

SÄKERHET PÅ INTERNET!



Nästa



Hem



Säkerhet på Internet



Nästa

Föregående

Hem



Varför ska vi prata om säkerhet igen?

Nästa



Föregående



Hem



Varför ska vi prata om säkerhet igen?

Svar: *För att förhoppningsvis öka din kunskap.*

Nästa



Föregående



Hem



Varför behöver du öka din kunskap?

Nästa



Föregående



Hem



Varför behöver du öka din kunskap?

Svar: Därför att din kunskap är ditt bästa skydd!

Nästa



Föregående



Hem



Vilka faror finns där ute?

Hur skyddar du dig på bästa sätt?

Nästa



Föregående



Hem





Du kan klicka på en rubrik för att komma direkt till ämnet

- E-post/E-handel
- Lösenord
- Skydda din dator och ditt nätverk
- ID-kapning
- Ransomware
- Phishing (nätfiske)
- Backup
- Tänk på vad du gör
- Viktiga säkerhetstips
- Begrepp/Utryck
- Bra länkar



Epost och E-handel



- Skicka inte känslig eller hemlig information i E-post.
- Öppna inte mail eller bilagor från okända avsändare.
- Handlar du på nätet ska du ta reda på mer om företaget du handlar ifrån.
- Var försiktig med att "parkera" ditt kreditkort för automatisk förlängning av t.ex. en prenumeration.
- När du är färdig med det du ska göra på din Internetbank, andra betalningstjänster, offentliga portaler och andra webbplatser bör du **LOGGA UT**.



Lösenord

“Ditt lösenord måste innehålla stora bokstäver, små bokstäver, siffror, bisarra tecken, varannan bokstav i namnet på en utdöd valuta, och hälften av sista stavelsen av din mormors första husdjurs smeknamn.”

Använd lååååånga lösenord!



Lösenord

Starkt lösenord=kombination av olika sorters bokstäver (gemena och VERSALER), siffror/symboler som helst ska vara minst åtta tecken lång.

Lösenordet är ofta nyckeln

Skrämmande många konton är skyddade på ett enda sätt – ett lösenord. Ofta väldigt kassa lösenord som "hammarby123", "SuperSecret" eller "abcdef". Sådana lösenord tar inte lång tid att knäcka, d.v.s. försöka logga in tills det funkar med hjälp av speciella program. Det finns enorma databaser med vanliga lösenord som används vid sådana här automatiserade attacker.

Stora sajter utsätts kontinuerligt för sådana här försök. Varje dag, varje minut. Många hundra tusen lösenordsförsök per sekund.

Folk använder samma lösenord överallt

Säg att du använder lösenordet "Gustav25" på SL (Accesskortet). Det är lätt för dig att komma ihåg (för att din man hette Gustav och var född 1925), men tyvärr använder du det överallt.

SL klantar sig och läcker sin databas. Nu finns nyckeln till alla dina konton ute i det fria, och det är bara en fråga om tur/otur om du blir hackad.

Skapa ett lösenord med hjälp av en fras som bara Du känner till.
Skriv upp frasen, och förvara på ett ställe som du kommer ihåg.

Exempel: *Min far föddes i Haparanda den 21 april 17*



Nästa

Föregående

Hem



MffiHd21a17



Nästa

Föregående

Hem



Tvåstegsverifiering

Många stora tjänster som Gmail, Facebook eller Dropbox erbjuder detta. Det går till så att när du vill logga in krävs det både ditt vanliga lösenord och en PIN-kod som skickas till din telefon. Det gör att **även om ditt lösenord blir hackat** så kan inte en obehörig ta över din e-post och därmed ditt liv, såvida hen inte har din telefon också. Detta ökar säkerheten **enormt mycket** – aktivera genast på känsliga ställen! Att ha detta påslaget för e-post borde vara obligatoriskt :)

Instruktion för Gmail: <https://www.google.com/landing/2step/>



Skydda telefonen också!

