och shareware, föreslår jag Download.com.



Figur 10: Download.com är en bra sajt för att ladda ner shareware och freeware på ett säkert sätt.

Jag understryker att jag på intet sätt förespråkar **piratnerladdningar**, men eftersom många sysslar med det vill jag ändå skriva en varning. Virustillverkare och cyberkriminella utnyttjar folks ovilja att betala för kända kommersiella program.

Därför är det vanligt att de är snabba på att skapa piratversioner – och speciellt så kallade **crackverktyg** som knäcker kopieringsskydd, och program för att generera registreringskoder – smittade med trojaner, virus och allt möjligt. Dessa program laddar de sedan upp på BitTorrent-sajter, där de snabbt får spridning.

Ett tips är att **viruskontrollera filer du laddar ner**, innan du installerar dem. Det kan du göra med ditt antivirusprogram och du kan också använda

webbtjänster. [VirusTotal](#) är ett bra webbverktyg som låter dig ladda upp en fil och få den kontrollerad av ett flertal olika antivirusprogram.

Phishing och stöld av uppgifter

Phishing, också kallat för *nätfiske* på svenska, är ett begrepp för att beskriva sätt att lura Internetanvändare att lämna ifrån sig **personliga uppgifter**. Detta är väldigt svårt för säkerhetsprogram att sätta stopp för, eftersom det riktar sig helt till användaren. Ett säkerhetsprogram kan inte hindra användaren från att skicka iväg sitt kreditkortsnummer till en cyberskurk.

Ett vanligt exempel på phishing, som vi sett flera gånger i Sverige, är när man gör ett massutskick som påstår sig komma från någon känd sajt eller **Internetbank**. Brevet utformas som att det ska se ut att vara legitimt, och det brukar innehålla något om att tjänsten drabbats av systemkrasch och skulle vilja att du skickar in ditt användarnamn och lösenord för uppdatering av databasen.

Det här är alltid **bedrägeri**. Inga seriösa företag skulle få för sig att be dig skicka ditt lösenord i fritext via e-post. Det händer inte, så denna form av brev ska man akta sig för.

Phishing görs också genom att man bygger en webbsajt som försöker se ut som en känd sajt. Det kan vara exempelvis en kopia av Facebook, där man ber dig logga in på ditt Facebook-konto. I samma sekund som du fyllt i dina uppgifter, har cyberskurkarna information för att logga in på ditt riktiga Facebook-konto.



Här är det viktigaste tipset att **alltid ha kontroll över webbadressen**. Befinner du dig verkligen på facebook.com eller är adressen facebook.xyz.com (där xyz kan vara vad som helst)?

Information är hårdvaluta på den svarta marknaden, och cyberskurkar gör sitt yttersta för att komma över så mycket kunskap om dig som möjligt. Det man främst är ute efter är så klart användarnamn och lösenord till olika sajter – det är därför **du aldrig ska använda samma lösenord** på olika sajter.

Databaser över medlemmar till forum och annat stjäls med jämna mellanrum, och om du då använt samma lösenord här som på ditt Paypal-konto eller dylikt, kan du råka ut för stora problem.

Kreditkorts- och kontokortsnummer är givetvis också väldigt attraktivt. Jag tycker inte att du ska vara livrädd för att uppge dina sådana nummer på nätet, men det finns saker du bör tänka på och de kommer jag att förklara här nedan under rubriken "Handla säkert på nätet".

Tänk på att aldrig ha dina lösenord eller kreditkortsnummer lagrade i läsbart format på din hårddisk. Skulle du drabbas av ett virus, söker de som sagt igenom din dator efter information och skickar vidare detta till de cyberkriminella. Skulle du då ha en textfil innehållande alla dina användarnamn och lösenord, blir följderna föga roliga.

Falska virusvarningar på webben

Ett av de största bedrägerierna på nätet handlar om **falska säkerhetsprogram**. Det har blivit ett enormt stort problem under det senaste året. Cyberskurkar skapar program som utger sig för att vara antispyware och antivirus, och lurar användare till att ladda ner dessa.

När man laddat ner och installerat ett falskt säkerhetsprogram kommer det att ställa till det genom att dels infektera datorn med trojaner, dels försöker det stänga av befintliga säkerhetsprogram och dels försöker det väldigt högljutt få användaren att registrera programmet för ett par hundralappar.

