Datasäkerhet

Datasäkerhet är den delen av IT-säkerhet som avser att skydda datorsystem.
I detta ingår förebyggande, upptäckt och åtgärdande av obehöriga användare av datorsystem, bland annat hackers och virus.
Men det innebär också att man skyddar datorsystem mot t.ex. förlust av data på grund av en hårddiskkrasch.

IT-säkerhet *ansvarar för att skydda en organisations (företags, myndighets, organisation och enskilda personers) värdefulla tillgångar som information, maskinvara ("hårdvara") och programvara ("mjukvara").*

Agenda

- Förebyggande åtgärder
- Samtal från utlandsnummer
- Meddelande från din bank
- Falska telefonsamtal
- Varning för falska poliser och andra bedragare
- Tre aktuella bedrägerier
- Falskmejl om återbäring av skatt
- Samtal från Microsoft-supporten
- Romansbedrägeri
- Skydda dig mot virus
- De digitala hoten
- ID-kapning
- Information om oss själva på Eniro.se och Hitta.se
- Ta backup på viktiga dokument, och bilder

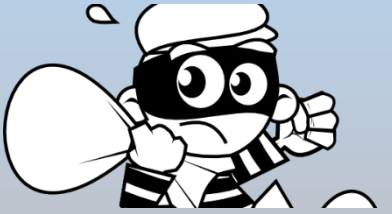
Förebyggande åtgärder

- Var uppmärksam och försiktig när det gäller telefonsamtal och e-post.

Förebyggande åtgärder

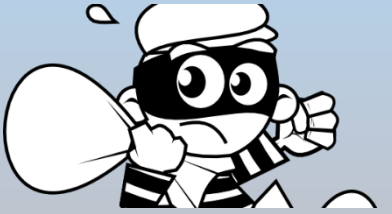
- Var uppmärksam och försiktig när det gäller telefonsamtal och e-post.
- Skydda dig mot virus.

Förebyggande åtgärder



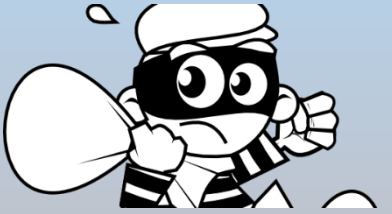
- Var uppmärksam och försiktig när det gäller telefonsamtal och e-post.
- Skydda dig mot virus.
- Se till att Windows ALLTID är uppdaterad (sker med automatik).

Förebyggande åtgärder



- Var uppmärksam och försiktig när det gäller telefonsamtal och e-post.
- Skydda dig mot virus.
- Se till att Windows ALLTID är uppdaterad (sker med automatik).
- Se till att ditt e-postprogram ALLTID är uppdaterat (om du har en s.k. klient i din dator).

Förebyggande åtgärder



- Var uppmärksam och försiktig när det gäller telefonsamtal och e-post.
- Skydda dig mot virus.
- Se till att Windows ALLTID är uppdaterad (sker med automatik).
- Se till att ditt e-postprogram ALLTID är uppdaterat (om du har en s.k. klient i din dator).
- Se till att din webbläsare ALLTID är uppdaterad (sker med automatik).

Du kan nu sova gott om nätterna!

1. Samtal från utlandsnummer

- Om du blir uppringd av ett utländskt nummer, svara inte om du inte förväntar dig ett samtal. Och om du har ett missat samtal som inleds med ett utlandsnummer ska du inte heller ringa upp.
  Samtalet är troligen ett bedrägeri och du riskerar att bli av med stora summor pengar.

2. Meddelande från din bank

- Du får ett mejl eller blir uppringd från din bank om att det har uppstått ett problem med ditt konto och att du ska skicka in dina kontouppgifter.

  Bedragarens mål är att:

  Få dig att lämna ut dina kontouppgifter och lägga beslag på dina pengar.

  Så skyddar du dig:

  Banker och andra kreditinstitut begär aldrig in dina uppgifter via mejl.
  Är du osäker på om meddelandet kommer från din bank, ring banken och fråga. Klicka aldrig på länkar i den här typen av mejl.
  Det finns en risk att din dator blir smittad med skadlig kod.

