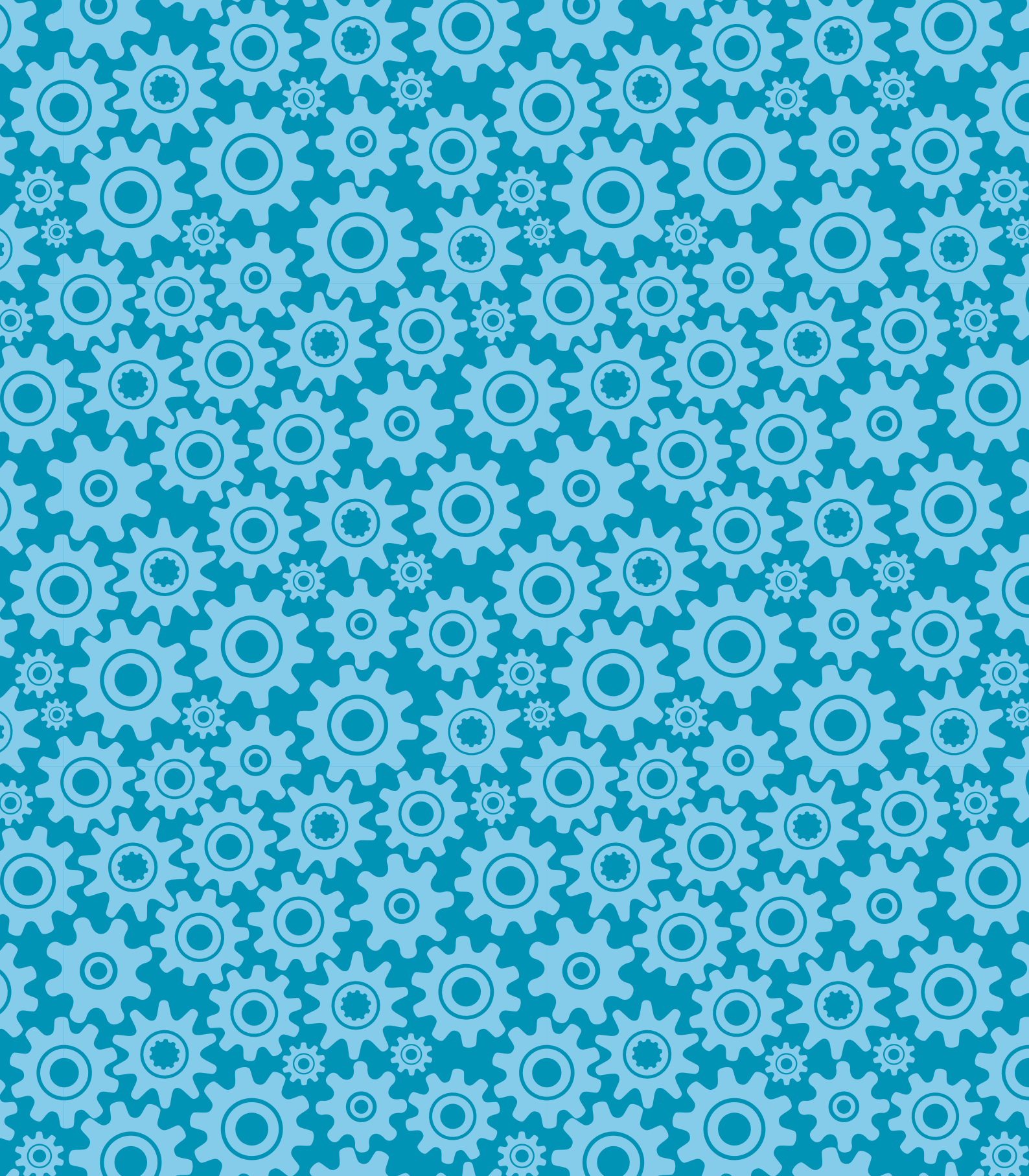
Daniel Goldberg och Linus Larsson

It-säkerhet för privatpersoner

– en introduktion

.se | Internetguider



Daniel Goldberg och Linus Larsson

It-säkerhet för privatpersoner

– en introduktion

IT-säkerhet för privatpersoner
.SE:s Internetguide, nr 30
Version 1.0 2013
Daniel Goldberg och Linus Larsson

.SE klimatkompenserar för sina koldioxidutsläpp och stödjer klimatinitiativet ZeroMission. Se www.zeromission.se för mer information om ZeroMission.

Författare: Daniel Goldberg och Linus Larsson
Redaktör: Hasse Nilsson
Projektledare: Jessica Bäck
Formgivning: Bedow
Omslagsillustration: Camilla Atterby
Första upplagan.
Tack till: Anne-Marie Eklund-Löwinder, .SE och Myndigheten för samhällsskydd och beredskap, MSB.
ISBN: 978-91-87437-05-2

.SE (Stiftelsen för Internetinfrastruktur) ansvarar för Internets svenska toppdomän. .SE är en oberoende allmännyttig organisation som verkar för en positiv utveckling av Internet i Sverige.

Alla .SE:s Internetguider
Du hittar alla .SE:s utgivna Internetguider på www.iis.se/guider. Du kan beställa en prenumeration på nyutgivna guider genom att skicka namn och adress till publikationer@iis.se.

Organisationsnummer: 802405-0190
Besöksadress: Ringvägen 100 A, 9 tr, Stockholm
Brevledes på .SE Box 7399, 103 91 Stockholm
Telefon: +46 8 452 35 00. Fax: +46 8 452 35 02
E-post: info@iis.se www.iis.se

Innehåll

Förord

Aldrig har it-säkerhet varit ett lika omtalat ämne som idag. Vecka efter vecka fylls löpsedlarna av nyheter om stulna lösenord, manipulerade bankomater och övervakningsskandaler. Varningsbrev från våra banker om illasinnade datorvirus, utformade för att i tysthet stjäla våra sparpengar, hör till vardagen. Kapade Facebook- och Twitterkonton likaså.

Inte undra på att många blir oroliga. Hur vet man att de filer som finns lagrade på ens dator inte kan läsas av någon annan? Hur vet man att ens e-postkonto inte får oväntat besök av en illasinnad angripare? Och kan man verkligen lita på att ens pengar är säkra hos nätbanken? Vågar man ge sig ut på nätet över huvud taget?

Det är för att ge svar på sådana frågor som vi har skrivit den här guiden som är till för att lära dig grunderna i hur man håller sig säker i den digitala världen. Vi bjuder på matnyttiga tips om enkla åtgärder för att hålla din e-post, ditt Facebookkonto och dina bankuppgifter i säkert förvar. Vi förklarar hur saker och ting fungerar och går igenom till synes knepiga ord och förkortningar som "kryptering", "ssl" och "fabriksåterställning". Vi ger dig också en inblick i vad som faktiskt händer bakom skärmen och tangentbordet när du knappar in ett lösenord eller loggar in på din nätbank.

Innhåller i den här guiden kräver inte särskilda förkunskaper. Vi har ansträngt oss för att göra den så lättläst som det bara går. För den oinvigde kan it-säkerhet kännas som ett ogenomträngligt komplicerat ämne. I själva verket är det inte alls särskilt svårt att få en känsla för hur allt hänger ihop. Om du klarar av att slå på en dator, ge dig ut på webben och logga in på ett Facebook-konto bör du inte ha några som helst problem att ta dig igenom den här guiden. När du läst klart är vår förhoppning att du ska kunna ge dig ut på nätet trygg i vetskapen om vilka faror som finns där ute, och hur man bäst skyddar sig från att råka illa ut. Med ett par enkla handgrepp går det att göra sig immun mot de vanligast förekommande hoten, och som i de allra flesta sammanhang räcker en skopa eftertänksamhet och sunt förnuft långt.

Daniel Goldberg och Linus Larsson
Stockholm, September 2013

01 Inledning

De kommande 67 sidorna är uppdelade i sammanlagt tio olika kapitel. I vart och ett av dem går vi igenom ett särskilt ämnesområde och ger handfasta tips på smarta tillvägagångssätt. Är du intresserad av något särskilt så bläddra gärna direkt till det kapitel som passar bäst, men för dig som vill ha en grundläggande teknisk genomgång rekommenderar vi att börja med kapitel 2 och kapitel 3. I dem förklarar vi några vanligt förekommande begrepp som även används senare i texten. I kapitel 10 ger vi dessutom tips på lämpliga frågor att ställa till det eller de företag du väljer att samarbeta med på nätet, något som blir allt vanligare i takt med att vi lägger vår e-post, vår kommunikation och våra filer i händerna på internetföretag som Google, Facebook och Microsoft.

Sist i guiden följer en ordlista, där vi förklarar vanligt förekommande termer och förkortningar. Använd den gärna som en lathund, eller ta chansen att imponera på dina mer tekniskt kunniga vänner.

Vår ambition har varit att texten du håller i din hand ska vara lärorik, intressant och lättläst, men också betryggande. Visst finns det många fallgropar att vara vaksam på, och visst kan man aldrig lita hundraprocentigt på att en okänd angripare inte upptäckt nya svagheter att utnyttja för att komma åt ens hemligheter. Men det betyder inte att man ska sluta använda sig av datorer.

Nätet och den digitala tekniken för med sig fantastiska möjligheter för oss alla. Givetvis ska man inte vara rädd för att dra nytta av dem. Det gäller bara att, precis som i vilket annat sammanhang som helst, göra sig medveten om riskerna och se till att skydda sig så gott det går.

02 Virus, trojaner och maskar

Datorvirus har funnits i årtionden och är bland de mest mytomspunna företeelserna i it-säkerhetsvärlden. I otaliga filmer och tv-serier har de framställts som datorvärldens monster, en slags ondsinta varelser som på egen hand kan sprida sig från dator till dator och ställa till problem. Som om de hade en egen vilja.

Verkligheten är, som så ofta, lite mindre dramatisk. Men vad som stämmer är att datorvirus mycket riktigt kan ställa till med rejäl skada.

Först några ord för att undvika begreppsförvirring. Ordet datorvirus används ofta, lite slarvigt, som benämning på alla typer av skadlig kod. Det är vanligt inte minst i tidningarnas rubriker. Men faktum är att verkliga virus har försvunnit nästan helt. Istället har andra, liknande typer tagit över, till exempel trojaner och maskar. Här ska vi gå igenom hur de skiljer sig från varandra. Därför kommer vi att använda "skadlig kod" som sammanfattande benämning, en översättning av de engelska begreppen "malware" och "malicious code".

2.1 Olika typer – samma syfte

Man ska inte blanda ihop virus, trojaner och maskar som om de vore samma sak. Rent tekniskt skiljer de sig rejält från varandra. De sprids på olika sätt och kräver olika mycket resurser att utveckla. Däremot har de mycket gemensamt. Alla utnyttjar de säkerhetshål i din dator för att lura sig in och ta kontroll över den. Väl inne försöker de ofta göra två saker: Utnyttja din dator för att sprida sig själva vidare till andra, eller utnyttja din dator för sina egna syften. Oftast handlar det i slutändan om att tjäna eller stjäla pengar. Senare i kapitlet går vi igenom hur det går till i närmare detalj.

Här följer kortfattade beskrivningar av de tre vanligaste typerna av skadlig kod: virus, trojaner och maskar.

2.2 Virus

Att datorvirus kallas som de gör är ingen slump. De beter sig nämligen på ett sätt som påminner om virus i naturen, trots att de är skapade av programmerare.

Datorvirus "infekterar" ett program genom att hänga sig fast vid det, ungefär som naturens virus angriper ett djurs eller en människas kropp. När datorn är infekterad kan information på hårddisken raderas, avlyssnas eller ändras. Dessutom kan viruset utnyttja datorns beräkningskraft utan att användaren märker det. Många av de tidiga exemplen på virus tycktes vara skapade av personer som mest ville visa upp hur skickliga programmerare de var. Därför gjorde vissa av dem ingen skada på den infekterade datorn. Sådana virus har dock blivit mindre vanliga med tiden.

Verkliga virus är mycket komplicerade att programmera ihop. Dessutom har antivirusprogrammen blivit skickligare på att upptäcka dem. Det har fått kriminella att överge virus till förmån för de andra typerna av skadlig kod, framförallt trojaner och maskar.

2.3 Trojaner

Trojaner har fått sitt namn efter legenden om den trojanska hästen. Där gömde sig grekerna inne i en trähäst för att lura sig in i staden Troja. Trojanen lurar sig in på datorn på ett liknande sätt, ofta dolda i ett annat program eller i en fil.

Till skillnad från virus, som infekterar vanliga program, kan trojanen existera helt för sig själv. Men det som har fått kriminella att välja trojaner framför virus är framförallt en sak: De är enklare att programmera och väl så effektiva.

När en trojan har fått fäste på ens dator kan den användas för en hel del. Till exempel kan den avlyssna det du skriver på tangentbordet för att komma över dina lösenord, kontokortsnummer eller annan känslig information. Informationen som snappas upp kan skickas vidare till personen som styr trojanen – helt utan att du märker det.

En annan vanlig funktion är att en infekterad dator kan kapas och fjärrstyras. Det kallas ofta att den ingår i ett botnät (där bot är en förkortning av robot), det vill säga ett stort nätverk av kapade datorer som kontrolleras av en person eller grupp. Ett omfattande botnät är värt stora pengar. Det kan exempelvis användas för att skicka ut gigantiska mängder oönskad reklam, bedrägeriförsök via e-post, eller rikta överbelastningsattacker mot webbplatser. En sådan går ut på att mängder med infekterade datorer på kommando

börjar skicka skräpinformation mot en webbplats, tills den inte klarar av mer och slutar fungera. Tänk själv vilken makt det skulle innebära om man kunde få tiotusentals datorer att utföra nästan vilken handling som helst på kommando.

Trojaner brukar ha fantasifulla namn och benämningar, Haxdoor eller Zeus för att ta två vanliga exempel. Namnen har antingen bestämts av trojanens skapare, eller kommer från antivirusföretaget som upptäckte dem.

2.4 Maskar

Till skillnad från virus är maskar fristående program som inte behöver infektera en viss fil för att infektera en dator. Namnet kommer från dess förmåga att sprida sig själv – man brukar säga att masken kryper sig fram mot nya datorer att ta kontroll över.

Olika maskar tar sig fram på olika sätt. Vissa kan kopiera sig över ett nätverk, andra lägger sig på usb-minnen som flyttas mellan datorer och en tredje typ sprider sig genom att själv börja skicka e-postmeddelanden från den dator den har tagit över.

När en mask har infekterat en dator kan den göra ungefär samma skada som en trojan. Men genom åren har det också dykt upp maskar utan tydligt syfte – allt de verkar göra är att sprida sig vidare och ta över fler datorer. Ändå har de ställt till rejäl skada eftersom de sprider sig med sådan fart att de tynger nätverk och överbelastar e-postservrar.

2.5 Vad kan de ställa till med?

En dator som har infekterats av en trojan, en mask eller ett virus fortsätter ofta fungera som om ingenting hade hänt. Möjligtvis går den lite långsammare än tidigare eftersom datorns prestanda och uppkoppling till nätet används till annat än vad du sysslar med. Så vad är då problemet?

En hel del, och inte bara för dig själv. Vi nämnde tidigare att tangentbordet kan avlyssnas. Det är något av en standardfunktion i moderna trojaner, och den kan anpassas för speciella syften. Till exempel kan den reagera när du får upp ett inloggningsformulär på skärmen. När du knappar in användarnamn och lösenord snappas de upp och skickas vidare till den som kontrollerar trojanen.

Mest eftertraktade är de lösenord som angriparen kan använda för att tjäna pengar, till exempel inloggning på konton som Paypal eller andra som är kopplade till ett kontokort. Även internetbanker har drabbats av den här typen av inloggning, framförallt på den tiden då engångskoder på plastbrickor (så kallade skrapkoder) an-

vändes för att logga in. I dag har bankerna börjat ta säkerheten på större allvar och det krävs mer avancerade trojaner för att stjäla pengar. Se kapitel 7: "Så skyddar du dina pengar", för en närmare beskrivning.

Men datorer som har kapats med trojaner används inte bara för att komma över ägarens konton och känsliga information. En angripare kan också vilja utnyttja din dator för helt andra syften. Ett är utskick av skräppost. Sådana utskick förenklas med tillgång till ett par tusen (eller ännu fler) kapade datorer, eftersom källan blir svårare att spåra.

Om du skulle drabbas av en trojan är det möjligt att du inte ens själv märker det. Men i bakgrunden pågår handlingar som du troligtvis inte vill ha något att göra med.

2.6 Hur blir du infekterad?

För att smyga in en trojan eller mask på din dator måste angriparen ta till speciella metoder. De kan se mycket olika ut, men har alla en sak gemensam: Antingen lurar de din dator eller så lurar de dig. Att lura din dator innebär att angriparen känner till en säkerhetslucka i till exempel Windows som hen kan utnyttja. Att lura dig är precis vad det låter som. Det kallas social ingenjörskonst och är minst lika effektivt.

2.7 Social ingenjörskonst

När du sitter vid din dator, inloggad med rätt lösenord och därmed med full tillgång till alla funktioner kan du själv ställa till en hel del skada. I sig är det helt i sin ordning – du ska ju kunna radera filer, installera program och till och med fjärrstyra din egen dator.

Men det för också med sig en fara. Om en angripare kan lura dig att utföra en handling är det som om hen satt vid tangentbordet själv. Många har begripit att det är enklare att lura personen vid datorn än att hacka själva datorn.

E-postmeddelanden med falsk avsändare är en variant av social ingenjörskonst. Ibland är de utformade för att se ut att ha en bank som avsändare. Andra gånger använder de formuleringar som angriparen förstår att mottagaren kommer att ha svårt att motstå.

2.8 Säkerhetsluckor

Även om social ingenjörskonst är effektiv så utnyttjar bedragare också rent tekniska svagheter i program och operativsystem för att plantera trojaner och föra in maskar. Inför sådana hot vilar det största ansvaret på företagen som utvecklar operativsystemen och programmen. Men som vanlig användare finns det ett par nöd-

Överkurs!

E-postmasken som blev film

Ett tidigt exempel är e-postmasken ILOVEYOU (ibland kallat Love Letter) som började sprida sig på nätet år 2000. Det spreds genom ett mejl med ämnesraden "ILOVEYOU" och en bifogad fil som såg ut att vara ett kärleksbrev. Men när man klickade på filen installerade man istället den skadliga koden. Därefter plockade masken fram ens kontaktlista i e-postprogrammet och skickade sig själv vidare till de 50 första adresserna. Med andra ord spreds ILOVEYOU från vän till vän. Inte konstigt att många gick på bluffen – det såg ju ut att vara ett kärleksbrev från någon de kände. Tiotals miljoner datorer infekterades innan masken kunde stoppas.

Exemplet är gammalt, men bedragare använder fortfarande metoder som bygger på samma princip: Locka med någonting mottagaren har svårt att stå emot (sex eller pengar, ofta i form av lotterivinster är två favoriter) och lägg till en uppmaning att klicka på en fil eller besöka en webbadress.

Just masken ILOVEYOU har gått till historien även av andra anledningar. År 2011 förevigades historien om den i den romantiska thrillern "Subject: I love you".