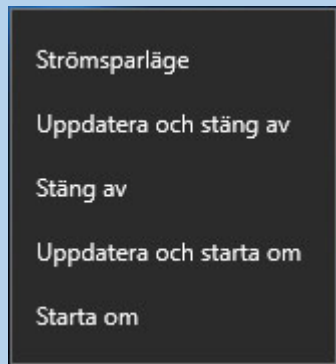
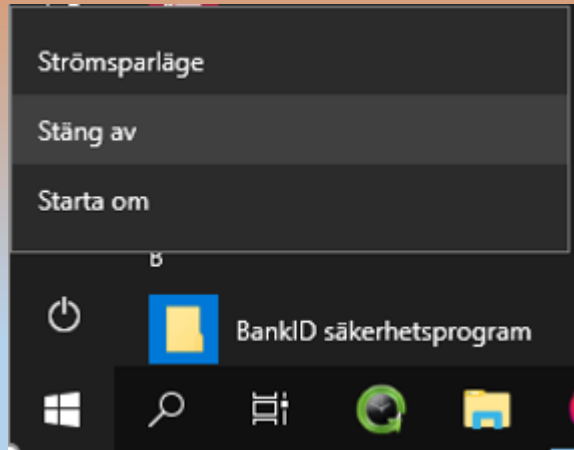
Glöm inte att ha PIN-kod med låsning påslagen på mobilen, eftersom telefonen oftast är konstant inloggad på alla tjänster. Man kan om man vill sätta upp mekanismer för att rensa telefonen om den blir stulen. PIN-kod är **minimum**. Mönsterupplåsning funkar också, se bara till att det inte går att följa fingeravtrycken på skärmen. Givetvis är både PIN och mönsterupplåsning hackbart om den som snott telefonen har tid och kunskap.



Skydda datorn

- Se till att ditt operativsystem (Windows) på datorn uppdateras automatiskt.

- Använd **INTE** Windows **XP**. Inga säkerhetsuppdateringar efter April 2014.
- För Windows **Vista** finns inga säkerhetsuppdateringar efter 11 april 2017.



Skydda datorn

- Se till att ditt operativsystem (Windows) på datorn uppdateras automatiskt.
- Tacka alltid JA till uppdateringar av kända program som du redan har installerat på din dator, t.ex. Google Chrome, Internet Explorer, Adobe Flash Player, Java, Adobe Reader, Microsoft Office.

Skydda datorn

- Se till att ditt operativsystem (Windows) på datorn uppdateras automatiskt.
- Tacka alltid JA till uppdateringar av kända program som du redan har installerat på din dator, t.ex. Google Chrome, Internet Explorer, Adobe Flash Player, Java, Adobe Reader, Microsoft Office.
- Ha ett uppdaterat antiviruskydd på din dator (MS Defender är ok)



Skydda datorn

- Se till att ditt operativsystem (Windows) på datorn uppdateras automatiskt.
- Tacka alltid JA till uppdateringar av kända program som du redan har installerat på din dator, t.ex. Google Chrome, Internet Explorer, Adobe Flash Player, Java, Adobe Reader, Microsoft Office.
- Ha ett uppdaterat antiviruskydd på din dator (MS Defender är ok)
- Tänk på vilka webbplatser du besöker och vad du laddar ner, installera inte okända program.

Skydda datorn

- Se till att ditt operativsystem (Windows) på datorn uppdateras automatiskt.
- Tacka alltid JA till uppdateringar av kända program som du redan har installerat på din dator, t.ex. Google Chrome, Internet Explorer, Adobe Flash Player, Java, Adobe Reader, Microsoft Office.
- Ha ett uppdaterat antiviruskydd på din dator (MS Defender är ok)
- Tänk på vilka webbplatser du besöker och vad du laddar ner, installera inte okända program.
- Skydda alltid datorn med ett lösenord så att den är låst för obehöriga.