Hej,
Onsdagen den 29 januari kl. 22.35 ringer en okänd man till en målsägande boende på Lojovägen på Lidingö. Mannen utger sig för att vara polis och säger att målsägandens son råkat ut för en olycka. När målsäganden berättar att hon inte har någon son ändrar sig mannen och säger dotter. Målsäganden sa då att hon inte heller hade någon dotter varpå mannen ändrar sig till att säga anhörig och försöker sedan förmå målsäganden att använda sin bankdosa och logga in på sin internetbank. Målsäganden förstod att mannen försökte lura henne och sa att hon skulle anmäla det till polisen.

Mannen pratade bra svenska men det var inte hans modersmål. Han var mycket artig och trevlig, hade en behaglig röst och pratade med baryton röstläge.

Bifogar information om hur ni skyddar er mot s.k. Vishing →
(vidarebefordra till era medlemmar).

FALSKA TELEFONSAMTAL

Vishing (voice phising – kombination av falska telefonsamtal och e-postmeddelanden) innebär att en person blir uppringd av en bedragare som utger sig för att vara från exempelvis banken, för att lura till sig personlig-, finansiell- eller säkerhetsinformation.

VAD KAN DU GÖRA?

- Vid ett oväntat telefonsamtal från en välkänd motpart, lägg på och ring tillbaka till ett nummer du säkert vet går till mottagaren.
- **Logga aldrig in på annans begäran.**
- **Anta inte att en uppringare är äkta** bara för att de har personliga uppgifter om dig. Bedragare kan hitta grundläggande information om dig på nätet.
- Lämna inte ut information från ditt bankkort eller ditt lösenord till internetbanken. **Din bank skulle aldrig ringa upp och be om dessa uppgifter.**
- Banken skulle heller aldrig ringa upp och begära att du för över pengar till något annat konto.
- Om du misstänker att du är utsatt för vishing, kontakta din bank.

EUROPOL EC3 European Cybercrime Centre · EBF · Polisen

#CyberScams

Polisen

Varning för falska poliser och andra bedragare

Den senaste tiden har äldre personer utsatts för bedrägerier av falska poliser. Det kan ske via telefon eller hembesök.

Det kan gå till på olika sätt. Till exempel att någon ringer upp och säger sig arbeta för Polismyndigheten, och behöver tillgång till ditt bankkort, pin-kod och värdesaker. En stund senare kommer någon för att hämta sakerna. Men bedragarna kan också ange andra orsaker till att vilja komma in i din bostad.

Så skyddar du dig:

- **Lägg på luren om någon ringer och du blir osäker.** Det gäller oavsett om personen utger sig för att vara en nära släkting, från banken, ett företag eller en myndighet som t.ex. polisen.
- **Kontrollera personen som ringer, skickar mejl eller ringer på dörren.** Om personen säger sig vara polis kontakta 114 14 för att komma till växeln och där be att få ta reda på om det är en polis. Är det personal från någon annan myndighet eller företag ringer du deras växel. Be dem kontrollringa personens mobiltelefon för att bekräfta att det är rätt person som besöker dig.
- **Ring en anhörig eller bekant,** sök stöd.
- **Släpp aldrig in en obekant person i ditt hem.** Stäng dörren om du känner oro. Polisen åker aldrig hem till någon för att hämta bank- och/eller kreditkort eller andra värdesaker. Om någon kontaktar dig med ett sådant ärende är det en bedragare.
- **Lämna aldrig över** legitimation, bankkort eller din kod till någon annan person.
- **Vid pågående brott ring 112.** Om brottet inte är pågående ska du ringa 114 14.

Om du utsätts för brott

ring 112

Tre aktuella bedrägerier

1. Bluff-SMS
   - Även om det står PostNord eller SF-Bio eller något annat välrenommerat företag kan det röra sig om en bluff.
     Åtgärd: Klicka inte på länken. Är du tveksam, ring upp företaget som anges vara avsändare och kontrollera att det stämmer.