E-post är inte det enda sättet att sprida skadlig kod. Samma trick har börjat användas på sociala medier i takt med att användarna har flyttat dit. Förbluffande ofta använder angriparna till och med telefonen. En bedrägerimetod går ut på att någon ringer upp och utger sig för att vara supportpersonal, ofta från Microsoft. Därefter lotsas användaren genom åtgärder på datorn som i själva verket innebär att hen lämnar ifrån sig känslig information som inloggnings- och bankuppgifter.

Det är svårt att helt skydda sig från social ingenjörskonst. Då och då måste man trots allt lita på en avsändare. Men du kommer en bit på vägen med två grundregler.

- För det första – om det låter för bra för att vara sant så är det förmodligen så. Nej, du har inte vunnit stora pengar på ett lotteri du inte har deltagit i.
- För det andra – seriösa företag använder aldrig e-post för att sprida uppdateringar till din dator. Dubbelkolla med källan, läs på den officiella hemsidan eller ring och fråga om du är osäker. Du kan också använda Google för att söka på formuleringar i ett mejl. Ofta har någon annan redan skrivit om bluffen.

vändiga åtgärder som man måste vidta.

Följande tre råd är en bra grund för vardaglig it-säkerhet. De kommer ursprungligen från Brian Krebs som är en välkänd skribent inom it-säkerhet.

2.9 Om du inte letade efter ett program, installera det inte

Surfar du runt på måfå och plötsligt får upp ett fönster som uppmanar dig att rensa din dator? Kanske ett fejkat meddelande om att du har fått virus som måste tas bort? Eller löften om bättre kvalitet på strömmad film?

I sådana lägen ska man direkt stänga fönstret utan att installera något program. Med stor sannolikhet rör det sig om en ren bluff. Programmet kommer inte utföra vad det utlovar. Det kommer kanske kräva dig på pengar och kan mycket väl installera skadlig kod på din dator, just det som programmet lovar att rensa bort.

Så tänk efter innan du installerar ett program: Letade jag efter just det här? Om inte, hur gick det till när det hamnade på min skärm?

2.10 Om du har installerat det, uppdatera det

Nya säkerhetshål upptäcks hela tiden. Det gäller både operativsystem som Windows eller Mac OS och enskilda program. Det har mjukvaruföretagen insett och därför skickar de regelbundet ut uppdateringar som täpper till luckorna, förhoppningsvis innan kriminella kan utnyttja dem.

Sådana uppdateringar är gratis och ska installeras så snart de finns tillgängliga. Visst kan det kännas tröttsamt med ständiga meddelanden om uppdateringar, men se till att omedelbart installera åtminstone de som handlar om säkerhet. Det finns gott om exempel på vad som kan hända annars. För några år sedan var pdf-filer bland de mest populära för att infektera datorer med trojaner. Det kunde ske på grund av ett säkerhetshål i Adobe Reader, programmet som många använder för att läsa pdf-filerna. Adobe fick kritik för att företaget dröjde med att släppa lagningar, men även när de fanns tillgängliga så kunde attackerna fortsätta eftersom inte alla uppdaterade.

I dag har de flesta program funktioner som automatiskt kontrollerar om det finns uppdateringar tillgängliga. Se till att aktivera den!

2.11 Om du inte behöver programmet, avinstallera det

Varje installerat program är en potentiell genväg in till din dator. Ju färre program du har installerade desto svårare blir det

Tips!

Antivirus för Mac?

De flesta antivirusprogram riktar sig till Windows-användare, eftersom majoriteten av all skadlig kod angriper just Windows. Men även om Mac-användare fortfarande är tryggare så har ett antal hot även mot Mac dykt upp på senare år, och det finns säkerhetsprogram med antivirusfunktioner att tillgå även där. Tänk på att även om du som använder Mac inte smittas av skadlig kod skriven för Windows, så kan du av misstag föra smittan vidare till pc-användare genom att vidarebefordra e-post med skadliga filer, bedrägliga webbadresser och så vidare.

att ta sig in. Gör det därför till en vana att ta bort program som du bestämmer dig för att du inte behöver. Som en bonus sparar du därmed på hårddiskutrymme. Tänk på att principen inte bara ska gälla vanliga program, utan också instickspro-gram (“plugins” eller “extensions” som de kallas på engelska) i webbläsare.

2.12 Hur upptäcker man att man är infekterad?

Skapare av trojaner och maskar lägger ner ofantliga resurser på att hålla sina program osynliga efter att de har infekterat en dator. Därför är det mycket svårt att upptäcka dem på egen hand som vanlig användare.

Det är här antivirusprogram kommer in i bilden. De använder ett par metoder för att upptäcka skadlig kod. Dels innehåller de en lista med “signaturer”, som kan liknas vid den skadliga kodens fingeravtryck. Genom att jämföra datorns filer med signaturerna kan man upptäcka skadlig kod, och förhoppningsvis ta bort den. Dessutom spanar den efter program som beter sig märkligt i största allmänhet, eftersom det kan vara ett tecken på infektion.

Förutom att granska filer på hårddisken brukar antivirusprogrammen blockera falska webbsidor som försöker stjäla dina uppgifter och kontrollera inkommande e-post. Därför marknadsförs de inte alltid som antivirusprogram utan som heltäckande säkerhetsprogram. Men inte desto mindre är ett av deras viktigaste syften fortfarande att upptäcka och ta bort skadlig kod.

2.13 Uppdatera, uppdatera, uppdatera

Eftersom ny skadlig kod upptäcks hela tiden är det viktigt att antivirusprogrammet hålls uppdaterat. I regel säljs de med en prenumeration för nya signaturfiler. Genom att regelbundet ladda hem nya lär sig programmet vad det ska leta efter. När programmet är inställt att hämta nya filer behöver du inte tänka mer på det, uppdateringen sker i regel automatiskt i bakgrunden.

En rad företag säljer antivirusprogram. Symantec, McAfee, Kaspersky, F-Secure och Sophos är några av de mest kända. De varierar både i pris och funktioner, så vilket som passar dig bäst är svårt att säga. Många finns i en gratis testversion som kan laddas hem och användas under en kortare tid. Testa dig gärna fram! Utöver detta så har de senaste versionerna av Windows och Mac OS X säkerhetsfunktioner som du bör ha aktiverade.

Varning!

”Antivirus håller mig säker mot allt!”

- Det finns inget hundraprocentigt skydd mot skadlig kod, inte ens för den som köper dyra säkerhetsprogram och betalar för regelbundna uppdateringar.
- Ny skadlig kod kan spridas på nätet och ställa till med skada innan de identifieras av säkerhetsföretagen och programmen lär sig känna igen dem. Om du hör till de första att bli infekterad av ny skadlig kod finns det därför risk att din dator skadas.
- Därför gäller det att vara försiktig med att ladda hem program och klicka på bifogade filer eller länkar i e-post om du inte är helt säker på att de kommer från en trygg avsändare. I kombination med antivirus kommer sådan försiktighet räcka långt för att hålla datorn fri från infektioner.

03 Nätfiske och den okända avsändaren

En av de vanligaste metoderna för att komma över känslig information på nätet och sprida skadlig kod, trojaner och virus är med hjälp av det som kallas för "phishing". Ordet är en omskrivning för "fishing", och brukar översättas till nätfiske på svenska. I korthet går det ut på att en angripare lurar dig att lämna ifrån dig känslig information genom att låtsas vara någon annan. I det här kapitlet går vi igenom de vanligaste formerna av nätfiske, och förklarar hur du skyddar dig.

Ibland kan nätfisket vara lätt att genomskåda: Alla nätsurfare är bekanta med de


Nordea

Kära kund,

Nordea tekniska serviceavdelning håller på att utföra en planerad uppgradering av mjukvaran för att förbättra servicekvaliteten åt bankens kunder.

Vi ber dig att börja proceduren för att bekräfta dina bankkontodetaljer.
Klicka på länken, som du hittar i slutet av det här e-postmeddelandet, för att göra detta.

http://app.nordea.se/cprocedure_idU144BUU7/widecarea.aspx

Copyright 2007 Nordea

Falsk e-post som ser ut att komma från din bank eller ditt kreditkortsföretag är en vanlig form av nätfiske.

enorma mängder skräppost som landar i våra e-postlådor varje dag. Ibland är det en påstådd släkting i ett avlägset land som lovar att överlämna ett bortglömt arv om du bara skickar över en liten administrationsavgift. Ibland är det en påstådd vinst i en tävling, där värdefulla prylar blir dina om du bara uppger dina bankuppgifter för avsändaren.

De flesta har lärt sig att genomskåda sådana enkla bluffar och snabbt förpassa dem till papperskorgen. De flesta mejlprogram har dessutom inbyggda filter för att automatiskt sortera bort oönskad skräppost.

På senare år har dock många nätfiskare blivit mer sofistikerade. Framförallt de phishing-mejl som försöker komma över inloggningsuppgifter till banker har blivit svårare att skilja från äkta vara. Genom att använda logotyper, text och bilder stulna från bankens verkliga webbplats går det att få till mejl som ser ut att vara äkta. Inte sällan ber avsändaren dig logga in för att bekräfta exempelvis din adress, eller installera en säkerhetsuppdatering. I själva verket smusslas dina inloggningsuppgifter undan och används sedan av angriparen för att länsa ditt konto (se kapitel 7: ”Så skyddar du dina pengar”, för mer om detta). Regeln här är att din bank aldrig någonsin mejlar och ber om dina inloggningsuppgifter eller att du ska logga in på en sida för att kolla att dina uppgifter stämmer.

3.1 Din vän kan vara vem som helst

Att många försök till nätfiske är enkla att genomskåda beror på att avsändarna siktar brett. De flesta skräppostare skickar ut sina mejl till flera miljoner mottagare, ofta på flera språk och i många olika länder. Strategin ger dem väldigt lite utrymme att anpassa utskicken till just dig. Det tvingar dem att formulera sig brett och opersonligt i sina texter, och det gör det lättare för e-postprogrammens automatiska filter att identifiera skräpposten och omedelbart förpassa den till papperskorgen.

Givetvis är det en svaghet som listiga angripare lärt sig utnyttja. Det kanske bästa sättet att göra nätfiske mer effektivt är nämligen, något paradoxalt, att begränsa antalet mottagare. Om en angripare bara väljer ut svenskar kan hen koncentrera sig på att förbättra språkbruket, exempelvis. Genom att bara välja kunder till ett visst företag, eller boende i ett visst område, går det att bättra på trovärdigheten ytterligare genom att strössla texten med bekanta detaljer och referenser.

Checklista!
Tre anledningar att bli misstänksam

De flesta phishingmejl är lätta att avslöja. Här är tre saker att vara uppmärksam på när du försöker avgöra om avsändaren är den hen utger sig för att vara.

1. Stavfel

Nätfiskare behöver inte vara svenskar även om de försöker lura svenska användare. Ofta översätts textinnehållet i mejlen automatiskt med hjälp av verktyg på nätet. Var därför uppmärksam på märkliga formuleringar, rena stavfel och underliga ordval. Brukar din bank inleda mejl till dig med "Käre herre/fru"? Brukar din mobiloperatör inleda påminnelser om obetalda fakturor med orden "Fel bill", en misslyckad översättning av det engelska ordet för räkning? Båda är exempel ur verkligheten, och lätta att genomskåda för den som läser noga

2. Varifrån kommer mejlet?

Ett enkelt sätt att avgöra ett mejls äkthet är att kika närmare på avsändaren. Intill eller strax under namnet (beroende på vilket mejlprogram du använder), ser du mejladressen i sin helhet. Titta noga på e-postdomänen, det vill säga vad som står efter "@" i adressen. Ett mejl från Telia bör rimligen komma från telia.com eller telia.se, inte från exempelvis global.client@receive.com. Även det är ett exempel från verkligheten, och ett tydligt tecken på att något inte står rätt till. Men även om adressen stämmer ska du inte känna dig helt säker, det går faktiskt att fejka en riktig avsändaradress.

3. Vart leder länkarna?

De flesta nätfiskare försöker få dig att klicka på en länk i mejlet, antingen för att skicka dig vidare till en falsk inloggningssida eller för att installera skadlig kod på din dator. Undersök därför länkarna lite extra innan du klickar. I de flesta mejlklienter kan du enkelt förhandsgranska länkar genom att hålla muspekaren över dem. I fönstrets botten, eller intill muspekaren, visas då destinationsadressen. För att återgå till exemplet ovan: I ett mejl från Telia bör länkarna rimligen leda till telia.se- eller telia.com-adresser. Inte, som i detta fall, till en suspekt tysk shoppingsajt. Tyvärr har banker och e-handelssajter ofta långa och komplicerade adresser till specifika sidor och tjänster så här gäller det att vara extra uppmärksam.

Genom att gå ännu ett steg längre, och fokusera utskicket på just dig, kan en skicklig nätfiskare göra bluffen nästan omöjlig att upptäcka. Det kallas för "spear fishing", spjutfiske på svenska, och syftar på nätfiske där måltavlan har krympts ned till att omfatta en enskild individ, eller en mycket liten grupp av mottagare.

Ett välkänt exempel inträffade år 2011, och fick minst sagt ödesdigra konsekvenser. Någon skickade då ett mejl till en handfull anställda på säkerhetsföretaget RSA, med det bifogade exceldokumentet "2011 recruitment plan.xls". Mottagarna valdes noggrant ut av angriparen – de var just sådana som skulle beröras av en rekryteringsplan. En av dem gick på bluffen och öppnade den bifogade filen. I exceldokumentet gömde sig ett stycke skadlig kod, som snabbt tog kontroll över den anställdes dator och letade sig vidare på företagsnätverket. Måltavlan var RSA:s mest känsliga företagshemlighet, krypteringstekniken SecurID, som används av mängder av företag för tvåfaktorsautentisering (läs mer om den tekniken i kapitel 5: "Lösenord och tvåfaktorsinloggning"). Angreppet lyckades, och årets största säkerhetsskandal var ett faktum. Allt tack vare ett oanseligt nätfiskemejl.

3.2 Att fejka en avsändare är ingen konst

Metoden som användes för att komma åt säkerhetsföretaget RSA:s hemligheter kan enkelt anpassas även mot privatpersoner. I regel är folk mer benägna att klicka på länkar eller lämna över viktig information till personer de känner och litar på. Det är inte så konstigt – men hur vet du att vännen som mejlar, eller pratar med dig på Facebook, verkligen är den hen utger sig för att vara?

Det finns inga inbyggda spärrar på internet som förbjuder oss att registrera exempelvis e-postadresser i falskt namn, så länge just den adressen inte är upptagen. Dessutom finns verktyg på nätet som låter en angripare fejka en avsändaradress utan att ens registrera den på riktigt. Hösten 2012 roade sig exempelvis en skämtsam hackare med att skicka tramsigt skrivna mejl från adressen "jimmy.akesson@sverigedemokraterna.se" till journalister. För den som inte noterade stavningen i förnamnet (Sverigedemokraternas partiledare skriver Jimmie, inte Jimmy) var bluffen svår att genomskåda. I det fallet var avsikten bara att roa, men samma metod kan användas även för att sprida trojaner och maskar. Fråga dig själv: Hur noga tänker du efter innan du laddar ned en fil eller klickar på en länk som skickats till dig av en vän?

Överkurs!
”Ingen klickar väl på spam?”

Det kan tyckas märkligt att skräpposten fortsätter att flöda in i våra e-postlådor år efter år. Ingen kan väl vara så dum att den klickar på vad som i de flesta fall så uppenbart är försök till bedrägeri? Faktum är att nätfiske är ett mycket effektivt verktyg för att sprida skadlig kod och lura av nätsurfare känslig information.

År 2009 genomförde företaget Trusteer en undersökning där mer än tre miljoner nätanvändares beteende analyserades under en tremånadersperiod. Resultatet visade att ungefär en procent av alla amerikanska bankkunder luras att klicka på en länk i ett nätfiskemejl, som utgett sig för att komma från deras bank, under varje enskilt år. Av dem fyller nästan hälften i sina inloggningsuppgifter på sidan de sen skickas vidare till.

En av hundra kanske inte låter mycket, och mycket riktigt är träffgraden på ett enskilt skräppostutskick låg. Men med tanke på de enorma volymer som skickas ut räcker den ändå långt. Erfarna spammare jobbar nämligen enligt hagelbösseprincipen, och siktar så brett det bara går och hoppas att tillräckligt många går på bluffen.

En titt på siffrorna räcker för att bekräfta den bilden. En vanlig dag skickas som regel tiotals miljarder skräppostmeddelanden. Inte sällan utgör den mer än två tredjedelar av all e-posttrafik som flödar över nätet. Världen över skickas det alltså dubbelt så mycket skräppost som “riktig” e-post. Det mesta är dåligt formulerade säljbrev för billig Viagra och suspekta dejtingsajter, men även försök att komma över bankuppgifter eller annan känslig information är vanligt förekommande.

Enligt en undersökning gjord av säkerhetsföretaget Symantec var 0,35 procent av alla mejl som skickades i världen under juni 2011 utformade för att lura mottagaren att lämna ifrån sig ett lösenord, ett kontokortsnummer eller någon annan form av känslig information.

Av samma anledning är inloggningsuppgifter till konton på sociala medier, exempelvis Facebook eller Twitter, mycket åtråvärda. Genom ett stulet Facebookkonto är det i många fall en barnlek att lura av andra känslig information – kanske pojk- eller flickvännen kan övertygas att knappa in sitt kontokortsnummer i chattfönstret för att lösa en akut situation? Kanske kan bästa vännen övertygas att ladda ned ett roligt spel, som i själva verket innehåller en lömsk trojan? Bläddra till kapitel 5 för att läsa mer om detta.

Det bästa sättet att skydda sig från nätfiske är alltså att så ofta det går kontrollera om avsändaren verkligen är den hen utger sig för att vara. Ett enkelt knep är att helt enkelt kontakta avsändaren via en e-postadress du har sedan tidigare, och be avsändaren bekräfta sin identitet. Vill du vara extra säker så ställ en kontrollfråga som bara avsändaren kan svara på. Kanske minns din vän någonting som hände i er barndom? Kanske kan dina föräldrar svara på någonting som är välkänt i familjen, men inte för andra?

För den verkligt försiktige finns ännu en åtgärd att ta till: Lyft telefonen och ring upp! Då kan du helt enkelt fråga avsändaren om hen verkligen skickat just det där misstänkta meddelandet till dig eller ej.

04 Trådlösa nätverk

Trådlösa nätverk i hemmen har varit en självklarhet i många år. Inte minst gick fler över till trådlöst när bredbandsoperatörer för några år sedan började skicka ut utrustningen som krävs gratis till sina kunder. Att tekniken slog igenom var knappast förvånande. Det är mycket praktiskt att kunna flytta sig med en bärbar dator från köket till vardagsrummet utan att krångla med nätverkskablar.

Men vad vissa glömmer är att det trådlösa nätverket inte bara fungerar inom hemmets väggar. Bor du i lägenhet ser du säkert grannarnas nätverk. Plocka med dig datorn ner på gatan och du kommer märka att både ditt eget nätverk och grannarnas går att nå även där.

Det är alltså fullt möjligt för vem som helst att nå ditt nätverk och utnyttja det för sina egna syften, bara genom att vara i närheten av bostaden. Därför måste ditt trådlösa nätverk skyddas på ett annat sätt än ett som består av kablar.