Skydda datorn

- Se till att ditt operativsystem (Windows) på datorn uppdateras automatiskt.
- Tacka alltid JA till uppdateringar av kända program som du redan har installerat på din dator, t.ex. Google Chrome, Internet Explorer, Adobe Flash Player, Java, Adobe Reader, Microsoft Office.
- Ha ett uppdaterat antiviruskydd på din dator (MS Defender är ok)
- Tänk på vilka webbplatser du besöker och vad du laddar ner, installera inte okända program.
- Skydda alltid datorn med ett lösenord så att den är låst för obehöriga.
- När du har utfört dina ärenden på en webbsida (ex: bankärenden) bör du logga ut från sidan.

Skydda datorn

- Se till att ditt operativsystem (Windows) på datorn uppdateras automatiskt.
- Tacka alltid JA till uppdateringar av kända program som du redan har installerat på din dator, t.ex. Google Chrome, Internet Explorer, Adobe Flash Player, Java, Adobe Reader, Microsoft Office.
- Ha ett uppdaterat antiviruskydd på din dator (MS Defender är ok)
- Tänk på vilka webbplatser du besöker och vad du laddar ner, installera inte okända program.
- Skydda alltid datorn med ett lösenord så att den är låst för obehöriga.
- När du har utfört dina ärenden på en webbsida (ex: bankärenden) bör du logga ut från sidan.
- Lämna inte datorn i bilen eller på andra platser där den är lätt att stjäla.

ID-kapning



Säkerhet på Internet

Hur märker du det?

- En bedragare med hjälp av stulna personuppgifter köper dyra varor & tjänster i ditt namn och dina pengar
- Nya bankkonton öppnas i ditt namn
- Ansökan om kreditlån du inte känner igen
- Telefonabonnemang du inte känner igen
- Fakturor på varor du inte beställt
- Hur vanligt är detta idag?

Ökar lavinartat – mer än 200 000 personer drabbas varje år

Hur kan du skydda dig?

Nästa

Föregående

Hem



ID-kapning

Minska risken för id-kapning

- Skydda dig mot falsk adressändring med Skatteverkets tjänst. **Spärra obehörig adressändring**. Med den kan du anmäla att du bara tillåter adressändring digitalt (via din e-legitimation).
 - <http://www.skatteverket.se/privat/sjalvservice/allaetjanster/tjanster/sparraobehorigadressandring.4.361dc8c15312eff6fd123f5.html>
- Skydda dig på <https://www.adressandring.se/private/watch> så din eftersända post bara kan ändras via din egen e-legitimation.
- Se till att skydda din dator mot eventuella angripare (Läs mer på sidan: [Skydda datorn](#)) *

ID-kapning

Minska risken för id-kapning



Säkerhet på Internet

- Skaffa brevlåda med lås så att ingen kan stjäla din post och komma åt dina personliga uppgifter.
- Skylta inte om din semester i sociala medier

Nästa

Föregående

Hem



ID-kapning

Minska risken för id-kapning

- Om butiken frågar efter ditt personnummer, visa ditt leg eller körkort. Säg det inte så att alla hör!
- Släng inte post med personlig information i sopor eller i pappersinsamling.
- Uppdatera/skicka aldrig dina identitetsuppgifter, lösenord eller bankkortsuppgifter via e-post.
 - Banker frågar aldrig via e-post eller sociala medier om dina koder, lösenord eller bankkortsnummer.

ID-kapning

Minska risken för id-kapning

- Öppna inte bilagor i e-post från okända eller oväntade avsändare. Kontakta istället den aktuella avsändaren om du vill undersöka vidare.
- Kolla regelbundet dina kontoutdrag för att se att det inte sker några oförklarliga transaktioner.

Nästa



Föregående



Hem



ID-kapning

Minska risken för id-kapning

- Kolla kreditupplysningen
När någon tar en kreditupplysning får du som regel en kopia på detta. Om du inte vet varför ett företag tar en kreditupplysning bör du kontakta dem och kontrollera vad orsaken är. En oförklarlig kreditupplysning kan vara ett tecken på att någon vill ta ett lån eller handla på kredit.
- Spärra ditt betalkort för användning på internet eller i utlandet och lås bara upp det när du behöver använda det.