Tre aktuella bedrägerier

1. Bluff-SMS
   - Även om det står PostNord eller SF-Bio eller något annat välrenommerat företag kan det röra sig om en bluff.
     Åtgärd: Klicka inte på länken. Är du tveksam, ring upp företaget som anges vara avsändare och kontrollera att det stämmer.

2. Utpressarmejl
   - Du får e-post som säger att de har en inspelning från din webbkamera att du porrsurfat, ”*Om du inte betalar summa X i bitcoin till det här kontot visar jag klippen för alla du känner*”.
     Åtgärd: Polisanmäl

Tre aktuella bedrägerier

1. Bluff-SMS
   - Även om det står PostNord eller SF-Bio eller något annat välrenommerat företag kan det röra sig om en bluff.
     Åtgärd: Klicka inte på länken. Är du tveksam, ring upp företaget som anges vara avsändare och kontrollera att det stämmer.

2. Utpressarmejl
   - Du får e-post som säger att de har en inspelning från din webbkamera att du porrsurfat, ”*Om du inte betalar summa X i bitcoin till det här kontot visar jag klippen för alla du känner*”.
     Åtgärd: Polisanmäl

3. Investeringsbedrägeri
   - Inkörsporten är ofta fejkade nyhetsartiklar som ser ut att komma från betrodda medier. Där utnyttjas folkkära kändisar som Leif GW Persson och Filip Hammar.
     Åtgärd: Fråga dig ”*Är detta för bra för att vara sant? Då är det nog en bluff*”. Polisanmäl

3. Falskmejl om återbäring av skatt

- **Scenario:** Du får ett mejl om att du är berättigad till skatteåterbäring och avsändaren påstår sig vara Skatteverket. Avsändarens mejladress kan vara refund@skatteverket.se, skatt@skatteverket.se och liknande adresser. Du blir ombedd att klicka på en länk som ser ut att gå till skatteverket.
- **Bedragarens mål är att:**
  Få dig att lämna ut dina kontouppgifter och lägga beslag på dina pengar.
- **Så skyddar du dig:**
  - Klicka aldrig på länkar i den här typen av mejl. Den här typen av bedrägeri kallas för phishing eller nätfiske.

4. Samtal från Microsoft-supporten

- **Scenario:** Du blir uppringd av en person som utger sig för att vara en representant från Microsoft eller Windows supportavdelning.

Personen påstår att din dator är utsatt för virus eller liknande och att du riskerar att förlora all data på hårddisken. Du får sedan instruktioner om att skriva in komplicerade kommandon till din dator, det vill säga du accepterar att personen i andra änden får fjärrstyra din dator.

4. Samtal från Microsoft-supporten

- **Bedragarens mål är att:**
  - Få åtkomst till data som finns sparad på din dator, t.ex. kontoinformation, ladda ner skadlig kod till din dator. Den gör att datorn kan kontrolleras på distans och att data du har sparat blir tillgänglig.
  - Du ska betala för utfört arbete, oftast genom att uppge ditt kortnummer. Många gånger dras sedan betalningen flera gånger.
  - Komma åt konto- och bankinformation för att kunna göra obehöriga överföringar från ditt konto.

Så skyddar du dig:

Lägg helt enkelt på luren.

5. Romansbedrägeri, amerikansk militär eller desertör

- **Scenario**: Du får ett mejl av en person som påstår sig vara en amerikansk hög militärofficer på uppdrag i olika delar av världen eller en desertör från armén i ett annat land. Personen skickar bilder på sig själv i syfte att utveckla en relation med dig. När relationen har etablerats ber personen om pengar för att kunna komma och träffa dig i Sverige.
- **Bedragarens mål är att:**
  Spela på känslor och förmå dig att skicka pengar.
- **Så skyddar du dig:**
  Ställ dig frågan om hur stor chansen är att en person, ofta från en annan kontinent, kontaktar just dig?
  Skicka aldrig pengar till någon som ber om det via internet.

Skydda dig mot virus

I dagligt tal kallar man ofta alla typer av skadlig programkod för **VIRUS**.

Skydda dig mot virus

I dagligt tal kallar man ofta alla typer av skadlig programkod för **VIRUS**.

Hur smittas man av virus?