4.1 När det går riktigt illa – därför ska du skydda ditt nätverk

Man kan fråga sig varför man ska skydda sitt trådlösa hemmanätverk med lösenord och kryptering. Är det inte en trevlig gest att bjuda grannar och förbivandrande på gratis uppkoppling? Jo, visst är det så. Men samtidigt är det förknippat med risker att låta vem som helst surfa via ens uppkoppling.

För att förstå varför måste man förstå grunderna i hur polisen arbetar för att utreda it-baserad brottslighet. När en misstänkt spåras på nätet börjar polisen ofta med en ip-adress som har fastnat i en loggfil någonstans. Det gäller oavsett om brottet är hot via e-post, dataintrång eller illegal fildelning. Om brottet bedöms allvarligt nog kan polisen sedan vända sig till internetoperatören och begära ut information om vem som använde ip-adressen vid tillfället då brottet begicks. När namn och adress har lämnats ut har

polisen allt som behövs för att genomföra en husrannsakan.

Ip-adressen säger alltså ingenting om vem som har utfört ett brott, bara vilken uppkoppling som användes. Men det är mot ägaren av uppkopplingen som en eventuell husrannsakan riktas, vilket kan vara nog så otrevligt även om det senare visar sig att innehavaren är helt oskyldig.

Scenariot är inte hypotetiskt, vilket ett antal boende i Dalarna blev varse en tidig vårmorgon 2012. Då slog polisen till mot flera bostäder i Ludvikatrakten. Personen de sökte misstänktes för ett allvarligt dataintrång mot bland annat it-företaget Logicas servrar. Adresserna de slog till mot hade tagits fram genom spårning av ip-adresser. Polisen klampade in, beslagtog mobiltelefoner, datorer och hårddiskar. De boende tvingades sitta igenom förhör där de anklagades för allvarliga brott som kunde ge långa fängelsestraff.

Först senare framkom att de allihop var helt oskyldiga. De var vanliga datoranvändare som surfade på nätet, skickade e-post och betalade sina räkningar via internetbanker. Däremot hittade polisens tekniker något intressant när de tittade närmare på deras trådlösa nätverk. De hade hackats och använts av en främmande person som bodde i närheten. Vid en husrannsakan hemma hos honom hittade man en förstärkningsantenn monterad på balkongen. Med hjälp av den kunde han nå trådlösa nätverk på långt håll – och mycket riktigt återfanns knäckta lösenord till grannarnas nätverk sparade på en av hårddiskarna i bostaden.

Därmed avfördes de oskyldiga grannarna helt från förundersökningen, men några av dem har efteråt vittnat om hur

Tips!

Frågor till din operatör

Ställ krav på din internetoperatör om en trådlös router ingår i abonnemanget. Här är tre frågor som du ska kräva svar på:

- → Är lösenordskrav och kryptering aktiverat från start?
- → Kan jag själv byta till ett eget lösenord? Be om hjälp om det är komplicerat!
- → Vilken typ av kryptering används?

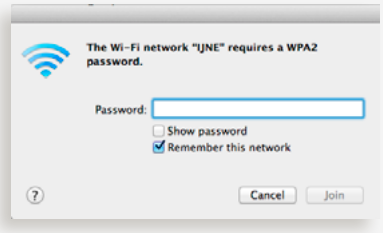
omskakande det var att få poliser instormande en tidig morgon utan att förstå vad som hade hänt.

4.2 Så skyddar du nätverket

I huvudsak behövs två sorters skydd för trådlösa nätverk: Dels ska nätverket förses med lösenord och dels ska det krypteras (läs mer om kryptering i Kapitel 6: ”E-post är som vykort”). Lösenordet stoppar obehöriga från att ansluta sig. Krypteringen hindrar dem från att avlyssna din surfning. Som tur är löser man både och med en enda inställning.

Så varför behövs kryptering för att nätverket inte ska avlyssnas? Egentligen räcker det att tänka på hur trådlösa nätverk egentligen fungerar. När du surfar utan sladd flyger ju all information mellan din dator och routern genom luften. Det betyder att någon annan kan snappa upp den på vägen, till och med utanför ditt hem. Innehållet på hemsidor, text du själv skriver in, filer som laddas upp och ned. Samt – och detta är kanske det värsta – en hel del lösenord till sajter på nätet.

Alla moderna trådlösa routrar har i dag stöd för kryptering som duger gott för



Så här ser inloggningen till ett nätverk som skyddas med WPA2-kryptering ut på en Mac.

Och så här ser inloggningen till ett nätverk som skyddas med WPA2-kryptering ut på en PC.

Viktigt!

Välj rätt säkerhet för din router

Det finns flera olika säkerhetsstandarder för trådlösa nätverk. Alla gör de ungefär samma sak – de krypterar trafiken för att göra den oläslig för utomstående – men med olika resultat. Här är de vanligaste typerna:

1. WEP – gammalt och dåligt
   WEP är en gammal form av säkerhet för trådlösa nätverk som togs fram redan på 1990-talet. Även om din router fortfarande har stöd för WEP så ska det undvikas. För det ska sägas rakt ut: WEP erbjuder mycket svag säkerhet och ska aldrig användas. Faktum är att det kan knäckas på några sekunder.

2. WPA – efterföljaren
   Bland inställningarna kan du hitta möjligheten att välja WPA, en standard som följde efter WEP. Undvik även denna, eftersom den har fasats ut till förmån för efterföljaren WPA2.

3. WPA2 – bäst hittills
   Sedan flera år ska alla trådlösa routrar ha stöd för denna modernare säkerhetsfunktion. Det är denna du ska välja, om den inte är förvald redan när du plockar upp routern ur kartongen. I routrar för hemmabruk kallas den ibland WPA2 Personal eller WPA2-PSK.

hemmabruk. Exakt hur inställningarna görs beror på vilken routermodell du har. Men i grunden är det okomplicerat: Välj krypteringsmetod, ange ett lösenord och du är igång.

Det finns dock ett par fallgropar att undvika. Framförallt ska man akta sig för äldre typer av kryptering. Vilken typ av kryptering som används kan du se genom att logga in på routern, men ofta kan man också se det när man ansluter sig till nätverket.

4.3 Publika nätverk – hemligheter hör inte hemma på kaféet

Allt fler kaféer och hotell erbjuder trådlösa nätverk till sina kunder. Ibland skyddas

Varning!

Se upp med lösenordet!

I alla sammanhang där kryptering används gäller en regel: Det spelar ingen roll hur bra säkerhetsmekanismer du har aktiverat om du inte väljer ett starkt lösenord. Många routrar levereras med ett förinställt lösenord. Det är en bra idé att byta det mot ett eget som är långt och därmed svårt att knäcka. Se kapitel 5 för tips om bra lösenord!

dessa av lösenord, men ibland är de helt öppna. Som användare är det praktiskt – bara att ansluta och sätta igång att surfa. Men man ska komma ihåg att ens information då kommer flyga genom luften, ofta helt okrypterad och därmed möjlig att avlyssna.

Det finns till och med särskilda program som används för att snappa upp människors lösenord från sådana nätverk. De är förbluffande effektiva och kan enkelt användas av vem som helst som är i närheten av kaféet eller hotellet.

Därför är det en god idé att vara mer försiktig när man surfar från ett kafé. Visst är det okej att kolla nyhetssidor, men om du hanterar något mer känsligt bör du vidta vissa åtgärder.

För det första: Kontrollera om adressen i din webbläsare börjar på "https" istället för "http". Det betyder att anslutningen är krypterad och svårare att avlyssna.

4.4 Proffskryptering med VPN

Vill du vara riktigt säker på att ingen avlyssnar dig när du använder ett publikt nätverk så är det enda alternativet att kryptera allt du gör. Det enklaste sättet att lösa det är med tekniken VPN, som står för virtual private network – virtuellt privat nätverk.

Att använda VPN innebär att din uppkoppling mot en sajt, till exempel Gmail.com, inte går direkt från dig till Gmail. Istället går allt ditt surfande via en speciell server som du ansluter till med stark kryptering. Rent tekniskt använder du därför det lokala nätverket bara för att ansluta till en enda server: VPN-tjänstens server – och tack vare att anslutningen dit är krypterad så flyger ingen oskyddad information omkring i luften på kaféet där du sitter. Tänk på att din uppkoppling bara skyddas fram till den vpn-server du använder. Därefter kan den röra sig på nätet helt okrypterad,

Viktigt!

Lösenord – men ingen kryptering

Vissa publika nätverk släpper in användaren utan lösenord men kräver inloggning (och ibland betalning) innan man kan besöka en webbplats eller hämta sin e-post. Detta är en annan sorts inloggning än den som beskrevs här ovan och innebär inte att nätverket är krypterat. Med andra ord: Betrakta dem som helt öppna och använd dem därefter.

Detta system används till exempel av Telias tjänst Homerun och SJ:s trådlösa nätverk ombord på tågen.

men här fokuserar vi på att undvika avlyssning på kaféets trådlösa nätverk.

VPN används av många företag vars anställda arbetar utanför kontoret. Men det kan också köpas som en tjänst av privatpersoner för några tior i månaden. Det finns en mängd kommersiella tjänster att välja mellan. I grunden gör de alla samma sak, men hastigheten kan variera. Eftersom ditt surfande tar en omväg via en server så kan uppkopplingen bli långsammare. Därför är det värt att testa ett par tjänster och själv avgöra vilken som går snabbast för dig.

Tips!

Använd (nästan) alltid https

Många webbplatser erbjuder möjlighet att köra krypterat över https, men har det inte aktiverat från början. Om du använder antingen Google Chrome eller Firefox som webbläsare så finns ett gratis insticksprogram som heter HTTPS Everywhere. Med det installerat kommer webbläsaren alltid välja https när det är möjligt.

Läs mer och ladda hem:
https://www.eff.org/https-everywhere

05 Lösenord och tvåfaktorsinloggning

Tänk att du ska logga in på alla sajter du någonsin har registrerat dig på. Hur många lösenord skulle du behöva komma ihåg? Fem? Tio? Hundra?

Lösenordet är fortfarande det i särklass vanligaste sättet att identifiera sig på internet. Ändå är så gott som alla säkerhetsexperter överens – lösenord är ingen bra lösning och borde ersättas så snart det bara går. Problemen med dem är många. Knappt någon kan komma ihåg alla sina lösenord. Gång på gång kommer hackare över stora databaser med vanliga människors lösenord och kan logga in på deras konton.

Vi ska snart komma in på vilka alternativ som finns, men det är lika bra att vi på en gång slår fast en sak: Lösenorden kommer finnas kvar ett bra tag framöver. Därför är det viktigt att lära sig använda dem på rätt sätt. Vi börjar med själva ordet – hur ska ett bra lösenord se ut?

5.1 Att välja ett bra lösenord

Lösenord ska vara långa, svåra att gissa och innehålla mer än vanliga bokstäver. Låter det som ett recept för lösenord som ingen människa klarar av att komma ihåg? Jo, så kan det vara. Men det finns knep som gör det enklare. Här går vi igenom hur man kan välja ett lösenord som är svårare för en angripare att komma över. Se till att läsa guiden ända till slutet, för lösenordet vi börjar med är ett riktigt dåligt exempel.

Så här ser många lösenord ut, kanske speciellt för en hundintresserad: *rottweiler.*

Vad är då problemet? Vi börjar med längden. Ett vanligt råd är att lösenord ska vara minst åtta tecken långa. Det är en bra tumregel, men det finns egentligen ingen anledning att inte gå längre än så. Väljer du rätt så är det lika enkelt att komma ihåg ett lösenord som är femton tecken långt. Kom ihåg – ju fler bokstäver och andra tecken du väljer desto mindre är risken att någon

främmande kan komma in på ditt konto.

Den andra regeln är att det ska vara svårt att gissa. Här finns några regler som alla bör följa stenhårt: Ditt lösenord ska aldrig vara ett vanligt ord eller namn. Det största misstaget är att använda ett ord som är starkt förknippat med dig själv – namnet på ett husdjur eller en släkting, ditt eget efternamn eller liknande. Sådana är lätta att gissa sig till eller hitta på nätet. Kanske har du skrivit om ditt husdjur på Facebook eller bloggat om din familj? I så fall tar det inte många sekunder att identifiera ett par namn att prova som lösenord.

Med andra ord är *rottweiler* ett dåligt lösenord, speciellt om du har pratat om ditt intresse för denna hundras på nätet. Även om du inte skulle ha gjort det så finns ordet i ordlistor, vilket förenklar gissningsarbetet avsevärt. (Varför ordlistor gör en attack enklare går vi igenom i nästa avsnitt.)

Ett sätt att både göra lösenordet längre och slippa problemet med ordlistor är att helt enkelt lägga till fler ord. Det behöver inte göra lösenordet mycket svårare att komma ihåg:

minhundrottweilern

(Tänk "min hund rottweilern", men ofta får lösenord inte innehålla mellanslag.) Vips så är vi uppe i 18 bokstäver, vilket är betydligt bättre.

Den tredje regeln gäller vilka bokstäver och tecken man använder. Här gäller samma princip – ju svårare det är att gissa desto säkrare är lösenordet. Fler sorters tecken betyder fler möjliga varianter av lösenordet och därmed ett klurigare gissningsarbete. Ett första steg är att blanda stora och små bokstäver. Det finns många sätt att göra det:

MinHundRottweilern
MinHundROTTWEILERN
minHUNDrottweilern

Till sist – ett starkt lösenord innehåller inte bara bokstäver, utan också siffror och specialtecken som till exempel €, # eller &. Visst är det bra att välja tecken eller siffror som är lättare att komma ihåg, men undvik de mest uppenbara som till exempel ditt födelseår.

Som vän av rottweilerhundar kanske man vet att den registrerades av den amerikanska kennelklubben år 1931.

minHUNDrottweilern1931

… eller varför inte:

minHUND1931rottweilern

Att knäcka ett lösenord är aldrig helt omöjligt – men man kan göra det svårare för angriparen. Med ett lösenord av den här typen har du åtminstone inte gjort det onödigt enkelt, och dessutom slipper du ett obegripligt lösenord av typen *8F€€FvoZ2"€*.

Varning!

Enkla knep kan genomskådas

Ett vanligt knep för de som vill göra lösenord svårare att genomskåda är att ta ett vanligt ord och byta ut bokstäver mot siffror som liknar dem. *Telefon* blir *t3l3fon* och så vidare. Men eftersom knepet är välkänt kan angriparen ställa in sitt knäckningsprogram för att testa dessa varianter.

Att göra varje begynnelsebokstav i lösenordet stor är lockande, eftersom det är enkelt system att memorera. Men av samma anledning är det enklare att gissa sig till. Försök hitta ett system som inte genomskådas lika lätt.

Men varför behöver man krångla till det så här? För att begripa det måste man förstå hur en attack går till.

5.2 Så knäcks ett lösenord

Vi har nu visat skillnaden mellan ett lättknäckt och ett svårknäckt lösenord. Men varför är skillnaden så stor? Förklaringen ligger i de två vanligaste metoderna som angripare kan använda.

Man talar ofta om att "gissa lösenordet". Visst kan det hända – det är därför man aldrig ska välja till exempel sitt barns namn som lösenord. Men oftast handlar det om två automatiska metoder: Dels en så kallad *ordlisteattack* och dels metoden *brute force*, vilket kan översättas till "råstyrka" på svenska.

Du kanske har sett nyheter om att listor med lösenord har läckt från stora webbplatser. Ibland talas det om att lösenorden som har läckt är krypterade – och det kan ju låta tryggt. Det som är krypterat borde väl vara säkert?

Nej, faktiskt inte. För när angriparen väl har kommit över en läckt lösenordslista så kan hen använda speciella program för att gissa lösenord i blixtsnabbt tempo. Det kan liknas vid att försöka logga in flera miljarder gånger i sekunden, eller ännu oftare. Men de flesta sajter skulle stänga en angripare ute efter ett par misslyckade försök. För den som har kommit över listan med krypterade lösenord finns inga sådana begränsningar.

Vi börjar med att förklara brute force-attacken. Principen är simpel: Gissa varje tänkbart lösenord. Säg att vi utgår från att lösenordet som ska knäckas är mellan tre och åtta tecken långt. Då kan den första gissningen vara "aaa" som följs av "aab"

och sedan "aac". När alla kombinationer av tre bokstäver är testade är det bara att gå vidare till de med fyra bokstäver. Och så vidare. Som du förstår blir det en hel del gissningar, men en kraftfull dator kommer klara av alla möjliga kombinationer på några sekunder.

Men om angriparen inte bara behöver gissa mellan kombinationer av bokstäver, utan också vilka som ska vara versala och vilka som ska vara gemena? Då blir alternativen fler – och därmed krävs fler gissningar. Detsamma sker när du lägger in specialtecken eller gör ditt lösenord längre.

Ordlistan då? Att knäcka ett lösenord med hjälp av ordlista är den allra enklaste genvägen. När man ska knäcka ett lösenord testar man ofta först alla ord man har i en ordlista. De innehåller de vanliga ord, namn och annat som många väljer som lösenord. Det kan röra sig om hundratusentals exempel, men 100 000 gissningar är mycket litet i sammanhanget. En dator klarar det på bråkdelen av en sekund.

Kort sagt: Om du väljer ett vanligt ord kan du räkna med att lösenordet kan knäckas omedelbart. Låt oss ta några exempel:

- *fido*: Ett riktigt dåligt lösenord. Kan mycket väl finnas i angriparens lösenordslista, och även om det inte gör det så knäcks det på bråkdelen av en sekund.
- *rottweiler*: Något bättre, eftersom det är längre. Men även detta finns i ordlistor.
- *minhundrottweilern*: Redan här börjar det se riktigt bra ut. Förutsatt att angriparen inte har några ledtrådar om lösenordets längd eller vad det består av så är lösenordet svårt att gissa sig till.

Men sådan tur har man inte alltid. Ju fler av råden som nämns här ovan desto säkrare blir ditt lösenord. Om du byter från *minhundrottweilern* till *minHUND1931rottweilern* så ökar antalet möjliga kombinationer ytterligare.

Att knäcka ett långt lösenord med en vanlig hemdator skulle ta flera miljoner år om angriparen skulle vara tvungen att testa alla tänkbara alternativ. I praktiken är det sällan så. Genom sofistikerade metoder, till exempel så kallade regnbågstabeller, kan antalet gissningar som behöver genomföras sänkas dramatiskt. Därmed knäcks lösenordet snabbare – ännu ett gott skäl att använda ett långt och svårknäckt lösenord.

5.3 Samma lösenord överallt?

Du har säkert konton på nätet som skulle kunna bli hackade utan att det gör speciellt

stor skada. Till exempel inloggningen till en filmtjänst – att ditt lösenord dit knäcks skulle bara innebära att någon kan se film på din bekostnad. Värre saker kan hända.

Många resonerar så och väljer därför samma lösenord på en mängd sajter. Vad de inte tänker på är att om lösenordet läcker från en av dessa sajter så kommer angriparen åt dem allihop. Det är nämligen enkelt att testa om lösenordet som visade sig fungera på en webbplats även gäller på en annan.