ID-kapning

Minska risken för id-kapning

- Undvik papperspost där du kan
 - Papperspost är generellt osäkert, och ett bra alternativ är förstås att gå över till digital kommunikation.
 - [Kivra](#) är den största tjänsten, och den samlar både brev från myndigheter och privata företag.
 - En konkurrent är [Digimail](#) från postföretaget Bring.
 - Vill du bara ha digital post från myndigheter kan du använda tjänsten [Min myndighetspost](#).
Alla tjänster är gratis och använder inloggning via Bankid.

Om du redan blivit utsatt för ID-kapning

- Gör en polisanmälan direkt och bestrid fakturan
- Spärra personnumret hos kreditupplysningsföretaget
- Ring din bank – spärra konton och kreditkort
- Kontrollera hos Skatteverket din folkbokförda adress
- Om din hem/villaförsäkring täcker in "Hjälp vid ID-stöld"
 - Kontakta ditt försäkringsbolag så hjälper dem till med i stort sett allt – polisanmälan, kontakta bank och kreditkortsutgivare, begränsa konsekvenserna, m.m.
Ingår i hemförsäkring hos Folksam, Länsförsäkringar, m.fl.

Minska risken för id-kapning

- Använd ett bra lås till din brevlåda så att ingen kan stjäla din post och komma åt dina personliga uppgifter.
- Skydda dig mot falsk adressändring med Skatteverkets tjänst. **Spärra obehörig adressändring**. Med den kan du anmäla att du bara tillåter adressändring digitalt (e-leg).
 - <http://www.skatteverket.se/privat/sjaldvservice/allaetjanster/tjanster/sparraobehorigadressandring.4.361dc8c15312eff6fd123f5.html>
 - Skydda dig på <https://www.adressandring.se/private/watch> så din eftersända post bara kan ändras via din egen e-legitimation.
- Se till att skydda din dator för eventuella angripare (Läs mer på sidan: [Skydda datorn](#)) *
- Lämna inte ut ditt personnummer på nätet och släng inte post med personlig information i sopor eller i pappersinsamling.
- Uppdatera/skicka aldrig dina identitetsuppgifter, lösenord eller bankkortsuppgifter via e-post.
 - Banker frågar aldrig via e-post eller sociala medier om dina koder, lösenord eller bankkortsnummer.
- Öppna inte bilagor i e-post från okända eller oväntade avsändare. Kontakta istället den aktuella avsändaren om du vill undersöka vidare.
- Kolla regelbundet dina kontoutdrag för att se att det inte sker några oförklarliga transaktioner.
- Kolla kreditupplysningen
När någon tar en kreditupplysning får du som regel en kopia på detta. Om du inte vet varför ett företag tar en kreditupplysning bör du kontakta dem och kontrollera vad orsaken är. En oförklarlig kreditupplysning kan vara ett tecken på att någon vill ta ett lån eller handla på kredit.
- Spärra ditt betalkort för användning på internet eller i utlandet och lås bara upp det när du behöver använda det.
- Undvik papperspost
 - Papperspost är generellt osäkert, och ett bra alternativ är förstås att gå över till digital kommunikation.
 - [Kivra](#) är den största tjänsten, och den samlar både brev från myndigheter och privata företag.
 - En konkurrent är [Digimail](#) från postföretaget Bring.
 - Vill du bara ha digital post från myndigheter kan du använda tjänsten [Min myndighetspost](#). Alla tjänster är gratis och använder inloggning via Bankid.



LOGGA ALDRIG IN PÅ DITT BANK-ID
PÅ UPPMANING AV NÅGON ANNAN!

Nu blir det 10 minuter

PAUS!

Nästa

Föregående

Hem



Ransomware

Ransomware är en typ av skadlig kod som låser din dator eller krypterar dina filer, för att sedan kräva att du betalar en lösensumma för att få tillbaka åtkomsten. Du kan bli infekterad via bifogad fil i ett mail, eller via webbläsaren.

Det enda sättet är då att betala priset och se glad ut (även om det är omöjligt). I alla fall får du göra det om du inte har tillräckligt bra backup, och då på något annat ställe än enheter anslutna till datorn, för dessa kommer troligtvis också krypteras.