- Du klickar på en bilaga eller en länk som startar viruset.
- Du går in på en smittad webbsida samtidigt som du har låga säkerhetsinställningar på din webbläsare.
- Du har inte uppdaterat Windows (Windows Update fel inställt).
- Dålig säkerhetshantering av webbservrar som gör att du blir smittad.

För att skydda sig mot virus bör man göra detta grundläggande:

För att skydda sig mot virus bör man göra detta grundläggande:

1. Se till att ha ett bra ANTIVIRUSPROGRAM

För att skydda sig mot virus bör man göra detta grundläggande:

1. Se till att ha ett bra ANTIVIRUSPROGRAM

2. Uppdatera alltid ditt operativsystem (Windows)

För att skydda sig mot virus bör man göra detta grundläggande:

1. Se till att ha ett bra ANTIVIRUSPROGRAM
2. Uppdatera alltid ditt operativsystem (Windows)
3. Uppdatera ditt e-postprogram (om du har en klient)

För att skydda sig mot virus bör man göra detta grundläggande:

1. Se till att ha ett bra ANTIVIRUSPROGRAM
2. Uppdatera alltid ditt operativsystem (Windows)
3. Uppdatera ditt e-postprogram (om du har en klient)
4. Uppdatera din webbläsare (sker automatiskt)

De digitala hoten

Sammanfattning:

- **Virus** – infekterar och förstör filer
- **Maskar** – sprider sig själva via din adresslista
- **Trojaner** – gömda i andra program, t.ex. skärmsläckare
- **Utpressningsvirus** – krypterar hårddisken

Hur kan jag skydda mig på bästa sätt?

Skydda din dator

- **Windows alltid uppdaterat** (automatiskt i Windows 10, om du själv inte ändrat inställningen)

  - skyddar mot säkerhetshot som antivirus-programmen ***inte*** klarar av (vissa uppdateringar kräver omstart)

Hur kan jag skydda mig på bästa sätt?

Skydda din dator

- **Webbläsaren uppdaterad** (Chrome, Firefox, etc. automatiskt som standard)

  - använd alltid senaste versioner och uppdateringar av kända program såsom t.ex. Java, Adobe Flash Player, Adobe Reader