Värst är det om man har använt samma lösenord på "skräpsajter" och för konton som är viktiga – till exempel din e-postadress. I samband med att lösenord läcker ut läcker ofta även e-postadressen eftersom den används som användaridentitet. Säg att det är en Gmail-adress. Då är det lätt för angriparen att gå till gmail.com och försöka logga in med lösenordet som redan är på villovägar.

Därför är det viktigt att inte använda samma lösenord och e-postadress överallt. Börja med att identifiera dina viktigaste konton.

Din e-postadress hör till dem, inte minst eftersom den kan användas för att skapa nya lösenord på andra sajter. Det är ju dit mejlen kommer när du har glömt ett lösenord och ber att få ett nytt. Med andra ord kan den som har tillgång till ditt e-postkonto snabbt ta kontroll över varenda konto du har på nätet.

För många har Facebook blivit lika viktigt som e-post, och den som använder Twitter flitigt bör ha ett unikt, starkt lösenord även där. Hur listan över viktiga konton ser ut varierar från person till person. Vilket konto skulle det vara värst om någon utomstående tog över?

Här är det lätt att tänka "ingen bryr sig väl om mitt konto"? Men faktum är att just Facebookkonton är högvilt för bedragare, och det handlar inte om att de är nyfikna på dina meddelanden.

En vanlig bedrägerityp bygger nämligen på att en angripare tar över ditt Facebookkonto. Med det under kontroll kan hen starta en chatt med en av dina vänner, där hen utger sig för att vara du. Historien bedragaren diktar upp brukar handla om att du är utomlands och har blivit av med plånboken. Därför ber bedragaren om ett snabbt lån, som ska betalas direkt till utlandet via till exempel Western Union. Men i själva verket är det bedragaren som plockar ut pengarna, allt på grund av att lösenordet till ditt Facebookkonto hamnade på villovägar. När vännen väl upptäcker att det inte var dig hen pratade med är det i regel för sent.

Med andra ord – undvik till varje pris att använda samma lösenord överallt. Klarar du inte av att ha ett lösenord för varenda sajt du har registrerat dig på, ha åtminstone unika på de viktigaste.

5.4 Programmen som hjälper dig

Ju bättre du blir på att välja lösenord desto fler får du att hålla reda på. Det får många att snart falla tillbaka i att använda samma lösen överallt. Men det finns en rad program som kan hjälpa dig.

De kallas lösenordshanterare och bygger på en enkel princip: Hela din samling lösenord ligger sparade i en krypterad (och därmed oläslig) databas som skyddas med ett lösenord. Som du förstår är detta lösenord det viktigaste du någonsin kommer välja – med hjälp av det får man ju tillgång till alla lösen du har sparade.

Ett lätt sätt att lösa problemet är att låta webbläsaren spara lösenord. Det förenklar inloggningen, men innebär också att alla som kommer åt din dator kan logga in lika enkelt. Det har till och med visat sig möjligt att plocka fram de sparade lösenorden ur webbläsaren, vilket kan kännas oroande.

Om du istället vill använda ett separat program för att hantera lösenord finns det många alternativ, varav några syns i listan här intill.

5.5 Två faktorer – framtidens inloggning

Säkerhetsexperter har gång på gång dömt ut lösenorden som en förlegad säkerhetsmekanism. Men vad ska då användas istället?

Syftet med en inloggning är att kontrollera att bara rätt personer har åtkomst till informationen som söks, exempelvis den du har på ditt e-postkonto. För att få ett starkare skydd kan man komplettera användarnamn och lösenord med fler parametrar. Exempelvis någonting som berättar vem användaren är (fingeravtryckskläsning, röstanalys, ögonskanning) eller någonting som användaren har (ett smart kort eller en säkerhetsdosa).

Tanken är att lösenordet ska kunna hamna i händerna på en angripare utan att hen kan logga in på ditt konto. På samma sätt kan man tappa bort säkerhetsdosan utan att den som hittar den kan logga in.

Låter det märkligt? Förmodligen använder du redan tvåfaktorsinloggning, till exempel för din internetbank. Där används ofta säkerhetsdosor med kort tillsammans med en kod eller ett lösenord.

Det är en utmärkt idé att skydda även ditt e-postkonto med denna metod. Många av de stora mejltjänsterna har redan stöd för det. Ofta behöver du inte ens en extra

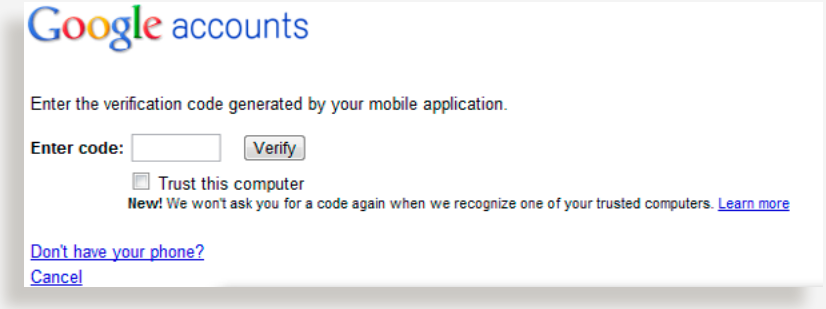
Tips!

Välj lösenordshanterare noga

Det finns en uppsjö program som hjälper dig att hantera dina många lösenord. De flesta fungerar som krypterade databaser där du lagrar lösenorden. Tänk dock på att du verkligen måste kunna lita på den tjänst du väljer. Om möjligt – välj ett program med öppen källkod, så experter har möjlighet att granska den i jakt på säkerhetsluckor. Vissa program lagrar lösenorden på sina egna servrar, eller "i molnet" som det ofta kallas. Här finns det anledning att vara skeptisk, eftersom du måste lita på att de skyddar sina servrar tillräckligt noga. Oavsett vilket du väljer så finns det några saker du bör tänka på.

1. För det första är det bra om programmet finns till både Windows och Mac, och kanske Linux om det är något du överväger. Skulle du byta dator så är det praktiskt att kunna ta lösenorden med dig, utan att behöva skriva av dem ett och ett.
2. För det andra fungerar många av dem också på mobiltelefoner. Så länge de säkras med bra lösenord är det en utmärkt idé, eftersom du då kan plocka fram de lösenord du behöver även när du inte sitter vid datorn, speciellt om du har sparat mer än bara lösenord till webbplatser. Många använder samma program för till exempel portkoder.
3. För det tredje – och detta är viktigast av allt – välj ett program som är betrott. Ladda bara hem det från den officiella webbplatsen och sök gärna runt efter information om eventuella säkerhetsrisker.

Lösenordshanteraren 1Password kräver huvudlösenordet för att öppnas.



Tvåfaktorsinloggning gör webbmejl och andra tjänster betydligt säkrare att använda.

säkerhetsdosa utan använder mobilen. När tekniken är aktiverad använder du en engångskod tillsammans med ditt vanliga lösenord för att logga in. Mejltjänsten skickar engångskoden till dig antingen i ett sms, eller via en särskild app.

Låter det krångligt? För att göra det enklare behöver du inte ange engångskoden vid varje ny inloggning, om den sker från samma dator. Hur ofta du måste skriva in ett nytt engångslösenord varierar mellan tjänsterna.

Tips!

Mejltjänsterna med stöd för tvåfaktorsinloggning

Gmail
Aktivera funktionen i dina kontoinställningar. Sedan anger du ditt telefonnummer för att få engångskoder skickade via sms, eller laddar hem appen Google Authenticator till Android eller Iphone.

Outlook (tidigare Hotmail)
Även Microsoft har en speciell app för sin tvåfaktorsinloggning.

Viktigt!

"Skriv aldrig ner ditt lösenord"

Att skriva sitt lösenord på en papperslapp och gömma det under tangentbordet beskrivs ibland som ett klassiskt misstag. Där lär ju den som vill stjäla det leta allra först.

Visst är det ett dåligt gömställe, och programmen för lösenordshantering vi nämner här ovan är betydligt bättre alternativ.

Men faktum är att Bruce Schneier, en av världens främsta säkerhetsexperter, argumenterar för att man visst kan skriva upp viktiga lösenord på en papperslapp och ha den i plånboken. Hans argument bygger på två delar: Dels att starka lösenord i dag måste vara så starka att de blir närmast omöjliga att komma ihåg. Dels att vi är vana vid att hantera små papperslappar säkert i våra plånböcker. Det är trots allt samma ställe som vi använder för sedlar.

06 E-post är som vykort

E-post är kanske den mest fundamentala kommunikationsformen på nätet. Du skriver några rader, klickar "send" (skicka), och vips har ditt meddelande landat hos mottagaren. Blixtsnabbt och enkelt. Men säkert? Inte alls.

Att skicka ett mejl kan mest av allt liknas vid att skicka ett vykort – utan kuvert – på posten. Faktum är att vykort förmodligen är ett bättre val om du har hemligheter att förmedla i text, för de passerar betydligt färre snokande ögon än ett genomsnittligt mejl.

På väg till mottagaren studsar ett mejl via en mängd servrar anslutna till nätet. Vid varje enskild punkt är det en lätt match att läsa vad som står skrivet i det. Din e-postleverantör, din internetleverantör och din arbetsgivare (om du använder företagsmejlen) kan alla enkelt ta del av de mejl du skickar. Likaså de personer som kontrollerar de övriga servrar mejlet passerar genom.

Det beror på att mejl skickas över nätet i klartext – som bokstäver, siffror och andra tecken – och därmed kan läsas med blotta ögat var som helst längs vägen. I e-posttekniken finns inga inbyggda säkerhetsåtgärder som döljer det du skriver för andra än mottagaren. Ej heller några sätt för dig som avsändare att avgöra om, och i sådana fall vem, som tagit del av informationen du skickat. En angripare som vill komma över just din kommunikation kan alltså ta hjälp av ett program för att spela in all trafik som rör sig in och ut från just din dator, för att sen i lugn och ro leta fram just de e-postmeddelanden som är intressanta.

Med andra ord är e-post i grunden otjänligt för den som är mån om att hålla hemligheter hemliga. Den som ändå vill mejla, men utan att nyfikna lägger näsan i blöt, måste ta saken i egna händer.

6.1 Kryptering – säkert men lite krångligt

Att kryptera ett meddelande innebär att kasta om bokstäverna i det så att ingen, förutom mottagaren, kan ta del av informationen. I grund och botten fungerar det på samma sätt som barndomens lekar med hemliga kodspråk: I Astrid Lindgrens böcker om mästerdetektiven Kalle Blomqvist pratar huvudpersonerna rövarspråk med varandra, genom att lägga

Tips!

Flera e-postkonton – en genväg till säkerhet

Ett enkelt säkerhetsknep är att använda olika e-postkonton för olika syften. Använd din ordinarie för seriös kommunikation. Det är den adress du kan skriva på visitkort och lämna ut till bekanta som du ska kommunicera med. Skaffa ett gratis, extra konto hos Gmail, Hotmail, Yahoo eller liknande som du bara använder när du registrerar dig på sajter. Se det som ditt "skräpkonto", speciellt för när du registrerar dig på mer "amatörmässiga" webbtjänster, där säkerheten kan misstänkas vara sämre.

Samma adress kan användas när du laddar hem program från nätet, vilket ibland kräver registrering. Det är den extra adressen som du kommer använda för att få ut nya lösenord från webbplatserna du är registrerad på om du har glömt bort det. Därmed slipper du lämna ut din ordinarie e-postadress till höger och vänster. Det minskar mängden skräppost och innebär dessutom att din mejladress inte ligger lagrad tillsammans med lösenord.

Men kom ihåg – även om du använder ett skräpkonto ska du aldrig använda samma lösenord till din viktigaste e-postadress som du använder på andra webbplatser. Du ska inte heller ha samma lösenord till ditt ordinarie konto som till ditt skräpkonto.

in ett "o" efter varje konsonant och sen upprepa den igen. Ordet "rövarspråket" blir då till "rorövovarorsospoproråkoketot". Tanken är att bara den som känner till metoden förstår vad som sägs.

Moderna krypteringsmetoder bygger på liknande principer, men är i praktiken omöjliga att ta sig igenom utan rätt nyckel. Texten körs genom en algoritm, ungefär som ett matematiskt recept, som gör den oläslig. Bara den som känner till lösenordet, dekrypteringsnyckeln, kan backa bandet och göra den till klartext igen.

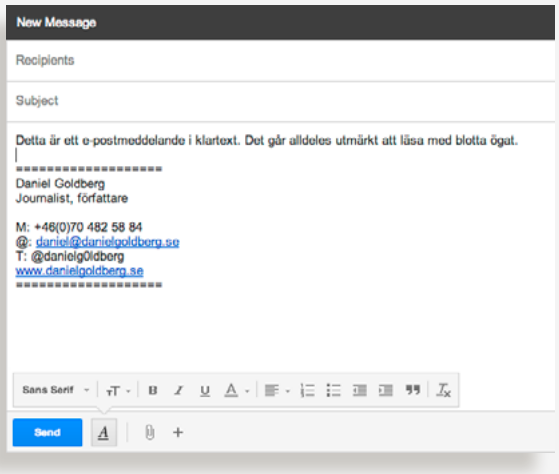
En av de mest spridda krypteringstekni-

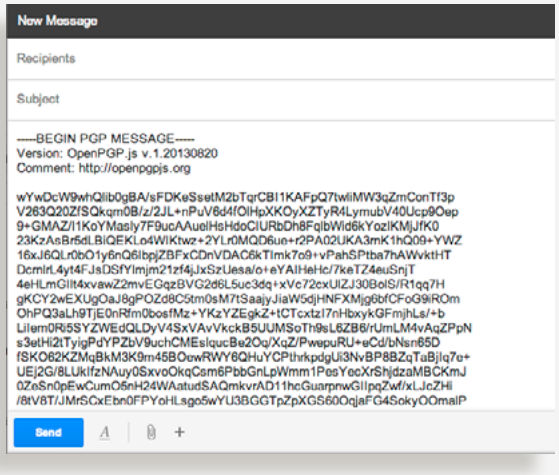
kerna idag heter PGP, vilket står för Pretty Good Privacy. Den uppfanns redan år 1991 av programmeraren Phil Zimmerman. Företaget PGP ägs idag av antivirusjätten Symantec men standarden, som går under namnet OpenPGP, är öppen och fritt tillgänglig för vem som helst att utveckla produkter kring (se nedan).

PGP bygger på ett system där två nycklar är inblandade: en publik och en privat. Båda behövs för att kommunikationen ska fungera, men bara den ena behöver hållas hemlig.

För att skicka ett PGP-krypterat meddelande till någon behöver du först personens publika nyckel. Denna är en serie till synes slumpmässigt utvalda tecken (se bild). Många som använder PGP publicerar sina publika nycklar öppet, till exempel längst ned i sin mejlsignatur, eller under kontaktfliken på sin sajt eller blogg. Andra gör sin publika nyckel tillgänglig på en så kallad nyckelserver. Det är att likna vid en telefonbok, där mängder av nycklar finns listade efter vem de tillhör. På samma vis måste du ge din publika nyckel till någon för att den personen ska kunna mejla dig.

Om du vill vara absolut säker på att den person som kontaktar dig verkligen är den hen utger sig för att vara så bör du vara noga med hur du delar ut din publika nyckel. Att bara skicka över den i ett mejl





Som synes blir ett e-brev oläsligt för obehöriga sedan det krypterats.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP.js v.1.20130627
Comment: http://openpgpjs.org