Detta går till så att dessa falska säkerhetsprogram säger sig hitta massor av farlig kod på datorn. För att få bort de påstådda infektionerna behöver man köpa fullversionen av programmet.

Det är **klassiskt bedrägeri** som på ett ironiskt vis spelar på folks rädsla för virus. Denna typ av bedrägerier omsätter idag väldigt stora pengar.

Tipset är att du aldrig ska ladda ner antivirus och andra säkerhetsapplikationer, hur bra de än säger sig vara, om du inte är säker på att det är legitima verktyg. Googla alltid på programmets namn innan du laddar ner. Det finns många bra gratis verktyg inom denna genre, men det **finns tyvärr alltså mycket farligt skräp**.

Säkerhet på sociala nätverk

Sociala nätverk som Twitter, Facebook och MySpace har blivit en form av lekstuga för cyberskurkar. Här hittar de hela tiden på nya sätt att försöka lura användarna att lämna ifrån sig personliga uppgifter, ladda ner falska programvaror och besöka sajter infekterade med trojaner.

Här ovan skrev jag om **phishing**, och det använder man för att få reda på användarnas inloggningsuppgifter. När de väl är uppsnappade sätter man i system att logga in och bland annat posta länkar till farliga webbsidor till användarens kompisar.

Eftersom man som regel har förtroende för sina kompisar, litar folk i allmänhet mer på länkar som ser ut att komma från någon man känner. Därför är det **viktigt att vara källkritisk** även om det ser ut att komma från din bästa kompis – det är inte alls säkert att det faktiskt är hon som skickat det.

Denna varning gäller även chattverktyg som **Microsoft Live Messenger** – eller MSN Messenger som det hette förrut. Även här använder man denna taktik. MSN-virus har du kanske hört talas om, och det är virus som sprider sig till ens kontakter på MSN.

Meddelandena som skickas innehåller ofta frågor som "Är det du som är naken på den här bilden?", vilket leder till att många förskräckt klickar sig vidare.

En annan form av bedrägeri på sociala nätverk är att skicka ut brev och **be om pengar**. Man berättar om att man befinner sig utomlands och har fått plånoken bestulen, och man behöver pengar för att komma hem. Betalar man här kommer pengarna att gå direkt till cyberskurkarna.

Handla säkert på nätet

Jag har personligen aldrig varit speciellt nervös över att **handla med kort på Internet**, för det är ungefär lika farligt som att använda kortet i en vanlig butik. Under alla år jag har handlat på nätet har jag bara stött på problem med dubbelbetalning en gång – och då var det ironiskt nog när jag förnyade ett antivirus hos ett känt säkerhetsföretag.

På Internet finns det många sätt att förbättra säkerheten ytterligare så att du minimerar risken att drabbas av några problem.

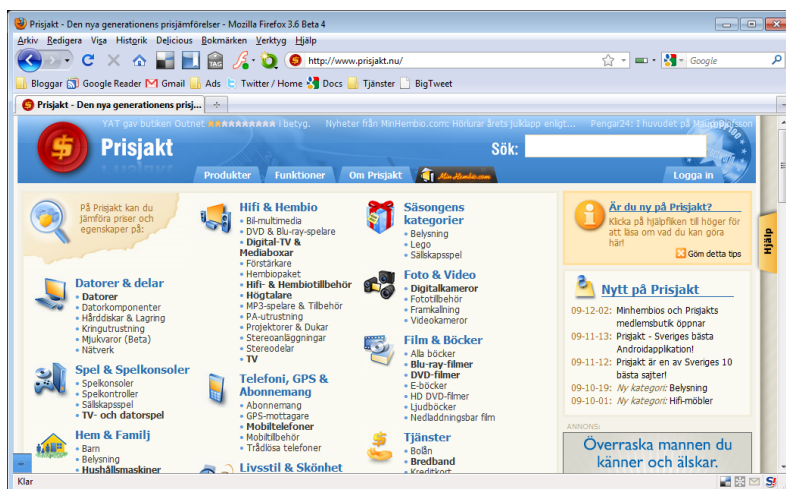


Figur 11: Trygg E-handel rekommenderar e-butiker som håller måttet.