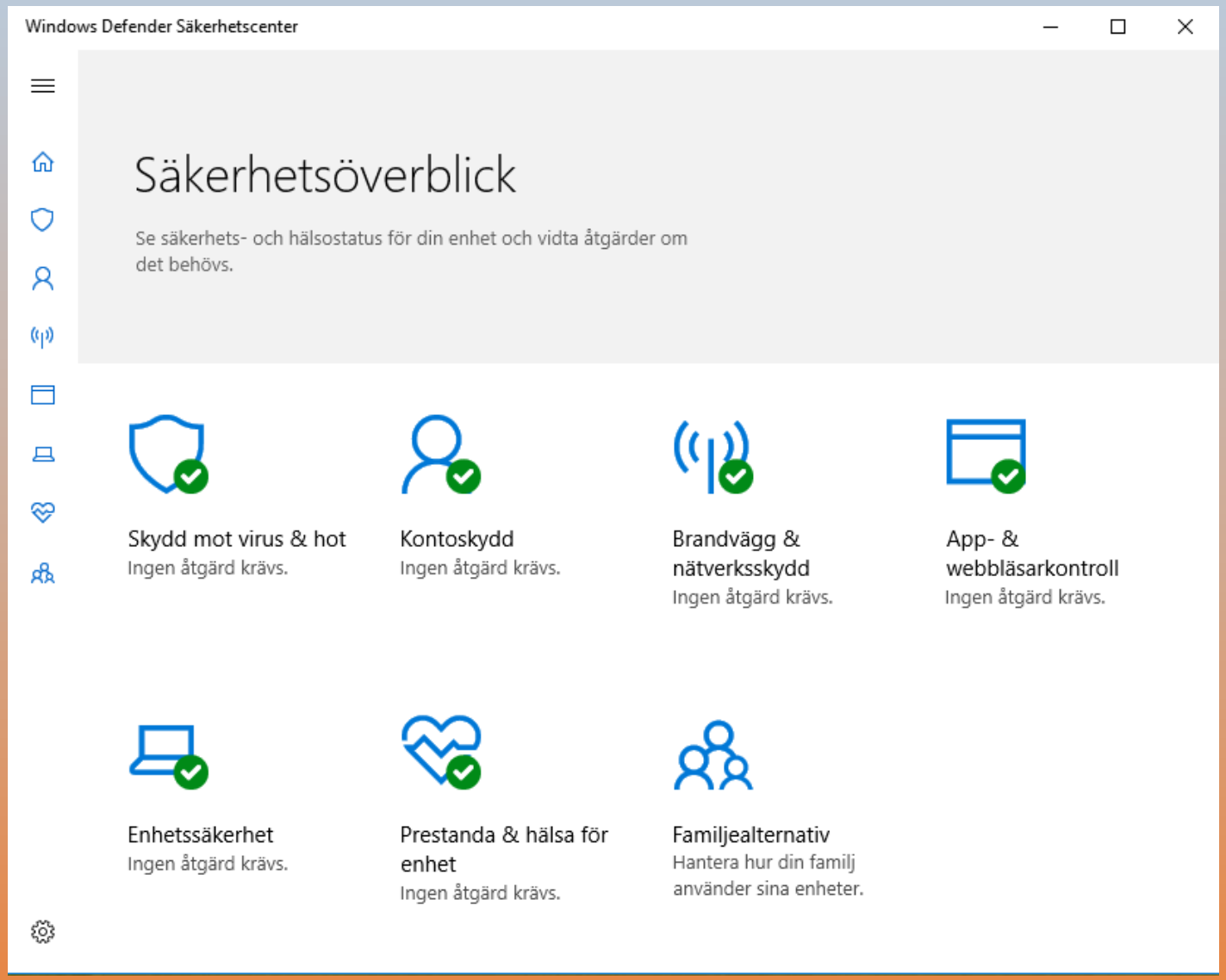
Hur kan jag skydda mig på bästa sätt?

Skydda din dator

- **Anti-virusprogram – uppdateras dagligen automatiskt**

  - söker efter virus, maskar o trojaner i e-post och andra filer på datorn.
  - *Windows Defender* ger ett bra grundskydd, men det finns också andra lösningar.

Windows Defender – ingår i Windows 10



<u>Större säkerhetspaket kan ge ytterligare skydd</u>

- Förlust av viktiga filer vid datorkrasch
- Bortglömda och osäkra lösenord
- Nätfiske på webben t.ex. via sociala medier
- Ej uppdaterade program
- Backup
- Stöldskydd
- Lösenordshanterare
- Skräppostfilter
- Filkryptering

Hur kan jag skydda mig på bästa sätt?

- Försiktighet med att öppna e-postbilagor

  - en av de främsta riskerna för att få virus/trojaner
  - öppna aldrig bilagor från okända/oväntade

Hur kan jag skydda mig på bästa sätt?

- Försiktighet med att klicka på ”hyperlänkar” i e-posten

  - öppnar webbplatser som ofta används för ”nätfiske”
  - klicka bara på länkar i e-post som du litar på

Att tänka på när du surfar

- Försiktighet med kreditkortsnr /kontonr /personlig info

  - endast om du litar på webbplatsen och att ett säkert betalsystem används

Att tänka på när du surfar

- Hur använder jag sociala media?

  - Facebook, Instagram, Blocket, m.fl.

ID-kapning – hur skyddar man sig

VIKTIGAST!!!

- 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. Kallas för Adresslåset.

ID-kapning – hur skyddar man sig

- Lämna inte ut personnummer utan att veta till vem eller vad det ska användas till.

ID-kapning – hur skyddar man sig

- Lämna inte ut personnummer utan att veta till vem eller vad det ska användas till.
- Säg inte ditt personnummer i butiken – visa leg/körkort i stället.

ID-kapning – hur skyddar man sig

- Lämna inte ut personnummer utan att veta till vem eller vad det ska användas till.
- Säg inte ditt personnummer i butiken – visa leg/körkort i stället.
- Riv sönder papper som innehåller personuppgifter innan du slänger eller återvinner.