xo0EUdaPXgED/2fEkPY9lbPpgXdr4lwZQr6i2KBdLVQvS1HEb4wxx3RUNxP/
2VDp5691vafRc6ZibHcC6BT7KuEjH4WwxJo2gR6my52HvMEzTXHzlmWlo6T3
v2+V2kSEmLofgmew31ztU7SLccnGB0PoUmTlSxiWp0Rt3F9ZETa7iQt1rRa4
Dv5XABEBAAHNLGRhbmllbCBnb2xkYmVyZyA8ZGFuaWVsZ29sZGJlcmc4MkBn
bWFpbC5jb20+wpwEEAEIABAFAlHWj18JEHFvcIUJYm9IAABSrgP/X0Jnpm8k
n3B089htqGZxkY0yEP051j/jstwksK7yeY8YnnfYPDYLT/y1/7xkzJnuzfbg
eX7F1uDy1YJMl/M+2NAXSzcAxfN3BEqDGbjc1l3SqlSfaPMx64JbFCi3nfZ3
Ik1n/qGqEnkqB/V7njRo3uguzk1Ad2H5zK/Cx3/vBt8=
=ghwW
-----END PGP PUBLIC KEY BLOCK-----
```

Exempel på en publik PGP-nyckel vilken används som signatur i e-post.

anses inte vara tillförlitligt – en person som avlyssnar kommunikationen kan då skicka krypterade mejl till dig.

Förr i tiden ordnades såkallade PGP-signeringspartyn, där deltagarna utbytte nycklar med varandra och samtidigt legitimerade sig med id-kort. På så sätt kunde alla vara säkra på att personen de pratade med verkligen var rätt. Om du vill vara extra noga så kan du bete dig på ett liknande sätt – stäm helt enkelt träff med den du vill mejla säkert med, och lämna över nycklar öga mot öga.

Nästa steg är att skriva ditt meddelande i krypteringsprogrammet, för att sen kryptera det med mottagarens publika nyckel. Resultatet, ett sjok till synes oläslig text, klistrar du in i ett vanligt mejl och skickar till din mottagare. Hen kan sedan dekryptera texten med sin hjälp av sin privata nyckel.

Din privata nyckel sparas i regel som en fil på din dator. Du kan även exportera den i textform eller som en fil, för att lagra den på exempelvis ett USB-minne. För att komma åt den privata nyckeln används ett lösenord, som du matar in i krypteringsprogrammet.

PGP anses vara en mycket pålitlig krypteringsstandard. Så länge du väljer ett starkt lösenord till din privata nyckel (se kapitel 2: ”Lösenord och tvåfaktorsinloggning” för mer om bra och dåliga lösenord) och ser till att hålla den hemlig kan du alltså vara trygg i att ingen tjuvlyssnar på ditt mejlande.

Men vad händer om en angripare listar

ut mitt lösenord? Då är det givetvis fritt fram för personen, förutsatt att hen också har tillgång till datorn där din privata nyckel finns lagrad, att läsa all din krypterade e-post. Men så länge du valt ett ordentligt starkt lösenord är det mycket osannolikt att så sker.

6.2 Tre enkla krypteringsverktyg

Det finns en uppsjö program på nätet som hjälper dig att komma igång med kryptering snabbt och enkelt. Här är tre alternativ som är värda att titta närmare på.

SÄKRARE WEBBMEJL MED MAILVELOPE

Mailvelope är ett enkelt insticksprogram för dig som använder webbmejl som Gmail eller Outlook.com. Med det installerat krävs bara ett par knapptryckningar för att göra dina mejl oläsliga för andra utom mottagaren. Vissa är skeptiska till att låta ett insticksprogram i webbläsaren hantera krypteringen, men för webbmejl som Gmail är det definitivt bättre än ingen kryptering alls. Mailvelope bygger på PGP och är mycket smidigt att använda.

Viktigt att komma ihåg är att Mailvelope bara krypterar textinnehållet i dina mejl. Vill du även skydda dina bifogade filer krävs ytterligare mjukvara (läs mer om Truecrypt nedan).

Börja med att installera programmet via www.mailvelope.com. Det fungerar för både Chrome och Firefox, både till Mac och Windows. När det är på plats och aktiverat i webbläsaren (klicka dig fram till plugins-fliken i din webbläsare) så kommer du att se en ny ikon i form av ett hänglås, till höger om webbläsarens adressfält.

Det första du behöver göra är att skapa din krypteringsnyckel. Den publika delen måste du ge till mottagaren, för att hen ska kunna skicka mejl till dig (oroa dig inte för att den hamnar i orätta händer, den publika nyckeln är till för att spridas öppet). Den privata nyckeln måste du däremot se till att hålla hemlig. Om någon får tag på den så kan de direkt avkryptera alla hemliga mejl som skickas till dig.

Klicka på hänglåset, välj “options” och sedan “generate key”. Fyll i ditt namn och din e-postadress. Istället för lösenord ber Mailvelope om en “passphrase” – ett råd om att lösenordet ska vara långt som en hel mening. Följ detta råd!

Klicka sen på ”display keys” så ser du din egen publika nyckel i listan. Via “Export”-menyn kan du skicka den direkt till din mottagare.

Dina vänners nycklar lägger du till genom att klicka på “import keys”.

Nu är du redo att mejla säkert! Logga in

Varning!

Håll din privata nyckel hemlig – men tappa inte bort den

Säkerheten i PGP hänger helt och fullt på att din privata nyckel aldrig hamnar i orätta händer. Se därför till att välja ett starkt lösenord till den (se kapitel 2 för mer information om detta). Se även till att memorera det i huvudet och ha det inte antecknat på några papperslappar som ligger framme. Använd aldrig din privata nyckel, och knappa aldrig in ditt lösenord, på en dator som du inte vet är fri från avlyssningsprogram eller annan skadlig kod (till exempel en allmän dator på ett kafé eller ett bibliotek).

Lika viktigt är att inte tappa bort nyckeln. Utan din privata nyckel är det i praktiken omöjligt att låsa upp information som krypterats för dig.

på webbmejlen och påbörja ett nytt mejl. Notera den nya hänglåsknappen i textfältets övre högra hörn. Klicka på den för att öppna ett specialfönster för kryptering.

Det listiga med detta fönster är att orden du skriver aldrig lämnar din egen dator. Det finns alltså ingen möjlighet ens för Google att läsa av texten i okrypterat tillstånd. Skriv alltså precis som vanligt. När du är klar klickar du på hänglåset, väljer mottagare (av de vars nycklar du har importerat) och bekräftar. Vips blir texten obegriplig – ja, just det – krypterad. Tryck på "Transfer" för att klistra in det i mejlet, och skicka därefter som vanligt.

Om du får ett krypterat mejl av en vän, klicka då på hänglås-symbolen som syns över den krypterade texten. Mata in ditt lösenord och vips – texten förvandlas till läsbart skick igen.

GPGMAIL – KRYPTERING PÅ DEN EGNA MACEN

Mailvelope är ett utmärkt alternativ för webbmejlanvändaren. Men för den som håller fast vid lokala e-postprogram behövs andra alternativ. För dig som kör Mac är GPGMail ett bra alternativ. Det bygger i grunden på samma PGP-teknik för att hålla dina meddelanden trygga.

GPGMail är en plugin till Mac OS X inbyggda e-postprogram Mail. Det ingår i paketet GPG Suite som också innehåller fler krypteringsverktyg, men här fokuserar vi på e-postkrypteringen.

Ladda hem paketet från www.gpgtools.org. Installationen behöver ingen närmare beskrivning, och principen är densamma som för Mailvelope. Du be-

höver importera dina kontakters publika nycklar och de behöver importera din publika nyckel innan ni kan kommunicera med varandra.

När programmet är installerat dyker några extra knappar upp i fönstret där du skriver din e-post. Hänglåset är den viktiga knappen – precis som i Mailvelope är det den du klickar på för att förvandla ditt vanliga e-postmeddelande till ett krypterat.

Att ta emot krypterade brev är ännu enklare. Dessutom visar programmet tydligt att meddelandet skickades på ett säkert sätt, även när det har låsts upp så du kan läsa det.

Till skillnad från Mailvelope krypterar även GPGMail dina bifogade filer. Även dessa är alltså oläsliga för alla utom din tilltänkta mottagare.

SKYDDA BIFOGADE FILER MED TRUECRYPT

Med hjälp av Mailvelope skyddar du textinnehållet i dina mejl, men inte bifogade filer. För det behövs andra program, som till exempel Truecrypt.

Truecrypt är ett välkänt krypteringsprogram som finns för både PC och Mac. Det kan användas både för att kryptera enskilda filer eller hela minnesenheter, exempelvis ett USB-minne eller en hårddisk. Vad gäller enskilda filer kan man, något förenklat, säga att Truecrypt skapar en låst behållare i vilken dina filer göms. Behållaren kan bara öppnas av den med rätt lösenord. Programmet är gratis att använda och kan laddas ned från www.truecrypt.org.

Genom att bifoga en Truecrypt-behållare med ett mejl krypterat med Mailvelope skyddar du alltså både mejlets textinnehåll och dina bifogade filer från avlyssning.

Tips!

Mejlkryptering till Windows

En bra och kostnadsfri lösning som liknar GPGMail för Mac är GPGWin för dator som använder Windows. Finns att laddas ned från www.gpg4win.org

Varning!

Din e-postadress syns fortfarande

Genom att kryptera ett mejl skyddar du dess innehåll från objudna gäster. Däremot visas fortfarande din egen adress och mottagarens adress (samt en hel del annan information som till exempel vilken tid och vilket datum mejlet skickades) öppet. Sådana uppgifter brukar kallas för metadata, och är i de flesta fall mindre viktiga att skydda än mejlets själva textinnehåll. Men för dig som är mån även om att skydda din och mottagarens identiteter är det viktigt att känna till.

Ett enkelt sätt att komma runt problemet är att kombinera kryptering med anonyma och temporära mejladresser. Är du riktigt mån om både din och mottagarens anonymitet, be hen göra det samma.

Grundprincipen med Truecrypt är enkel: Du använder programmet dels för att skapa krypterade behållare, men också för att öppna de som skickas till dig. Varje behållare skyddas av ett lösenord som behövs för att öppna den. Vill du skicka någon en Truecrypt-behållare måste du alltså även skicka personen rätt lösenord (ett smidigt sätt är att göra detta i form av ett krypterat mejl. På så vis förhindrar du att lösenordet snappas upp av någon annan på vägen).

I praktiken kan Truecrypt vara ett ganska knepigt program att använda. En utmärkt nybörjarguide finns på http://www.truecrypt.org/docs/tutorial. Den beskriver steg för steg hur du går till väga för att skapa en krypterad behållare.

Viktigt!

Regeringar kan nog inte knäcka allt

Det har varit svårt att undgå rapporteringen om amerikanska NSA:s massavlyssning av e-post och internettrafik. Hösten 2013 avslöjades dessutom, med stöd i dokument från visselblåsaren Edward Snowden, att de amerikanska och brittiska underrättelsetjänsterna lyckats knäcka flera av de mest använda krypteringsformerna på nätet.

Varför, kanske du undrar, ska man då ens bry sig om att försöka mejla säkert, när hemliga agenter ändå kan läsa allt?

För det första: Att regeringar kan avlyssna allt som sägs på nätet är en sanning med modifikation. Edward Snowdens uppgifter om knäckta krypteringstekniker påstår, något förenklat, tre saker. Amerikanska NSA har lyckats ta sig förbi den standard som gäller för krypterad trafik över nätet (den teknik som är aktiv när du ser ett litet hänglås i webbläsarens adressfönster, och som till exempel används när du köper någonting med ditt bankkort hos en e-handlare). Man har dessutom lyckats påverka internationella krypteringsstandarder för att göra dem lättare att knäcka, samt övertygat kommersiella säkerhetsleverantörer att installera bakdörrar i de produkter de säljer. Det är mycket allvarliga uppgifter, men de gäller inte allt. Som säkerhetsexperten Bruce Schneier konstaterade: "De gör det genom att fuska, inte genom matematik".

I skrivande stund vet ingen om även de program vi rekommenderar i det här avsnittet är öppna för avlyssning. Mycket talar för att så inte är fallet. PGP-standarden har existerat i mer än 20 års tid. Lika länge har den synats i sömmarna av världens främsta säkerhetsexperter. Ingen har lyckats hitta svagheter i den, ej heller spår av hemliga bakdörrar som låter de amerikanska myndigheterna smita förbi krypteringen.

Förutsatt att inga hittills okända bakdörrar finns i koden – de "fusk" som Bruce Schneier talar om – så återstår bara rå kraft. Men att knäcka en PGP-nyckel genom att testa alla möjliga kombinationer är i praktiken mer eller mindre omöjligt.

Låt oss också anta att du använder en specialbyggd superdator, som kan testa en miljard miljarder kombinationer i sekunden (vilket är långt över vad som är möjligt i skrivande stund). Även då skulle det ta dig mer än 10 000 miljarder år att testa alla möjliga kombinationer.

Givetvis går det inte att säga med fullständig säkerhet att de amerikanska myndigheterna inte även lyckats ta sig förbi de tekniker vi rekommenderar i den här guiden. Men i nuläget är öppna standarder som PGP och Truecrypt de bästa alternativen för den som vill hålla sitt mejlande säkert.

07 Så skyddar du dina pengar

Du har säkerligen sett rubriker i tidningarna om hur "bedragare länsar ditt kontokort" eller hur hackare tar sig in på din internetbank och tömmer sparkontot på pengar. Brottsligheten på nätet har vuxit blixtsnabbt de senaste åren, och den visar inga tecken på att avta. Lite tillskruvat kan man till och med säga att den har ersatt den gamla tidens rån och stölder – för många brottslingar har nätbedrägerier helt enkelt visa sig mer lönsamma.

För en vanlig användare som har drabbats kan det framstå som ett mysterium. Plötsligt är bankkontot tömt på pengar och det är svårt att begripa vad som hänt. Så hur går digitala bedrägerier till egentligen – och vad kan man göra för att skydda sig?

För att svara på det måste man sätta sig in i några av de vanligaste typerna av itbrott. De ser nämligen helt olika ut beroende på om de riktas mot ditt kontokort eller din internetbank.

7.1 Nätbanken – viktigast av allt

För den som försöker stjäla pengar från privatpersoner på nätet är internetbanken det "bästa" målet. Orsaken är uppenbar – väl inloggad har bedragaren tillgång till samtliga konton och kan därför komma över stora pengar, betydligt mer än ett stulet kontokortsnummer ger. Det är ju kopplat till ett enda konto, i regel ägarens lönekonto.

Lägg till att internetbanker kan användas för att skicka tiotusentals kronor till ett främmande konto så blir det lätt att förstå varför det är nätbankerna som bedragarna helst försöker ta sig in på.

Tidigare var intrång mot nätbanker relativt enkla att genomföra på grund av de undermåliga säkerhetssystemen. Bland de svenska bankerna gällde det framförallt Nordea. Om du var kund i banken för några år sedan så kanske du kommer ihåg engångskoderna som man skrapade fram på ett plastkort och använde för att logga

in och signera betalningar. De var förbluffande enkla att lura till sig. Allt bedragaren behövde göra var att skicka ut tusentals e-postmeddelanden som skickade kunden till en falsk kopia av Nordeas webbplats. Där ombads man knappa in två koder. Men istället för att användas för inloggning skickades de till bedragaren, som i lugn och ro kunde använda dem för att logga in och föra över pengar till ett annat konto, ofta i utlandet (läs mer om sådana bedrägerier i kapitel 3: ”Nätfiske och den okända avsändaren”).

Då och då tog angriparna till mer sofistikerade metoder. Istället för den fejkade Nordeasidan användes också en trojan som snappade upp engångskoder i bakgrunden och smusslade undan dem till bedragarna. På så sätt kom de över flera miljoner kronor.

Sedan dess har säkerheten skärpts, vilket har gjort det svårare för bedragarna. Lösningen består i de flesta fall av säkerhetsdosor med kort samt en pin-kod.

Men det vore fel att tro att faran är helt över. För sedan dess har en ny generation trojaner dykt upp. De är utformade för att överlista just de säkerhetssystem som bankerna införde när skrapkoderna visade sig odugliga – den säkerhetsdosa som du troligtvis använder för att logga in på din internetbank.

Men hur fungerar de? Något förenklat kan man säga att den lägger sig som ett extra lager mellan dig och din internetbank. När trojanen väl har tagit kontroll över din dator så har den i princip fritt spelrum att göra vad den behagar. Till exempel vad du ser på skärmen när du loggar in på din internetbank, eller att ändra det du skriver in till något helt annat.

Anta att du ska betala din elräkning. På pappret från elbolaget står kontonummer, summa och en ocr-kod. Du plockar fram dosan och loggar in som vanligt. Men sedan börjar trojanen agera. När du klickar i menyn för att starta en ny betalning kidnappar trojanen formuläret.

Du skriver in elbolagets kontonummer, men utan att du ser det så ändras det till ett konto som bedragaren kontrollerar. Även summan kan ändras i bakgrunden, utan att det syns på skärmen.

Så när du tror att du godkänner en betalning på 150 kronor till ett elbolag godkänner du i själva verket att en betydligt större summa skickas till ett konto du aldrig har hört talas om. I vissa fall har transaktioner som genomförs på detta sätt uppgått till flera hundra tusen kronor.

Flera trojaner har dykt upp i nätbanksattacker av det här slaget. Ofta har de fantasifulla namn som Zeus (en äldre va-

riant som fått stå modell för efterföljare), SpyEye, Citadel och Ice IX.

Frågan är vad man kan göra för att skydda sig. I kapitel två beskrev vi hur trojaner och annan skadlig kod fungerar, samt vad man kan göra för att hålla sig säker. Om du följer råden där säkrar du dig också mot trojanbaserade angrepp på internetbanken.

Detsamma gäller phishing, alltså utskick av falsk e-post för att lura bankkunder. Från bankhåll har det upprepats gång på gång, men det tål att sägas ännu en gång: Svenska banker skickar aldrig mejl och ber om koder eller andra känsliga uppgifter. Om du får ett sådant – kasta det direkt.

7.2 Kontokortet – bedragarens favorit

Kontokortsbedrägerier har funnits lika länge som det har funnits kontokort. I grunden bygger de alla på samma princip: Någon förfalskar ditt kort eller skaffar ett kort i ditt namn och lyckas använda det för att ta ut pengar ur en bankomat eller köpa varor med det. I många fall behöver bedragaren inte ens skapa en fysisk kopia av kortet, eftersom kortets nummer och ytterligare några uppgifter är allt som behövs för att göra köp på nätet.

Däremot måste bedragaren alltid komma över uppgifterna på något sätt. Det finns två huvudsakliga metoder för att göra detta: Genom att läsa av kortets magnetremsa i smyg vilket är mer känt som skimming. Eller genom att komma över en större databas med kortnummer från till exempel en e-handlare.

7.3 Skimming, den gamla tidens kortbedrägeri

Du har säkerligen hört talas om skimming. Det är vad det kallas när kriminella monterar utrustning på bankomater som kopierar kortnummer från alla kort som passerar. Sådana maskiner är både billiga och enkla att använda. När de har suttit uppe någon dag är de fulla med kopierade kortuppgifter. Då kan personen som satte upp den återvända, ta med sig den och i lugn och ro föra över bytet till en dator, ungefär på samma sätt som man flyttar filer från ett usb-minne.