Läs mer här: <http://blogg.tkj.se/ransomware-bedrageri-cryptware/>

Mer att läsa här: <http://blogg.tkj.se/undvika-farliga-lankar-bedragerier-19-guider/>
<http://blogg.tkj.se/malwarebytes-anti-malware-tar-bort-virus-spyware/>

Vi rekommenderar starkt programmet Malwarebytes:

Premiumversionen kostar 449 kr/år, alternativt 669 kr/två år

Ladda ner endast från denna webbplats:

<https://www.malwarebytes.com/>

Skyddar dig i realtid mot:

- Ransomware
- Spyware
- Adware
- m.m.

Gratisversionen kompletterar ditt antivirusprogram
Premiumversionen ersätter ditt antivirusprogram



Phishing (Nätfiske)

Var misstänksam om du får e-post där du exempelvis uppmanats att klicka på en länk och ange dina personliga koder. Följ aldrig sådana instruktioner. Det finns inga seriösa företag eller banker som skulle skicka ett sådant e-postmeddelande.



Smarta telefoner och surfplattor

- Hantera din smarta telefon/surfplatta på samma sätt som du hanterar din dator.
- Använd alltid skärmlås (ex: pinkod, lösenord) på din mobil eller surfplatta så att inte vem som helst kan komma åt applikationer och personliga uppgifter.
- Lämna inte din smarta telefon eller surfplatta utan uppsikt och tänk på vem du lånar ut den till.
- Klicka inte på okända länkar och öppna inte okända filer, oavsett om det är via webbläsaren, genom epost eller som SMS.
- Tänk efter vad du installerar. Ladda endast ned applikationer, appar från kända och välrenommerade "butiker" som AppStore och Google Play.
- Tänk på att säkerhetskopiera information som du inte vill bli av med från din smarta mobil/surfplatta.
- Uppdatera din mobila enhet så fort det finns en uppdatering tillgänglig.
- Om du förlorar din surfplatta eller smarta telefon är det viktigt att du genast ringer och spärrar ditt abonnemang.

Backup (säkerhetskopiering)

Om du har alla bilder på en separat hårddisk – **räkna** med att hårddisken förr eller senare går sönder.

Diskar slits, och det är *alltid bara en tidsfråga innan den lägger av*.

Att kombinera en mekanisk disk med en onlinetjänst som t.ex. OneDrive, Dropbox eller iCloud är ofta bra och löser problemen!

Se helt enkelt till att ha backup på mer än ett fysiskt ställe!



Tänk på vad du gör



- Det viktigaste tipset av alla. Var försiktig.
- Behöver du verkligen spara kreditkortsuppgifter hos online-shoppen?
- Är det en bra idé att ha min PIN-kod uppskriven i plånboken?
- Vad händer om min dator blir stulen på ett fik?

Lär dig själv att ställa de här frågorna i vardagen.

Räkna med att nästan allt du gör på nätet har potential att bli publik och oåterkallelig information. Se till att i alla fall ha hyfsat koll på vad du kan göra för att skydda dig, och du är genast mycket säkrare än den stora massan.

Viktiga säkerhetstips

1. Välj starka lösenord
 - *Minst 8 tecken (helst 12 tecken eller fler)*
2. Skydda dig mot s.k. spionprogram
 - *Antivirus + Malwarebytes*
3. Skydda dig mot falsk adressändring med Skatteverkets tjänst.
4. *Skydda dig också via www.adressandring.se*
5. Skydda din integritet på nätet
 - *Var försiktig med sociala nätverk*
6. Var försiktig med telefonförsäljare
 - *Ha som princip att ALDRIG köpa över telefon*
7. Var allmänt vaksam



- Håll din dator och dina program uppdaterade
- Skaffa ett bra antivirusprogram (*inbyggt i Windows 10 duger bra*)
- Skaffa Malwarebytes Premium *
- Använd sunt förnuft



Om du följer dessa enkla råd, kan du sova gott på natten!