ID-kapning – hur skyddar man sig

Klicka inte på länkar från okända avsändare

- Lämna inte ut personuppgifter via tel/internet/epost om du inte är säker vem du har att göra med.

ID-kapning – hur skyddar man sig

- Lämna inte detaljerad info om dig på sociala media

ID-kapning – hur skyddar man sig

- Byt till låsbar brevlåda

ID-kapning – hur skyddar man sig

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.
  - Vill du bara ha digital post från myndigheter kan du använda tjänsten Min myndighetspost.

    Alla tjänster är gratis och använder inloggning via Bankid.

Kan jag redigera information om mig själv på eniro.se och hitta.se ??

Insamling och uppdatering av Kontaktuppgifter
Eniro inhämtar Kontaktuppgifter (här: namn, adress och telefonnummer) från olika leverantörer såsom t.ex. operatörer och i vissa fall andra officiella uppgiftsregister.

Person kan själv lägga till, ändra eller ta bort Kontaktuppgifter rörande sig själv genom att kontakta Eniros kundservice eller genom att på https://www.eniro.se/kontakt själv lägga till, göra ändringar eller ta bort Kontaktuppgift och därefter bekräfta dessa ändringar genom uppringning eller SMS från telefonnummer som finns som befintlig Kontaktuppgift för den Person som ändringen avser. De uppgifter som Person själv lägger till eller ändrar gällande Kontaktuppgifter publiceras när de granskats och godkänts av Eniro i enlighet med Eniros vid var tid gällande publiceringspolicy.

Här gör du motsvarande på **Hitta**.se https://www.hitta.se/kontakta-oss#redigera-mina-uppgifter

Ta backup på viktiga dokument & foton

- **Säkerhetskopiera till externt lagringsmedia**
  - USB-minne/sticka - 32 GB har plats för ca. 10.000 foton
  - Extern hårddisk – 500 GB har plats för ca. 150.000 foton

Ta backup på viktiga dokument & foton

- **Alternativ - Säkerhetskopiera till ”molnet”**
  - Lagra gratis dina foton, videoklipp, dokument (till en viss gräns)
  - Titta och dela - var som helst med valfri enhet
  - Microsoft Onedrive, Google Drive, Dropbox, m.fl.

En sista påminnelse!

Det allra bästa skyddet är ***din egen kunskap***

- Håll alltid dator och program uppdaterade!
- Var försiktig och uppmärksam på e-post och telefonsamtal!
- Var försiktig när du surfar!
- Glöm inte att säkerhetskopiera viktiga filer/foton!
- Var försiktig med sånt som är ”*för bra för att vara sant*”!

...och klicka aldrig på sådana här ”erbjudanden”!

Malware – ett samlingsbegrepp

Sabotageprogram, **skadeprogram**, **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.

Sabotageprogrammen kan klassificeras enligt hur de sprider sig, vad de gör eller någon annan aspekt:

- Virus – Sprider sig till filer lagrade på den infekterade datorn och följer med infekterade filer när de överförs till andra datorer.
- Mask/Worm – Sprider sig via datornätverk mellan datorer.
- Trojansk häst/Trojan – Utger sig för att göra en sak, men utför andra saker vanligen dolda för en användare, till exempel nedladdning av spionprogram.
- Logisk bomb - Utför en (skadlig) handling under speciella villkor, till exempel på ett visst datum.
- Spionprogram/Spyware – Spionerar på privat information och skickar informationen över internet.
- Annonsprogram/Adware – Visar annonser på infekterade datorer.
- Keylogger – Registrerar information om de tangenter som trycks på datorn, till exempel lösenord, och lagrar informationen lokalt för senare åtkomst eller skickar den via internet.
- Bakdörr/Backdoor – möjliggör åtkomst till datorn förbi de normala säkerhetskontrollerna.
- Ratware – kod som används för att skapa massutskick av skräppost över Internet.
- Utpressningsprogram/Ransomware – Hindrar användaren att använda datorn tills en lösensumma betalats.

Framtidens mobiltelefoner?

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

Nu är det slut!