Därefter kan kortnumren antingen läggas in på tomma kort, användas för köp på nätet eller säljas vidare. Oavsett så slutar det ofta med att någon tar ut pengar eller köper varor – och pengarna dras från ditt konto.

De mer avancerade nöjer sig inte med kortnummer utan snappar även upp din pinkod, tack vare en liten kamera som monteras i bankomatens ovansida. Och det är inte

bara vanliga bankomater som blir skimmade. Samma knep har använts på så väl bensinstationer som i biljettautomater.

Ofta är skimmingutrustningen diskret utformad för att se ut som en del av bankomaten, men den kan genomskådas. Eftersom den är tillfälligt monterad kan den sitta löst. Om det ser misstänkt ut finns det alltså ett enkelt knep att ta till: Försöka dra lite i plaststycket som sitter kring springan för kortet. Om det skulle vara bedragarens utrustning som sitter där så lär det lossna utan större ansträngning.

Skimmingen bygger alltså helt på kortets magnetremsa, den svarta linjen som syns på baksidan. Moderna, svenska kort har också säkerhetschip. Det är den guld- eller silverfärgade lilla fyrkanten du ser på kortets ovansida. Bankerna och kortföretagen talar ofta om hur mycket säkrare chipen är. Det stämmer, men är inte hela bilden. Eftersom magnetremsan finns kvar så är det fortfarande fullt möjligt att kopiera den. Orsaken till detta är att inte alla kortterminaler har stöd för köp med chipet än.

7.4 Den hackade e-handlaren

En ytterligare orsak till att skimmingen har gått ner är att den är relativt ineffektiv. Även om skimmingutrustningen sitter monterad vid en bankomat som många använder rör det sig sällan om mer än några hundra kortnummer som fångas upp under en dag.

Det finns betydligt större samlingar med kontokortsuppgifter än så, till exempel hos webbutiker som tar emot kontokortsbetalningar. Många av dem anlitar speciella fö-

Tips!

Slipp bli skimmad

- Kontrollera springan på bankomaten eller kortläsaren innan du stoppar in ditt kort.
- Se efter om det sitter någonting som liknar en kamera ovanför knappsatsen där du skriver in din kod.
- Håll handen över knappsatsen när du skriver in pin-koden.

Tack vare tekniska åtgärder har skimmingen gått ner dramatiskt i Sverige. Men på andra håll i världen är den fortfarande utbredd, så tänk extra på hur du hanterar ditt kort när du är ute och reser. Kom ihåg att kortföretagens nätverk sträcker sig över hela världen. Ett svenskt kort är lika intressant för en korttjuv i Thailand som i Östersund.

retag som sköter kontokortsbetalningarna, men det betyder inte att uppgifterna inte sparas någonstans.

Om ett sådant företag blir hackat finns risken att kontokortsnummer läcker, och det kan röra sig om gigantiska mängder. Till exempel drabbades det amerikanska storföretaget TJX, som driver detaljhandelskedjor med tusentals butiker runt om i världen, av ett intrång där inte mindre än 90 miljoner kontokortsnummer kom på vift.

Som enskild kund är det svårt att skydda sig mot sådana kortstölder, eftersom det är företagets säkerhet som brister och lämnar öppet för en hackare att komma över uppgifterna. Istället handlar det om att tänka efter både en och två gånger innan man plockar upp sitt kort och knappar in numret på en e-handelsbutik.

7.5 Betaltjänster – en (lite) tryggare mellanhand

Som vi redan har nämnt lägger många e-handlare helt enkelt ut hanteringen av kontokort på specialiserade företag. Orsaken är att detta kräver it-säkerhet som många vanliga butiker inte klarar av att upprätthålla.

Du har säkert själv märkt av det när du har shoppat på nätet. Efter att beställningen är lagd och det är dags att betala ändras webbadressen från butikens egen till betalningsförmedlarens, även om e-handlarens logotyp ofta följer med längst upp på sidan.

I praktiken innebär detta att butiken aldrig ser ditt kortnummer. Företaget du handlar från får bara ett meddelande om att betalningen är godkänd och skickar varan till dig. Två exempel på sådana företag är Payex och Dibs. Det finns också företag som hjälper privatpersoner att ta emot kortbetalningar. Det kanske mest kända är amerikanska Paypal, som också används av vissa småföretag.

I princip är detta positivt, eftersom specialiserade betalningsföretag har större resurser för att säkra sina system. Det gör det också lättare att handla från mer okända butiker och ändå känna sig trygg.

7.6 Men jag får väl tillbaka pengarna?

Bankerna har genom åren varit ganska generösa med att ersätta kunder som har drabbats av elektroniska bedrägerier. Ofta kommer ersättningen efter att banken på egen hand har upptäckt vad som håller på att hända och betalar tillbaka samma summa som har dragits från kontot.

Det har gällt både vid stölder från ett kontokort och efter intrång mot en internetbank.

Men på senare år har bankerna börjat ställa högre krav på att man ska hålla ord-

ning på sitt kort och sina koder. Vid vissa typer av bedrägerier bedömer de nämligen att kunden har varit så slarvig att hen mer eller mindre får skylla sig själv.

Ett exempel är bedrägerier via Facebook eller chattprogram. Genom att ta över en av dina vänners konton utger bedragaren sig för att vara din vän. När bedragaren har fått ditt förtroende får du höra att hen försöker betala räkningar men har tappat bort sin säkerhetsdosa. Därför får du frågan om du kan hjälpa till genom att knappa fram engångskoder och skriva in dem i chatten. Bedragaren tar emot dem, loggar in på ditt konto och plockar ut pengarna.

Den som vet hur säkerhetsdosorna fungerar skulle reagera direkt. Koderna är personliga och det är omöjligt att "låna ut" koder till någon annan. Men inte desto mindre har denna bedrägerityp lyckats många gånger, med tömda konton som resultat.

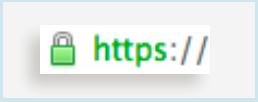
I sådana fall har svenska banker varit ovilliga att betala ut ersättning. Går man på en sådan bluff har man helt enkelt varit försumlig och får ta hela smällen själv.

Andra orsaker kan vara att man har dröjt för länge med att anmäla ett stulet kort eller en försvunnen säkerhetsdosa. Det fick en kvinna i Linköping erfara. År 2011 bröt sig någon in i hennes hem medan hon var

Checklista!

Ska du använda kortet?

→ Är anslutningen säker? Använd aldrig ditt kort på en sajt som inte har en krypterad anslutning. Du känner igen dem genom att adressen börjar med "https://" istället för "http://", där bokstaven s står för – just det – "secure". På sådana sajter visas också ett hänglås bredvid adressen.



→ Är hänglåset rött, eller fick du en varning? Då kan sajten du besöker vara en fejkad variant. Undvik den, och skriv absolut inte in ditt kortnummer!

→ Men hänglåset är bara en garant för att kortnumret skickas till handlaren på ett säkert sätt, inte för att det hanteras säkert därefter. Egentligen är det svårt att som kund påverka det, men en tumregel är att bara använda kortet på butiker som är välkända och respekterade.

Viktigt!

Dosan som säkrar dina kortköp

- På senare tid har det blivit vanligare att kortköp på nätet måste verifieras med samma säkerhetsdosa som man använder för att logga in på internetbanken.
- För att köpet ska gå igenom måste man generera en engångskod, oftast med knappen på dosan som är märkt "buy". Syftet är att säkerställa att det är kortets verkliga ägare som använder det.
- Systemet kallas Verified by Visa eller Secure Code när korten kommer från Mastercard.
- Det kan ge sken av att köpet är säkrare för dig, men det är en illusion. Det enda systemet gör är att förhindra en bedragare att använda ett stulet kort på just denna butik. Det gör ingenting för att hindra ditt kortnummer från att läcka ut.
- Dessutom används systemet inte överallt, och på alla dessa platser är det fritt fram att använda en kopia av ditt kort.
- Med andra ord är dosan till för att skydda butiken, eftersom den slipper skicka varor till bedragare. Men det gör inte dig som kund säkrare.

bortrest över helgen. En granne upptäckte vad som hade hänt och kontaktade kvinnan som polisanmälde händelsen via telefon. Eftersom hon hade alla sina kontokort med sig på resan tänkte hon inte mer på dem – men glömde att säkerhetsdosan till internetbanken låg kvar hemma. Det gjorde även pappret där hennes kod fanns nedtecknad. Först när hon återvände upptäckte hon vad som hade hänt. Dosan och koden var båda stulna, och flera hundra tusen kronor hade plockats ut från kontot, pengar som banken inte ville betala tillbaka eftersom anmälan inkom flera dagar efter att de försvann.

Rådet är alltså: Lämna aldrig ifrån dig kortnummer eller koder om du inte är säker på vem mottagaren är, och anmäl försvunna kort och dosor så snabbt du bara kan.

08 Mobilen – nästa säkerhetsarena

För många är it-säkerhetstänk synonymt med datorn på jobbet eller hemma. Att antivirus på datorn är en bra idé, det vet de allra flesta, likaså att man bör vara noga med att installera säkerhetsuppdateringar från Microsoft (om du kör Windows) och Apple (om du kör Mac). Men idag är det långt ifrån hela sanningen. För det är inte längre datorerna på jobbet och i hemmet som är våra huvudsakliga kontaktpunkter med nätet – utan mobiltelefonerna i våra fickor.

Världen över såldes 1,75 miljarder mobiltelefoner år 2012, enligt siffror från analysföretaget Gartner. Det är nästan fem gånger så många som den totala försäljningen av pc-datorer under samma år. I Sverige var mer än 70 procent av alla mobiltelefoner som såldes det året så kallade smarta telefoner, det vill säga telefoner som kan användas till betydligt mer än bara ringa med: Surfa på nätet, skicka e-post och göra bankärenden, till exempel.

Med det i åtanke är det inte så konstigt att de som är intresserade av att komma över känslig information i allt högre grad vänt sin uppmärksamhet mot telefonerna i våra händer. Kort sagt: För den som vill skydda sig från angripare är det idag minst lika viktigt att hålla koll på sin mobiltelefon som på datorn i hemmet eller på jobbet.

8.1 Så ser hoten ut

I grunden är metoderna som används för att komma över känslig information i en mobiltelefon, eller ta kontroll över den, de samma som i datorvärlden. Trojaner och andra former av skadlig kod är sedan ett par år tillbaka vanligt förekommande även i mobilvärlden. Däremot sprider angriparna sina verktyg på ett lite annorlunda vis. Dessutom är programmens funktioner ofta unikt anpassade för just mobiltelefoner.

I särklass vanligast är att skadlig kod sprids via mobiltelefonens programbutik (Google Play för dig som använder en

Androidtelefon, App Store för dig som kör Iphone). Precis som med trojaner för datorer handlar det om att skadliga program "göms" i andra, till synes helt ofarliga applikationer. I fjol upptäcktes till exempel att Iphone-appen "Find and call" i själva verket var en listigt maskerad trojan. Den kopierade de telefonnummer som fanns lagrade i användarnas telefoner och började sen skicka ut mängder med oönskad SMS-reklam till dem. Samma år upptäcktes flera fall av trojaner insmugna i Android-appar. Alla var utformade för samma syfte: När de väl hade installerats började de automatiskt skicka ut sms till dyra betalnummer, kontrollerade av angriparen. Användaren märkte ingenting förrän nästa telefonräkning landade i brevlådan. Då hade trojanens skapare redan haft god tid på sig att plocka ut de insamlade pengarna.

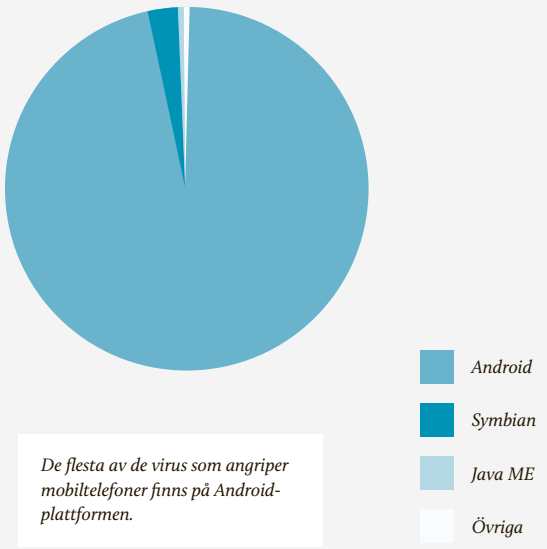
Det finns andra, betydligt mer oroväckande exempel. I vintras avslöjades hur en trojan utformad för Androidtelefoner användes för att stjäla mer än 300 000 kronor från sammanlagt 30 000 bankkunder i Spanien, Italien och Tyskland. Trojanen smögs in på telefonerna via SMS från angriparen, som innehöll en länk till en påstådd säkerhetsuppdatering. Väl på plats tog den kontroll över det SMS-baserade

Viktigt!

Lösenordsskydda din mobil!

Det är lätt att glömma hur mycket intressant information som finns att hämta i din mobiltelefon. De flesta av oss använder dem både som kalender, för att skicka e-post och för sociala nätverk som Facebook och Twitter. I adressboken finns dessutom namn, telefonnummer och kanske ännu mer information om dina arbetskamrater, vänner och bekanta. En angripare som får tag på din mobiltelefon kan alltså komma åt både din mejlkorg, din kalender och din korrespondens med alla du känner.

För att förhindra det är det första du bör göra att lösenordsskydda din mobiltelefon. En fyrsiffrig kod räcker i de allra flesta fall gott och väl. Även om den inte på något vis är oknäckbar så ger den dig åtminstone tid att ändra alla relevanta lösenord (till exempel till ditt e-postkonto) om telefonen hamnar i orätta händer, och innan angriparen tagit sig in i den.



De flesta av de virus som angriper mobiltelefoner finns på Android-plattformen.

inloggningssystem som bankerna använde sig av. På så vis kunde stora summor pengar smygas ut från kontona utan att telefonernas ägare märkte någonting.

8.2 Olika plattformar, olika risker

Två faktorer avgör vilken mobilplattform som blir mest utsatt för skadlig kod och andra säkerhetsrisker. Den första är antalet användare, den andra rör operativsystemens inbyggda säkerhetsmekanismer. I datorvärlden har Windows länge varit mer utsatt för skadlig kod än andra, konkurrerande operativsystem. Det beror dels på att den absoluta majoriteten av alla persondatorer i världen kör just Windows, dels på att där finns många potentiella sårbarheter och säkerhetshål för en angripare att utnyttja.

Enligt McAfee, ett av många säkerhetsföretag som följer utvecklingen av trojaner och virus, var 97 procent av all skadlig kod för mobiltelefoner som upptäcktes under 2012 skapad för operativsystemet Android. Ett par enstaka procent var för den äldre plattformen Symbian, som bland annat används i Nokias äldre telefonmodeller. Bara en bråkdel av den skadliga koden som upptäcktes var utvecklad för övriga operativsystem, som IOS och Windows Phone.

Men oavsett vilken plattform du använder är det klart att hoten blir allt fler. Faktum är att mängden skadlig kod som utvecklas för smarta telefoner formligen exploderat den senaste tiden. År 2011 upptäckte McAfee 792 former av skadlig kod utvecklad för mobiler. I början av 2013 hade siffran växt till över 36 000, en fyrtiofaldig ökning under bara drygt tolv månader.

8.3 Så skyddar du dig

UPPDATERA, UPPDATERA, UPPDATERA

Alla de stora mobiltillverkarna trycker regelbundet ut uppdateringar till sina operativsystem. För att hålla din telefon säker är det viktigt att du hänger med och installerar dem så fort de blir tillgängliga. Förutom att lägga till nya funktioner så täpper de nämligen till nyupptäckta säkerhetshål. Till exempel så stängde en uppdatering från Apple i december 2012 ett hål som utnyttjades av SMS-trojaner likt den som finns beskriven ovan. Den som installerade uppdateringen blev med andra ord immun mot den. De som inte gjorde det fortsatte vara potentiella offer för angriparen.

Att installera säkerhetsuppdateringar är i de allra flesta fall mycket enkelt. Android, IOS och Windows Phone har alla stöd för så kallade "over the air"-uppdateringar, vilket innebär att hela processen sköts över telefonnätet. Din telefon påminner dig när en ny uppdatering finns tillgänglig, allt du behöver göra är att godkänna installationen och sen vänta på att telefonen gör jobbet. Äldre modeller kan i vissa fall behöva anslutas till en dator – mer information om detta hittar du på din mobiltillverkares webbsida eller i de medföljande instruktionsböckerna.

Tänk efter före när du installerar nya appar på mobilen.

HÅLL KOLL PÅ DINA APPAR

De allra flesta trojaner smygs in i mobiltelefonen via programbutiker som Google Play och App Store. För att hålla dig säker gäller det alltså att vara noga med vad du installerar. Välj i första hand appar från utvecklare som du känner dig trygg med, och läs gärna omdömen på nätet innan du installerar (en snabb googling räcker ofta för att upptäcka om någonting är lurt med programmet du vill installera). De flesta mobiloperativsystem låter dig även granska i detalj vilken information på te-

Viktigt!

”Jag kör Iphone, alltså är jag säker”

Apples telefoner och surfplattor är betydligt mindre drabbade av skadlig kod och kända säkerhetsluckor än andra. Merparten av alla virus som upptäcks för mobiltelefoner riktar istället in sig på Googles operativsystem Android. Det beror dels på att Apples regler för vilken sorts appar som får säljas är betydligt strängare, dels på att den inbyggda säkerheten i en Iphone vanligtvis är högre än i en motsvarande Androidtelefon.

Men det betyder inte att man som Iphone-ägare kan känna sig helt säker. Appen “Find and call”, som finns beskriven ovan, är en av flera skadliga trojaner som upptäckts för Apples operativsystem på sistone. Siffror från det amerikanska myndigheten “department of homeland security” uppskattade år 2012 att 0,7 procent av all skadlig kod för mobiltelefoner var skriven specifikt för Apples Iphone. Det är en låg siffra, men de flesta bedömare är överens om att den kommer öka med tiden, i takt med att antalet Iphone-användare växer och skickliga angripare lär sig utnyttja nya svagheter i Apples operativsystem.

lefonen som specifika appar använder sig av. Ibland är dessa fullt rimliga – exempelvis är det naturligt att en kameraapplikation behöver tillgång till telefonens kamerafunktioner. Men om till exempel ett enkelt spel ber om fullständig tillgång till din adressbok kan det vara anledning att bli misstänksam.

När du laddar ned en app till en Androidtelefon eller en Iphone visas en lista på dessa krav innan du godkänner installationen. Vill du vara på den säkra sidan så läs igenom listan och fundera en gång extra om någonting ser märkligt ut. Du kan även granska olika appars rättigheter vid ett senare tillfälle under telefonens inställningar.

ANTIVIRUS FÖR MOBILEN

De flesta stora antivirusföretag erbjuder sedan en tid tillbaka programvara även för mobiltelefoner. Hur intressanta dessa är för hemanvändaren kan diskuteras. I grunden handlar det om ett slags filter, som genomsöker dina installerade appar i jakt på skadlig kod och varnar om du försöker ladda ned och installera en suspekt applikation. Den som är noga med att bara installera pålitliga program klarar sig långt utan särskild mjukvara för just det (se ovan).

Däremot finns andra funktioner i programmen som kan vara nog så använd-