Den första regeln är att **inte handla från suspekta webbshoppar**. Har du inte tidigare haft någon kontakt med en e-butik som verkar intressant, se till att

kolla upp den. Kontrollera att det finns kontaktuppgifter – adress, telefon och e-post. Det bör även finnas organisationsnummer utskrivet. Du kan kontrollera huruvida dessa stämmer genom att söka på [Allabolag](#).

Hos shoppingportalen och prisjämförelsesajter går det snabbt att få reda på om en butik är seriös eller inte. Besök [Pricerunner](#) och [Prisjakt](#), och gör sökningar på bolagets namn för att se om några diskussioner gjorts. Gör även samma sökning på Google.



Figur 12: Vill du veta om ett företag är seriöst eller ej, är Prisjakt en bra start för research.

När du ska genomföra ett köp med kontokort, se till att detta sker via en **säker överföring**. Det ser du genom att adressen börjar med https:// istället för http://.

Rent generellt bör du tänka till två gånger innan du gör en **förskottsinsbetalning**, speciellt om du inte har haft kontakt med företaget tidigare. Går det att lita på företaget du vill skicka pengar till?

Många banker har idag tjänster som **förbättrar säkerheten vid e-handel**. Skandiabanken låter dig till exempel lägga in ett lösenord som måste fyllas i

när du gör kortköp på Internet. Det hindrar att någon som kommit över dina kortuppgifter kan genomföra köp online.

Andra banker erbjuder möjligheten att använda ett **temporärt kontokortsnummer** som du använder enbart för det specifika köpet. Det gör att du slipper lämna ut ditt kontonummer, så att det inte hamnar i en databas någonstans.

En smittad dator är svår att hela

En vanlig missuppfattning är att om ens dator blir smittad av virus, kan du ladda ner och installera ett antivirusprogram för att ta bort viruset. Så fungerar det inte.

Ett antivirusprogram är till för att hindra virus från att kunna installeras. Om ett virus redan lyckats installera sig, på grund av att man som användare har saknat ett bra virusskydd, kan det bli en väldigt omständlig och ofta rent omöjlig process att få bort det.

Förr hade antivirusprogrammen rätt hyfsade funktioner för att försöka rensa bort smittor, men idag är det ytterst få av tillverkarna som har någon som helst utveckling inom detta område. **Antivirus är till för att stoppa virus – inte städa bort befintliga.**

Skälet till varför det är svårt att ta bort virus, är att de infekterar systemfiler och annat. Att plocka bort den skadliga koden från en fil, är ofta omöjligt att genomföra. Viruserna muteras hela tiden för att bli svårare att hitta, och de raderar data ur originalfilen för att ersätta med sin egen kod, så om du får en fil förstörd av ett virus är det som regel inte möjligt att återskapa originalfilen.

Det här är ett viktigt skäl till att alltid ha ett virusskydd aktivt.

Nyttiga länkar

[Tommy k Johanssons blogg](#)

Min blogg där jag skriver om allt inom datorer och Internet. Är idag Sveriges största IT-blogg.

[PCOnline](#)

Datortidning på webben, även denna drivs av mig. Nyheter, produkttester, reportage och artiklar.

[Mjukvara.se](#)

Christian Rudolfs sajt med bra koll på programvaror, även mycket om säkerhetsprogram.

[De bästa svenska säkerhetspaketen](#)

En lista över alla svenska säkerhetspaket som finns att köpa.

[Microsofts säkerhet i hemmet](#)

En bra informationssida från Microsoft om hur du skyddar dig och din dator.

[Allt du behöver veta om datorvirus](#)

Artikel som förklarar datorvirus och vad det är för något.

Slutligen...

Jag hoppas att du fått lära dig en del om säkerhet på Internet efter att ha läst den här boken. Besök gärna [min blogg](#), och skaffa en prenumeration på antingen RSS-flödet eller nyhetsbrevet, så missar du ingenting. Jag skriver kontinuerligt om nya hot, bra programvaror inom säkerhet och andra tips och guider inom ämnet.

Som avslutning skickar jag ut ett par tack:

Min familj Emma och Hjalmar, och katterna Lemmy och Selma.

För hjälp med barnpassning: mor och far, svärföräldrar, Tobbe, Ola och Björn.

För kunskapsutbyte, diskussioner och annat: Christian, Nicke och Bloggkollektivet.

Och ett stort tack till dig som köpt den här e-boken!