* Ladda ner endast från <https://www.malwarebytes.com/>

Nästa

Föregående

Hem



- **Virus** - **Datorvirus** eller **datavirus** är små [datorprogram](#) som sprider sig genom att lägga en kopia av sig själva inuti andra program, *värdprogram*, på sådant sätt att koden körs då värdprogrammet [körs](#). Då ett infekterat värdprogram körs kan dess virus spridas ytterligare och även utföra annat som viruset har konstruerats för att göra. I dagligt tal kallar man ofta alla typer av [skadlig programkod](#) för virus.
- **Malware** - **Sabotageprogram**, **skadlig programvara**, engelska **malware**, är ett samlingsbegrepp för oönskade [datorprogram](#) eller delar av datorprogram som har utvecklats i syfte att störa IT-systemet, för att samla in information i smyg, eller utnyttja för ändamål som inte gagnar användaren, såsom utskick av [skräppost](#), [intrång](#) på andra datorer eller [Denial of Service](#)-attacker. Sabotageprogram installeras på en dator eller ett datornätverk utan [administratörens](#) samtycke, eller med ett samtycke som inte innefattar alla aspekter av programvaran.
- **Exploit**
attackmetod, attack mot [sårbarhet](#), även: *svag punkt, lucka, sårbarhet* – metod som utnyttjar en sårbarhet i ett datorsystem för att komma åt skyddad information eller för sabotage.
- **Spyware** - **Spionprogram** ([eng](#): **spyware**) är [datorprogram](#) som körs på en dator utan [användarens](#) godkännande, och samlar och vidarebefordrar information till annan part. Informationen kan omfatta korrespondens, lösenord och liknande.
- **Ransomware** - **Ransomware** är en typ av [skadlig programvara](#). Namnet kommer av engelskans *ransom*, [lösensumma](#), och programmet hindrar användaren från att använda datorn på ett normalt sätt om inte användaren betalar en lösensumma, eller gör något annat som programmet kräver.
- **Phishing** - **Nätfiske** eller lösenordsfiske, är en form av [social manipulation](#) och en olaglig metod att lura innehavare av [bankkonton](#) och andra elektroniska resurser att delge [kreditkortsnummer](#), [lösenord](#) eller annan känslig information.
- **Brandvägg** - En brandvägg analyserar inkommande och utgående trafik och blockerar obehöriga [IP-paket](#).

Bra länkar

- <https://www.iis.se/>
- <https://www.folkbildning.net/amnen/media-it/informationssamhallet/it-sakerhet-for-privatpersoner/>
- <https://www.iis.se/lar-dig-mer/guider/it-sakerhet-for-privatpersoner/>
- <https://www.dinsakerhet.se/>
- <https://www.xn--itskerhet-x2a.com/links/>

Ett bra grundläggande antivirus-skydd är bra, men det räcker inte.

Det allra viktigaste skyddet är du själv och din kunskap.

9 bästa sätten att säkra din dator mot hot!

1. Håll dig informerad
2. Skaffa säkerhetsprogram (om du inte har Windows 10)
3. Håll ditt operativsystem uppdaterat
4. Uppdatera dina tillämpningsprogram
5. Använd tvåfaktorsautentisering
6. Använd unika lösenord
7. Ladda inte ner från osäkra källor
8. Skydda dig på osäkra nätverk

- ❓ **Virus** – infekterar och förstör filer
- ❓ **Maskar** – sprider sig själva via din adresslista
- ❓ **Trojaner** – gömda i andra program, tex skärmläckare
- ❓ **Falska virus/scareware** – varnar för angrepp
- ❓ **Adware/spionprogram** – visar popup-annonser
- ❓ **Utpressningsvirus** – krypterar hårddisken

Klicka aldrig på sådana "erbjudanden" ==>



Framtidens mobiltelefoner

<https://www.youtube.com/watch?v=B3W3SA2k5yo>



Nästa

Föregående

Hem



**Nu är det slut!
Hej då!!**



Föregående

Hem