bara, exempelvis automatisk säkerhetskopiering av data och möjligheten att låsa borttappade telefoner så att de inte kan användas – en sista utväg för att förhindra att känslig data hamnar i orätta händer.

EN MOBIL FÖR JOBBET, EN FÖR HEMMET

Har du småbarn hemma, eller vänner som gärna leker med din mobiltelefon när de är på besök, så vet du hur svårt det kan vara att hålla koll på exakt vad som händer med den. Har du mycket känslig information på din telefon kan det därför vara en idé att helt enkelt skaffa en till, som du använder för fritidssysslor. Det kan låta gammaldags, men är också ett smart sätt att särskilja känsliga uppgifter från sådant du inte bryr dig lika mycket om. Använd din privata mobil eller surfplatta för att spela spel och testa nya appar, jobbtelefonen för att ordna med viktiga mejl och sköta bankaffärer. Genom att aldrig installera fler appar än nödvändigt och vara noga med vad du klickar på för länkar så minimerar du riskerna att informationen hamnar i fel händer. Din privata mobil kan du vara mindre försiktig med – även om den smittas av ett virus kommer ju angriparen inte över någonting av värde.

09 Att radera på riktigt

På din dators skrivbord ligger en fil med känsligt innehåll. Kanske ett Word-dokument, kanske ett fotografi som du inte vill ska hamna i orätta händer. Genom att dra den till papperskorgen försvinner den för evigt. Eller?

Inte alls. Faktum är att det är betydligt mer omständigt än många tror att bli av med information som finns lagrad i din dator. Att kasta en fil i papperskorgen innebär inte att den försvinner. Snarare att den – precis som med en riktig papperskorg – knycklas ihop och förpassas till soporna. Precis som i verkligheten kan en angripare som kommer över din dator enkelt öppna soppåsen och rota rätt på det som finns i den.

Du kanske har gjort det till en vana att tömma datorns papperskorg? Men inte heller då försvinner filen på riktigt. För att verkligen bli av med informationen måste du ta till den digitala motsvarigheten till en dokumentförstörare.

Lyckligtvis finns det sätt att försäkra dig om att information du tagit bort från datorn verkligen är försvunnen. I det här kapitlet går vi igenom hur en hårddisk fungerar, och berättar hur du raderar på riktigt.

9.1 Enkelt återskapa borttagna filer

När du sparar någonting på din dator händer, något förenklat, två saker. För det första skrivs själva informationen till hårddisken, det vill säga alla de ettor och nollor som tillsammans utgör exempelvis textdokumentet, bildfilen eller ljudklippet i fråga. För det andra noterar datorn var någonstans på hårddisken filen befinner sig. Processen kan liknas vid att skriva ned det hela i ett slags kartotek, som hjälper datorn att hålla reda på vilken information som finns lagrad var. Utan dess hjälp vet inte datorn var en fil börjar och nästa tar vid på hårddisken – allt blandas ihop i ett obegripligt gytter av information.

När du tar bort en fil på din Mac– eller Windowsdator genom att slänga den i papperskorgen så raderas alltså inte själva informationen från din hårddisk. Istället är det noteringen om var just den filen befinner sig som tas bort. Informationen finns kvar, men kan sägas vara bortglömd. Din dator kommer att betrakta utrymmet som ledigt, och kan skriva över det med ny information vid behov.

Men med hjälp av specialprogram och särskild utrustning är det en lätt match att återskapa informationen. Sådana tjänster erbjuds idag av en mängd företag, specialiserade på att hjälpa företag och myndigheter att återskapa förlorad data. Någon med fysisk tillgång till din dator kan alltså i många fall återskapa även filer som du trodde var försvunna. Samma sak gäller för mobiltelefoner, surfplattor och andra prylar med inbyggda, elektroniska minnen.

9.2 Så sopar du undan spåren

Det är, i de allra flesta fall, enkelt att rensa din hårddisk på riktigt. På Mac-datorer finns funktionen till och med inbyggd i operativsystemet. Istället för att välja alternativet "Töm papperskorgen" i rullgardinsmenyn nästa gång du vill göra just det, flytta muspekaren ett steg nedåt och klicka på "Säker papperskorgstömning".

Tips!

Dataräddning kan vara en livlina

Samma specialistföretag som kan återskapa hemligheter du trodde var borttagna, kan också hjälp dig ur kniviga situationer. Om hårddisken i din dator gått sönder kan precis samma metoder användas för att rädda informationen som fanns lagrad på den.

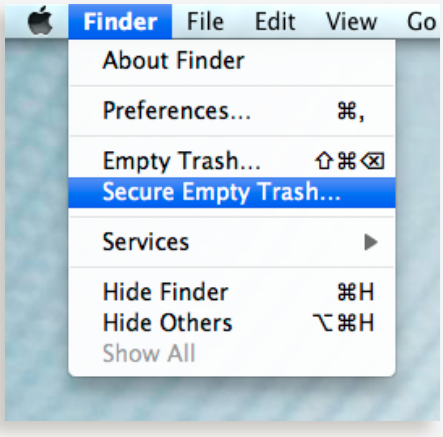
I Sverige finns flera dataräddningsföretag specialiserade på att hjälpa både privatpersoner och företag ur just sådana situationer. Ett av de äldsta heter Ibas och har sitt huvudkontor i Uppsala.

Ibas säger sig lyckas återskapa informationen på i genomsnitt hälften av alla hårddiskar av ssd-typ (hårddiskar utan rörliga delar, som används framförallt i nyare bärbara datorer, i mobiltelefoner och i surfplattor) som lämnas in för reparation. Motsvarande siffra för mekaniska hårddiskar av traditionell typ ligger på över 90 procent.

Då tar din dator inte bara bort filerna, utan skriver över platserna där de fanns lagrade med ny, slumpmässigt utvald information. Den som försöker återskapa filerna kommer alltså bara att hitta en obegriplig massa av utvalda ettor och nollor, istället för informationen du tagit bort.

Om du raderar stora filer på detta säkra sätt kommer du märka att det tar tid. Det beror på att datorn måste arbeta en hel del för att verkligen skriva över det du vill ta bort.

Kör du en Windowsdator behövs lite mer handpåläggning. På nätet finns flera gratisprogram som gör allt det Mac:ens inbyggda funktioner klarar av, plus lite till (se faktaruta nedan). Förutom att säkert radera enstaka filer låter vissa program dig schemalägga papperskorgstömningar, eller ställa in programmet för att automatiskt rensa en viss katalog från innehåll vid angiven tidpunkt.



Välj säker radering om du vill undvika att någon ska kunna återskapa filer du slängt.

9.3 Stulna telefoner – en guldgruva för tjuven

Många lagrar inte längre sin viktigaste information på datorn i hemmet utan i mobiltelefonen i fickan. Därför är det viktigt att ha en plan för om någonting går snett. Om exempelvis din mobiltelefon blir stulen, hur ser du till att tjuven inte kommer över känsliga bilder eller dokument som fanns lagrade på den?

Vintern 2013 genomförde tidningen Computer Sweden ett intressant experiment. Redaktionen överlämnade 50 begagnade mobiltelefoner till säkerhetsföretaget Bitsec för att se vilken information som kunde hämtas ur dem.

Resultaten var slående. Trots att samtliga telefoner var fabriksåterställda, det vill

säga tömda på filer och användarkonton, så lyckades Bitsec plocka fram fullt läsbar information ur 39 av dem. På 16 av telefonerna hittades information som kan klassas som känslig, bland annat privata mejladresser, kundlistor från företag, privata fotografier, bankdokument och bilder på pass.

Säkerhetsföretaget behövde inte ens anstränga sig särskilt mycket för att komma över informationen. De begagnade telefonerna kopplades in till en helt vanlig dator, och enbart program som finns fritt tillgängliga på nätet användes för att snoka upp informationen.

9.4 Så tömmer du din mobiltelefon

Liknande metoder som för att radera information ordentligt på en dator kan användas även för mobiltelefoner. Dock är tillvägagångssättet något annorlunda, och i vissa fall mer komplicerat.

Enklast är det för dig som kör en produkt från Apple som har Ios, det operativsystem som driver Iphone och Ipad. Precis som på Mac-datorer kommer de nämligen med inbyggda och väl fungerande funktioner för att tömma minnet utan spår av det som funnits där tidigare.

Den funktion du letar efter heter "Radera allt innehåll och inställningar". Ny-

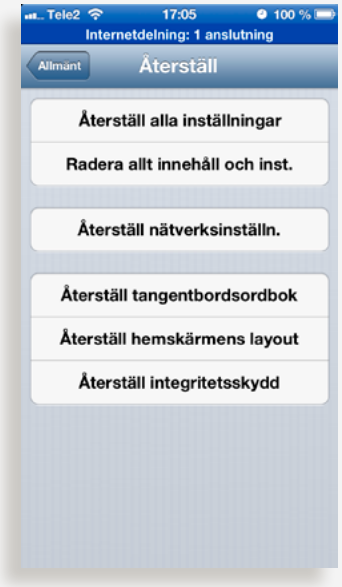
Tips!

Två Windowsprogram som gör jobbet

Killdisk är ett populärt gratisprogram för Windows som kan användas för att snabbt och enkelt tömma en hårddisk, ett USB-minne eller till och med en diskett på information. Killdisk är perfekt om du ska sälja eller slänga bort en dator, och vill vara säker på att ingen känslig information finns kvar. Programmet kan dock inte användas för att ta bort enskilda filer. Kan laddas ned från www.killdisk.com

DP Wiper är ett annat program som används för att ta bort enskilda filer. Det erbjuder flera säkerhetsnivåer, från "normal" till "paranoid", som tar olika lång tid att genomföra. Kan laddas ned från dp-wiper.softpedia.com

Både Killdisk och DP Wiper är testade av Microsoft, och rekommenderas av företaget som tilläggsprogram till Windows för den som vill radera filer på ett säkert vis.



På en Iphone kan du enkelt radera allt innehåll vid exempelvis andrahandsförsäljning.

are Apple-modeller har alla inbyggt stöd för hårdvarukryptering (läs mer om detta i kapitel 6, "E-post är som vykort"). När du aktiverar funktionen raderar operativsystemet helt enkelt den nyckel som behövs för att låsa upp innehållet i telefonen. Kvar blir bara en obegriplig massa av slumpvis utvalda siffror, helt omöjliga för en angripare att utläsa någonting av värde ur.

Kör du en Androidtelefon är tillvägagångssättet något knepigare. Vissa, men inte alla, telefoner och surfplattor som kör Googles operativsystem har stöd för hårdvarukryptering. På dem går det att utföra lika säker radering som på Apples enheter.

På telefoner som inte har stöd för tekniken går det visserligen att tömma telefonens minne genom en fabriksåterställning, men risken är stor att informationen ändå går att återskapa. Alla de telefoner som undersöktes i tidningen Computer Swedens experiment var fabriksåterställda, ändå kunde borttagen information hämtas ur dem.

Om din telefon eller surfplatta inte har stöd för hårdvarukryptering kan du istället använda en app för att göra jobbet. Ett populärt val för just Android är appen Advanced File Shredder, som du hittar genom att söka i telefonens eller surfplattans programbutik. Den låter dig radera och sen skriva över allt innehåll på telefonen med slumpmässigt utvald information. Rent tekniskt fungerar det precis som motsvarande program gör på Windowsdatorer, och funktionen "säker papperskorgstömning" på Macdatorer. Också resultatet är det samma: Efter att Advanced File Shredder gjort sitt jobb är det mycket svårt för en angripare att komma över det som ursprungligen fanns lagrat på telefonen.

Telefoner med äldre operativsystem, till exempel Symbian som körs på många av Nokias och Sony Ericssons äldre modeller, har som regel betydligt sämre funktioner för att radera data säkert.

Av de 50 telefoner som Bitsec undersökte på uppdrag av Computer Sweden var sådana med Android eller Symbian som operativsystem enklast att återskapa data på. Säkerhetsföretaget lyckades inte återskapa raderad data på någon av de fyra Iphone-telefoner som undersöktes.

9.5 Töm telefonen på avstånd

Både IOS (Iphone och Ipad) och Android har stöd för vad som på tekniskspråk brukar kallas för "remote wipe". Det innebär att du kan radera all data i en telefon på avstånd, genom att logga in på ditt Google- eller Applekonto över webben.

På IOS-enheter når du funktionen via Icloud, som är namnet på Apples molntjänst. Hos Google heter motsvarande funktion Google Sync, och måste manuellt aktiveras på din telefon.

Remote wipe är en oumbärlig funktion om din telefon till exempel blivit stulen, och du vill försäkra dig om att tjuven inte kommer åt känslig information. Men kom ihåg att raderingen aldrig blir säkrare än om du genomfört den med telefonen i handen. En skicklig angripare kan lika lätt återskapa information på en Androidtelefon som tömts på data via Google Sync, som på en som fabriksåterställts på mer traditionell väg.

På de flesta mobiltelefoner finns inbyggda verktyg. Funktionen du söker kallas van-

Viktigt!

Innan du säljer, formatera!

Oavsett vilken telefon eller dator du har, kom ihåg att tömma den på information innan en eventuell försäljning!

På en dator gör du det enklast genom att plocka fram skivan med operativsystemet (oftast Windows eller Mac OS) som följde med när du köpte datorn. Med hjälp av skivan kan du påbörja en ny, ren installation. På vägen kommer du få frågor om du vill göra en "snabbformatering" eller om du vill använda ett säkrare alternativ som skriver över innehållet på hårddisken. Välj det senare, men var beredd på att det kommer ta längre tid, precis som det tar längre tid att tömma papperskorgen säkert än på det vanliga sättet.

ligen för "fabriksåterställning". Det innebär att telefonen återställs i det läge den var när du slog på den för första gången: Alla installerade appar tas bort, alla mejlkonton raderas och telefonboken töms på information.

Som vi beskriver i det här kapitlet är det, åtminstone i vissa fall, fortfarande möjligt för en tekniskt kunnig angripare att återskapa informationen du haft lagrad i datorn eller telefonen. Men du har åtminstone gjort det så svårt som möjligt för köparen att komma åt bilder, chattkonversationer och annat som du ogärna vill ska hamna i fel händer.

Varning!
Ingen återvändo

Att slänga dokument i papperskorgen på en Mac- eller Windowsdator är lätt att ångra. Ett knapptryck är allt som behövs för att återställa filen till sin ursprungliga plats på hårddisken. Men att säkert radera filer med hjälp av de metoder som finns beskrivna i det här kapitlet innebär, i de allra flesta fall, att informationen går förlorad för alltid.

Var noga med att gå igenom informationen som finns lagrad på din telefon eller din dator innan du genomför en säker radering. Glöm inte att kopiera värdefulla dokument du vill ha kvar till en annan dator eller telefon, eller skapa en fullständig säkerhetskopia som du förvarar på en säker plats.

Se även till att mobiltelefonens adressbok finns sparad på annat håll. Både på Android- och IOS-telefoner är det enkelt att säkerhetskopiera informationen till din dator eller ditt Apple- eller Googlekonto på nätet.

10 Ställ krav!

Vissa delar av den här guiden har handlat om att skydda sin egen dator mot angrepp. Men i takt med att vi lägger ut allt mer av vår information på nätet – i "molnet" som man ibland säger – blir det viktigare att även ställa krav på företagen vi anlitar.

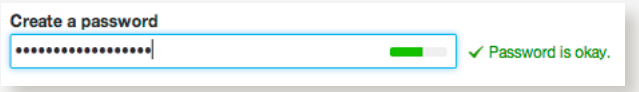
Kanske har du redan ett konto på till exempel lagringstjänsten Dropbox för säkerhetskopiering av filer. Din e-post ligger med största sannolikhet redan ute hos ett företag. För att inte tala om webbaserade kalendrar och ordbehandlingsprogram som Google Docs (numera kallad Google Drive) eller Microsofts Office 365.

Många av dessa tjänster är gratis, men inte desto mindre tjänar företagen pengar på att vi använder dem, till exempel genom att visa reklam. Därför är det inte mer än rätt att ställa frågor om hur de har det med säkerheten. Nöj dig inte med flummiga löften om "säkra servrar" – sådant kan alla säga utan att det betyder någonting i praktiken. Begär konkreta svar på vilka säkerhetsmekanismer de använder!

Troligtvis kommer du inte att få svar om du mejlar till något av de större företagen, men försök läsa på deras webbplats och se om de svarar på nedanstående frågor där.

10.1 Hur lagras mitt lösenord?

- Kommer lösenordet jag väljer att ligga krypterat eller i klartext (som okrypterad text kallas)?
- Ställer företaget krav på att jag väljer ett starkt lösenord? Många erbjuder en slags mätare som varnar för dåliga lösenord medan man skriver dem. De är dels en god hjälp för dig, men också ett tecken på att företaget tar säkerhet på allvar.
- Om det krypteras (eller "hashas" för att använda den korrekta termen) – med vilken metod? Om företaget lovar "saltad hash" så betyder det kryptering som har gjorts extra svår att knäcka. Mer än så är svårt att begära.



Använd alltid ett starkt lösenord om du vill vara på den säkra sidan.

→ Testa själv. De flesta sajter har en knapp för den som har glömt sitt lösenord. Om du klickar på den och fyller i din e-postadress, vad dyker upp? Om lösenordet du valde står utskrivet så saknas kryptering helt. Om det är ordentligt krypterat så ska inte ens företaget kunna få fram ditt lösenord, vilket mejlet bevisar att de kan. Om du däremot får ett mejl som innehåller en länk till sida där du kan välja ett nytt lösenord är systemet troligtvis byggt på rätt sätt.

10.2 Hur lagras mina filer?

→ Att lägga ut sina filer till ett företag är praktiskt. Även om din egen hårddisk går sönder kan du räkna med att få tillbaka semesterbilderna. Men det är viktigt att kunna lita på att företaget håller dem skyddade.

→ Ställ frågor om kryptering, och om vem som får ta del av filernas innehåll.

→ Används innehållet till exempel för att bygga en profil av dina intressen för att senare kunna rikta reklam därefter? Sådant ska den som tillhandahåller tjänsten kunna svara på.

→ Om du inte får de svar du vill ha men inte vill eller kan byta tjänst så kan du alltid kryptera den känsligaste informationen själv, redan innan den laddas upp. Tipsen om hur du innesluter filer i en krypterad "låda" (se kapitel 6, "E-post är som vykort") kan appliceras även på lagringstjänster på nätet.

10.3 Vad händer med min information?

Att samla information om användare och använda den för att rikta reklam till "rätt" personer är en jätteindustri på nätet idag. Bland andra Google och Facebook bygger hela sin verksamhet, som omsätter miljarder, på detta. Ibland kallas detta att de "säljer användarnas information" till annonsörer. Men det är en överdrift. Snarare säljer de möjligheten att nå just dig. För att lyckas med det måste deras kartläggning vara så detaljerad som möjligt. Ställ frågor om hur de skapar den.

- Vilken information kommer att användas för att rikta reklam? Om tjänsten är gratis kan du utgår från att det är allt du lämnar ifrån dig, inklusive innehållet i dina mejl och privata meddelanden.
- Äger jag fortfarande informationen? Hur konstigt det än låter kan en lagringstjänst faktiskt anse att det är de – inte du – som äger information du har laddat upp. Kontrollera villkoren för att säkerställa att du inte ger bort din information.
- Vem får tillgång till min e-postadress? Det är inte ovanligt att bli överöst med reklam i mejllådan efter att man har registrerat sig på en webbsida med sin e-postadress. Det gäller framförallt mindre, oseriösa tjänster. De seriösa ska deklarera hur adressen kommer att användas, och erbjuda möjlighet att avsluta utskick man har tröttnat på.
- I vilket land finns tjänsten? Webbtjänster är globala och kan ha användare spridda över hela världen. Men företaget har sin hemvist någonstans, och i regel är det detta lands lagar och regler som gäller. Det är alltså inte självklart att du i efterhand kan komma med klagomål baserade på svensk lag. Dessa är inte värda någonting om företaget är baserat i till exempel Kalifornien.

II Ordlista

Säkerhetsvärlden är full av svårtolkade förkortningar, knepiga begrepp och teknisk jargong. Det kan göra det svårt för en icke-insatt att hänga med i svängarna och förstå innebörden av det som sägs.

Nedan följer en lista över vanligt förekommande facktermer. Använd den gärna för att slå upp någonting du inte förstår!

1337
Omskrivning av ordet leet, i sig en kortform av elite. Används, med viss ironi, för att beskriva någonting imponerande eller respekterat.

Antivirusprogram
Mjukvara som installeras på en dator för att automatiskt skydda mot kända former av skadlig kod. Bra som grundskydd, men rår inte på mer sofistikerade intrångsförsök. De stora säkerhetsföretagen säljer antivirusprogram för både pc- och macdatorer, samt mobiltelefoner och surfplattor.

Black hat
En hackare som medvetet begår brott med hjälp av sin dator. Det kan handla om dataintrång för nöjes skull, sabotage eller kommersiell verksamhet i form av industrispionage eller utpressning. Vissa svarthattar tycks inte vara ute efter någonting annat än uppmärksamhet.

Botnät
Nätverk av datorer som infekterats med skadlig kod, till exempel en *trojan* och kan fjärrstyras. Från engelskans botnet, där bot är en förkortning av robot. Kan användas till exempel för stora utskick av *spam* eller för *överbelastningsattack*. Kallas ibland för zombienätverk.

Brute force
Metod för att knäcka krypterade lösenord. Utförs genom att ett program automatiskt testar stora mängder kombinationer av bokstäver och siffror för att hitta det rik-

tiga lösenordet. Kan riktas direkt mot systemet, men fungerar bäst om angriparen kommer över den interna lösenordsfilen där det krypterade resultatet finns lagrat. En närbesläktad variant är attacken med hjälp av en *ordlista*, som bara knäcker enklare lösenord men går betydligt snabbare.

Cracker
Hackare som sysslar med att knäcka kopieringsskyddade program och spel. Begreppet skapades för att skilja "riktiga" hackare från rörelsens mer ljusskygga element. Distinktionen är viktig för många av datorvärldens veteraner.

Dataintrång
Ett juridiskt begrepp och ett brott enligt svensk lag. Definieras i brottsbalken som: "Den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatisk behandling eller olovligen ändrar, utplånar, blockerar eller i register för in sådan uppgift". Påföljden är böter eller fängelse i upp till två år.

Defacement
Sabotage av en webbplats. Utförs genom att hackare som fått tillgång till webbservern byter ut information på en webbplats mot sitt eget budskap, inte sällan av hånfull karaktär.

Exploit
Mjukvara eller metod för att utnyttja säkerhetshål i ett system, för att till exempel ge en hackare superanvändarstatus. Exploits som utnyttjar oupptäckta säkerhetshål är särskilt åtråvärda bland hackare och kallas för zero-day exploits.

Grey hat hacker
En laglydig hackare som ibland tänjer på gränserna för vad som är tillåtet. En grey hat kan till exempel offentliggöra en stor säkerhetslucka bara för att tvinga de drabbade systemen att bättra på sin säkerhet.

Hash
Betecknar i dagligt tal ett krypterat lösenord, men betyder egentligen resultatet av en matematisk envägsfunktion som gör om ett visst värde till ett annat. Att återställa det ursprungliga värdet är mycket tidskrävande. Se även *brute force* och *ordlista*.

Ip-nummer
Unik sifferkombination som används på internet för att identifiera en dator eller ett mindre nätverk. Om en angripares riktiga ip-adress avslöjas vid ett intrång så kan polisen vända sig till en bredbandsoperatör och begära ut uppgifter om vem abonnemanget tillhör. En hackare som begår intrång gör

därför allt för att dölja detta, till exempel genom att gå via andra knäckta datorer.

It-säkerhet
Enligt Myndigheten för samhällsskydd och beredskap: "Säkerhet beträffande it-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation".

Kryptering
Konsten att göra information svårläst för de som inte ska kunna läsa den. Att göra krypterad information begriplig igen kallas för dekryptering. Lösenordsfiler och annan känslig information som lagras i datorsystem är ofta krypterad. Se även *hash*.

Logg/loggfil
En detaljerad återgivning av allt som skett på ett datorsystem under en viss tid. Till exempel så återger en loggfil från en webbserver alla anslutningar som gjorts till systemet. Även program kan ställas in för att spara loggfiler. Till exempel så sparar webbläsare ofta detaljerad information om vilka sajter som har besökts. Utredningar av dataintrångsfall börjar ofta med en grundlig analys av det drabbade systemets loggfiler.

Mask
Elakt program som sprider sig själv, till exempel via mejl, nätverk eller fickminnen. Liknar *virus*, men fungerar som fristående program medan virus infekterar program som finns på den angripna datorn. Till skillnad från en *trojan* kan en mask sprida sig vidare utan att användaren luras att köra ett skadligt program.

Ordlista/wordlist
En lista med vanligt förekommande ord som testas mot en krypterad lösenordsfil, i hopp om att hitta det ursprungliga lösenordet. Att knäcka ett lösenord med en ordlista går i regel betydligt fortare än att göra det med hjälp av en brute force-attack. Dock fungerar det bara om lösenordet är av enklare typ. Utförliga wordlists kan bestå av många miljoner ord och uttryck, bokstavs- och sifferkombinationer. Se även *brute force*.

Patch
Ett tillägg till ett program som i efterhand stänger ett nyupptäckt säkerhetshål eller lagar en bugg. Vanligt förekommande program patchas regelbundet, ofta flera år efter att de först lanserats, i takt med att nya sårbarheter och fel upptäcks. Se även *säkerhetslucka/säkerhetshål*.

Penetrationstest
Försök att bryta sig in i ett datorsystem på uppdrag av dess ägare. Syftet med ett penetrationstest är att hitta säkerhetsluckor under kontrollerade former innan mer illasinnade hackare (se *black hat*) gör det. Efter ett penetrationstest lämnar personen som utfört testet en rapport med information om hur säkerheten kan förbättras.

Phishing
Nätfiske, omskrivning av engelskans fishing. Metoder för att lura till sig känsliga uppgifter, som till exempel lösenord eller kreditkortsnummer, med hjälp av falska mejl. Målet kan vara att lura offret till att klicka på en länk eller en bifogad fil med skadlig kod, som låter angriparen ta kontroll över den drabbade datorn. Se även *social engineering* och *trojan*.

Regnbågstabell
Ett knep för att enklare knäcka komplicerade, krypterade lösenord. Angriparen använder sig av sedan tidigare röjda lösenord i kombination med matematiska knep för att göra arbetet mindre tidskrävande.

Root
Superanvändaren på ett system som kör operativsystemen Linux eller Unix. För en hackare är målet med ett intrång ofta att "få root", det vill säga fullständig tillgång till alla systemets funktioner.

Rootkit
Även kallat spökprogram. Ett program som modifierar ett datorsystem på väldigt grundläggande nivå, till exempel genom att göra förändringar i operativsystemet. Det kan i sin tur dölja annan, otillåten aktivitet i samma system.

Server
En dator i ett nätverk vars syfte primärt är att förse användare med information, eller samordna deras kommunikation. En server används ofta för att lagra filer. Till exempel är en webbserver en maskin ansluten till internet, där komponenterna som utgör en eller flera webbsajter finns lagrade.

Social engineering
Social ingenjörskonst på svenska. Metod för att komma över lösenord eller annan information genom att bluffa sig fram. En vanlig variant är att ringa upp en person inne på det företag som ska angripas och på ett trovärdigt och trevligt sätt presentera sig som tekniker som tillfälligt behöver tillgång till systemet för att laga eller underhålla det.

Spam
Även kallat skräppost. Mejl som skickas till ett stort antal, ofta flera miljoner, mer eller mindre slumpmässigt utvalda mejladresser. Spam skickas ofta i reklamsyfte, men försöker ibland lura läsaren att klicka på bifogade filer eller länkar och därmed ladda ned skadlig kod i form av till exempel en *trojan*. Se även *phishing*.

Superanvändare
Det högst uppsatta användarkontot i ett datorsystem. Superanvändaren har tillgång till alla systemets funktioner och samtliga filer som finns lagrade i det. Det till skillnad från "vanliga" användare, som ofta bara kan komma åt vissa filer, kataloger eller funktioner. Se även *root*.

Säkerhetslucka/säkerhetshål
En sårbarhet i ett program eller ett datorsystem som kan utnyttjas av en hackare för att bryta sig in i låsta delar av systemet. Säkerhetsluckor upptäckts kontinuerligt i populära program och täpps igen allt eftersom, antingen av systemets egna tekniker eller av programleverantören i form av en patch. Till exempel lagar Microsoft fortfarande nyupptäckta säkerhetsluckor i Windowsversioner som är flera år gamla. Se även *exploit*.

Trojan
Elakt program som gömmer sig inne i ett annat program. Ursprungligen kallades trojaner för trojanska hästar, efter berättelsen i den grekiska mytologin. En trojan är snarlik ett virus, men skiljer sig genom att inte ha "eget liv" och kan bara spridas när användaren öppnar filen som trojanen gömmer sig i. Kan användas för avlyssning, stöld av känsliga uppgifter ur den infekterade datorn eller för att bygga *botnät*.

White hat
Hackare som agerar lagligt och har som mål att IT-säkerheten ska förbättras. Som motsatsen till en black hat utnyttjar en white hat inte säkerhetshål han eller hon upptäcker för egen vinning utan informerar den drabbade. Vissa white hat-hackare arbetar för stora företag eller IT-säkerhetsbolag med att att upptäcka säkerhetsluckor.

Virus
Skadligt program som kan kopiera sig själv och infektera datorer. Infektionen sker i regel genom att viruset fäster sig själv vid ett annat program. Ibland används ordet för att beskriva all form av skadlig kod, men ett riktigt virus skiljer sig från både

trojaner och *maskar*. Alla datorvirus är skapade av människor. Vissa ställer till stor skada på infekterade system medan andra bara sprider sig själv vidare. På senare år har andra former av skadlig kod blivit vanligare än klassiska virus, delvis eftersom de är enklare att skriva, delvis för att de kan spridas mycket effektivt.

Äga
Att få fullständig kontroll över en dator eller ett datorsystem. Uttrycket har ingen exakt innebörd, men betyder i Linux- och Unix-sammanhang att inkräktaren blir superanvändare, se även *root*.

Överbelastningsattack
Även känt som DDoS, distributed denial of service-attack. Metod för att slå ut en tjänst eller en webbplats. Utförs oftast genom att ett stort antal datorer som har infekterats med skadlig kod, till exempel en *trojan*, på ett givet kommando börjar överösa en server med information tills den inte längre klarar av att hantera alla förfrågningar. Ett sådant nät att fjärrstyrda datorer kallas ett *botnät*. Servern börjar först fungera långsammare för att sedan försvinna helt från nätet.

12 Länkar

Fler resurser på nätet
Många av de program som finns beskrivna i den här guiden är fritt tillgängliga på nätet. Dessutom finns där mängder av information för den som vill fördjupa sig i ämnet. Nedan följer en rad nyttiga länktips.

Kryptering
I den här guiden beskriver vi huvudsakligen kryptering med hjälp av tekniken PGP, Pretty Good Privacy. På Wikipedia finns en bra introduktion till hur den fungerar:
http://en.wikipedia.org/wiki/Pretty_Good_Privacy

Mailvelope
Ett enkelt, smidigt och kostnadsfritt sätt att kryptera mejl du skickar via exempelvis Gmail eller Outlook.
http://www.mailvelope.com

Truecrypt
Ett kostnadsfritt och kraftfullt verktyg för att kryptera filer, kataloger eller hela din hårddisk. Det kan verka avskräckande till en början, men kommer med enkla steg-för-steg-anvisningar.
http://www.truecrypt.org

Tips och råd
Myndigheten för samhällsskydd och beredskap (MSB) har tagit fram råd och stöd till privatpersoner inom området informationssäkerhet.

Informationssäkerhet för privatpersoner
På MSB:s webbplats DinSäkerhet.se finns ett avsnitt om informationssäkerhet
http://www.dinsäkerhet.se/informationssakerhet

Webbutbildning i informationssäkerhet för användare
DISA är MSB:s informationssäkerhetsutbildning för användare.
http://disa.msb.se

Om MSB:s arbete med informationssäkerhet
Mer information om MSB:s uppdrag och arbete inom området informationssäkerhet.
http://www.msb.se/informationssakerhet

Bruce Schneier är en profilerad säkerhetsexpert som regelbundet uppdaterar sin blogg med nyheter, spaningar och funderingar kring it-säkerhet. Läsvärt och tankeväckande för den som vill fördjupa sig i ämnet.
http://www.schneier.com

Vill du testa hur säkert ditt lösenord är? Tjänsten "How secure is my password" låter dig göra just det. Ger dessutom en snyggt presenterad och fascinerande insikt i hur effektiva moderna knäckarverktyg faktiskt är.
http://www.howsecureismypassword.net

Lösenord som är vanligt förekommande går fortare att knäcka. Vill du vara säker på att ditt eget verkligen är unikt? Kolla då in Xato.net och listan på de 10 000 vanligast förekommande lösenorden.
https://xato.net/passwords/more-top-worst-passwords/

Antivirus
En rad företag tillhandahåller antivirusprogram, ofta som en del i ett paket som även innehåller andra säkerhetsfunktioner. Här är några av de mest kända:

Symantec
http://www.symantec.com/

F-secure
http://www.f-secure.com/

McAfee
http://www.mcafee.com/se/

Panda
http://www.pandasecurity.com/sweden/

Kaspersky
http://www.kaspersky.com/se/

Microsoft Security Essentials (för Windows 7, Vista eller XP. I Windows 8 finns det inbyggt och kallas då Windows Defender.)
http://windows.microsoft.com/sv-se/windows/security-essentials-download

Programleverantörer
Microsoft Security Bulletins
Senaste nytt om säkerhetsuppdateringar för Windows och annan mjukvara från Microsoft.
http://technet.microsoft.com/en-us/security/bulletin

Tips!

Uppdatera automatiskt

De flesta leverantörer av program skickar ut säkerhetsuppdateringar automatiskt. Som användare får du i regel ett meddelande om att det finns en uppdatering tillgänglig utan att gå in på webbplatserna, men de är bra resurser för den som vill fördjupa sig i vad som pågår

Apple Security Updates
Apples sida med information om säkerhetsuppdateringar. http://support.apple.com/kb/HT1222?viewlocale=sv_SE

Adobe Security Bulletins and advisories
Företaget som ligger bakom bland annat Photoshop och den populära pdf-läsaren Adobe Reader samlar här information om säkerhetsuppdateringar.
https://www.adobe.com/support/security/

Lär dig mer om nätet på nätet

Nedan hittar du några exempel på Internetguider från .SE. Du hittar dem alla på vår webbsida www.iis.se/guider. Där finns alla guider att ladda ner gratis i digitalt format, antingen som pdf eller för läsning direkt i webbläsaren. För miljöns skull hoppas vi att du väljer att läsa guiderna direkt på nätet. Vissa guider trycks dock i en begränsad upplaga och finns att beställa på vår webbsida för endast 20 kronor.

Skydda ditt företag mot bedragare

– nätfiffel, bluffakturor och vilseledande försäljning

Internet och telefoni skapar fantastiska möjligheter för företagare och privatpersoner att interagera och göra affärer. Den här guiden handlar om myntets baksida, bedragarna som utnyttjar möjligheterna för egen vinning. I guiden tar vi upp bedragarnas metoder, vad som kan hända och vad du bör se upp med. Viktigast av allt: du får reda på dina rättigheter och hur du skyddar din verksamhet. Ta del av drabbades berättelser och gå igenom checklistorna så du kan vara säker när du använder internet som en viktig del i ditt företagande.

Källkritik på internet

En kritisk hållning till innehållet på internet borde vara en del av allas digitala vardag. Men för att kunna värdera trovärdigheten hos informationen på nätet behövs verktyg och även grundläggande kunskaper om hur webben fungerar. Oavsett om du gör research för ett skolarbete, surfar för nöjes skull eller arbetar med informationsinhämtning finns det metoder att tillgå i sökandet efter fakta och sanningar på nätet. Guiden tar upp allt från traditionell källkritik till hur du spårar upp nättjänsters geografiska hemvist.

Skapa en webbplats med WordPress

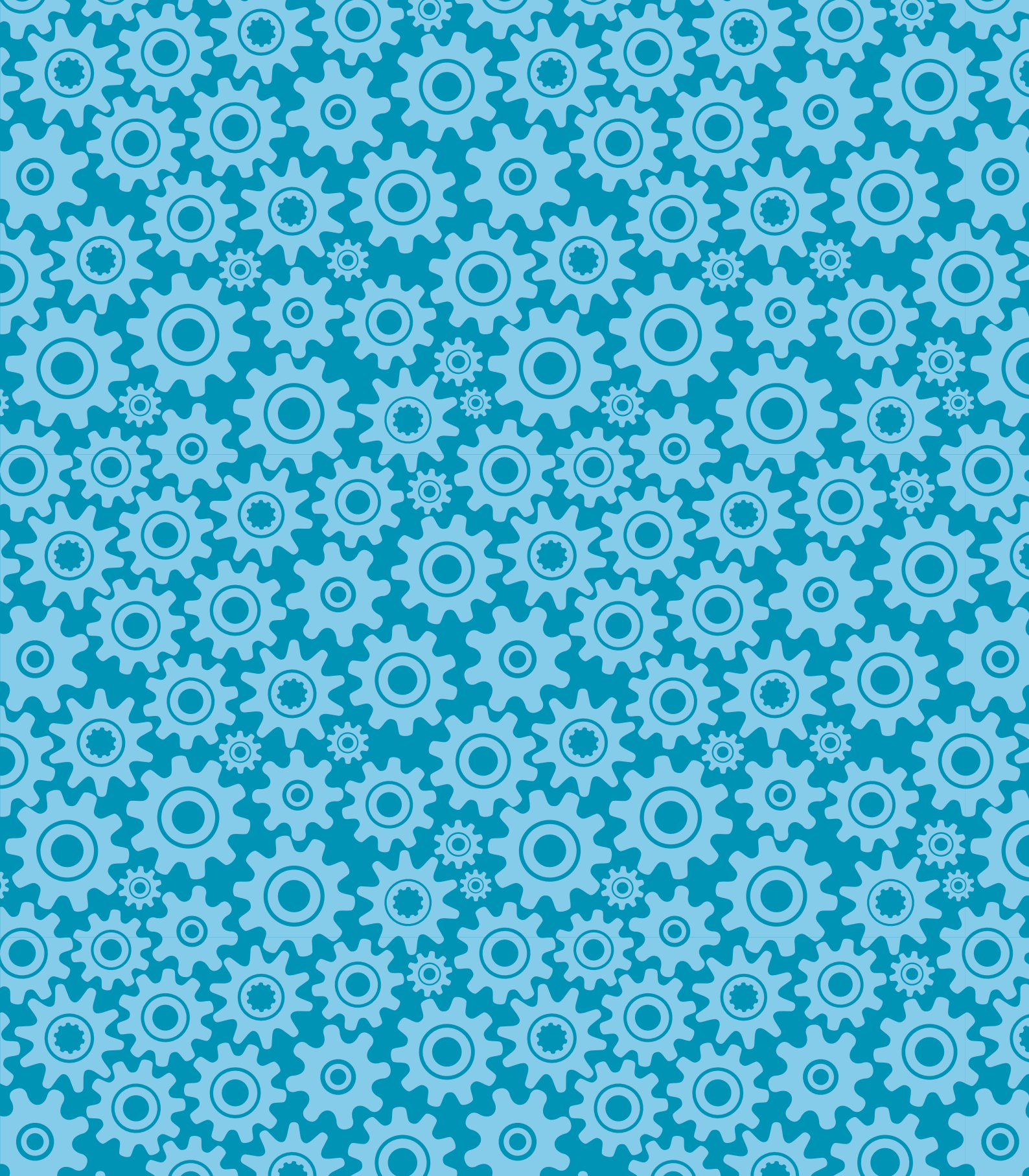
Vill du lära dig hur man skapar en snygg och personlig sajt från grunden? Då är detta internetguiden för dig. WordPress är nätets kanske populäraste verktyg för att skapa bloggar och hemsidor. Det är lätt att lära sig och används på ett oräkneligt antal webbplatser (till exempel www.iis.se, där du kan läsa fler guider). Ändå har det saknats en bra introduktion till WordPress på svenska – fram till nu.

Missa inte .SE-bloggen!

Här skriver .SE:s medarbetare om internet och internetrelaterade ämnen sett ur alla möjliga vinklar och vrår. Du får tips, information, kommentarer till aktuella händelser och mycket mer. Häng med på www. iis.se/blogg

Varje ny .se-adress bidrar till utvecklingen av internet

.SE (Stiftelsen för Internetinfrastruktur) ansvarar för internets svenska toppdomän och administrerar registreringen av domännamn under .se. Överskottet från registreringsavgifterna för domännamn investeras i internetutveckling som gagnar alla internetanvändare, bland annat den här Internetguiden!



.SE (Stiftelsen för Internetinfrastruktur) vill på olika sätt främja en positiv utveckling av internet i Sverige. En av våra viktigaste målsättningar är att alla ska kunna ta tillvara på nätets möjligheter. Därför publicerar vi lärorika Internetguider inom olika spännande ämnen. Det finns praktiska guider för dig som vill börja blogga, teknikguider för dig som undrar hur mejlen du skickar når fram till rätt mottagare och guider som förklarar vem som egentligen bestämmer på nätet.

.SE:s Internetguider är gratis om du läser dem online eller blir prenumerant via www.iis.se/guider. För tryckta exemplar tar vi ut en expeditionsavgift om 20 kr per guide.

.SE (Stiftelsen för Internetinfrastruktur)
Box 7399, 103 91 Stockholm
Tel 08-452 35 00, Fax 08-452 35 02
Org. nr 802405-0190, www.iis.se

9 789187 437052

.se
Vi driver Internet framåt