Datorsäkerhet

Skydd mot bedrägerier.

Lars Forsmark

Seniornet Bromma/Kungsholmen

SeniorNet Sweden

Bilder från informationsträff kring IT-säkerhet den 22 nov 2022 i Abrahamsbergskyrkan

- Exempel på bedrägeriförsök
- Hur du kan skydda dig
- *(Lars har använt sitt eget förnamn i kommande exempel)*

Brev från din hjälpbehövande vän (??)

- Hej Lars!
  Länge sen vi sågs!
  Nu har jag råkat illa ut och behöver din hjälp snabbt!
  Jag turistar i Nigeria. Jag har blivit rånad och bor nu hos en snäll polis. Om du kan vara snäll och sända 8.000kr till mig via hans bankkonto nr 98797897987999, så kan jag komma hem snart.
  Stort tack för din hjälp!

  Din tillgivne gamle vän
  Leopold Lunkentuss

1. Samtal från utlandsnummer

- Om du blir uppringd från ett utländskt telefonnummer, svara inte om du inte förväntar dig ett samtal.

  Om du har ett missat samtal som inleds med ett utlandsnummer bör du inte heller ringa upp.

  Samtalet är troligen ett bedrägeri och du riskerar att bli av med stora summor pengar.

Falsk uppringare (utlandsnummer?)

- **Så skyddar du dig:**
- Lägg helt enkelt på luren.
- Ställ dig frågan om det är troligt att ett stort it-företag ringer runt och erbjuder support? Vid minsta osäkerhet, be om personens namn och be att få ringa tillbaka senare.
- Skulle du ändå ha följt instruktionerna, betala absolut inga pengar.
- Koppla bort datorn från nätet. Ta hjälp av en expert som kan undersöka om något skadligt har installerats på din dator.

- Obs! Blockera numret som ringde!

Vanliga bedrägeriförsök:
2. 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 eller bilagor i den här typen av mejl.
- Den här typen av bedrägeri kallas för phishing eller nätfiske.

Vanliga bedrägeriförsök:

2a. Falskmejl om att du har betalt för mycket och har rätt till återbetalning från Telia, Blocket, IKEA, etc.

- **Scenario:** Du får ett mejl (eller SMS) om att du är berättigad till återbetalning och avsändaren påstår sig vara t.ex. ett företag.
- Avsändarens mejladress ser ut att vara företagets med rätt logga. Du blir ombedd att klicka på en länk som ser ut att gå till företaget.
- **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 eller bilagor i den här typen av mejl.
- Den här typen av bedrägeri kallas för phishing eller nätfiske.

3. Samtal från ”Microsoft-supporten”

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

- Personen påstår att din dator är utsatt för virus eller liknande och att du riskerar att förlora alla 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.

Bedragarens mål är att:

- Få åtkomst till data som finns sparad på din dator, till exempel bilder, e-post, kontoinformation,

(3. forts.) ”Microsoftsupporten”

- **Bedragarens mål är att:**
- Få åtkomst till data som finns sparad på din dator, till exempel bilder, e-post, kontoinformation,
- ladda ner skadlig kod till din dator. Den gör att datorn kan kontrolleras på distans och att data du har sparat blir tillgänglig. Din dator kan dessutom bli en del av ett fjärrstyrt nätverk (botnet) som används för attacker mot mål på nätet,
- 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
- Obs! Blockera numret som ringde!

Låst dator

- **Scenario:** Du surfar på internet när det dyker upp ett meddelande från ”Rikspolisstyrelsen” på dataskärmen. Det går inte att stänga meddelandet. Varken tangentbord eller mus fungerar längre. I meddelandet står det att du begått ett brott på internet och att du måste betala en summa pengar för att datorn ska låsas upp igen.
- **Bedragarens mål är att:**
- Du ska tro att meddelandet kommer från Polisen och att du ska betala summan.
- **Så skyddar du dig:**
- Rimligt?? Polisen skickar aldrig ut personliga meddelanden till internetanvändare, i synnerhet inte när någon misstänkts för ett brott.
- Betala aldrig pengar till någon som kräver det via nätet om du inte beställt något eller ingått ett avtal!

Låst dator, forts.

Om din dator redan blivit låst, kontakta din IT-leverantör.

Läs på www.nomoreransom.org **i förväg!**
Se till att du regelbundet tar ”back-up” på dina viktiga filer, dokument och bilder. Lägg dem på en extern hårddisk, i molnet eller på ett USB-minne.
Obs! Låt inte USB-minnet sitta i jämnt, ty då blir ju även dess innehåll krypterat och otillgängligt om och när ”ransomware” anfaller!
Betala inte till utpressarna! Förfarandet brukar vara betalning via ”bitcoins”. Du har ingen garanti för att dina pengar kommer fram elller att du verkligen får tillbaka dina filer.

”Nigeria-brev”

- Dear Sir/Madam,

  Ditt namn har jag fått av en vän. Du är tydligen en person man kan lita på. Jag skriver till dig i största förtrolighet och ber dig respektera detta.
  Jag är dotter till den mördade general Zuzu från Togo. Min far efterlämnade en koffert med US$1000.000. För att föra ut dessa pengar ur mitt land behöver jag ha tillgång till ett utländskt bankkonto. Om jag får tillgång till ditt bankkonto så får du 10% (US$100.000) efter överföringen som tack för ditt besvär. Hör av dig på mail-adressen härnedan.
  Yours …

Presentkort från IKEA!

- Som god kund hos IKEA har du deltagit i vårt nya lotteri och vunnit presentkort för 5000 kr hos IKEA. Pengarna läggs in på ett IKEA-kort, som kan skickas till dig inom kort,

- Klicka bara på länken nedan och fyll i dina uppgifter, så kan du snart börja handla!

Du får en ny iPad 99 om du …

- Du blir uppringd ELLER en sida dyker upp som säger:
  Du får en ny iPad 99 för bara 99 kr om du svarar på följande frågor, det tar bara en liten stund! Fyll bara i dina kreditkortsuppgifter (eller bankkonto-).
- Efter någon dag har de dragit 99kr. Dessutom tackar de för att du beställt och nu är med i tjänsten XYZ, som ger dig många fina erbjudanden och bara kostar dig 350 kr – per månad, kanske i all evighet. ;-)
- Någon iPad dyker inte upp. ☹
- Att säga upp ”abonnemanget” är jättesvårt.

Bedrägerier med Bank-ID eller bankdosa

Hej Lars!
Jag ringer dig från din bank. Det är mycket viktigt!
Ditt kreditkort (-snummer) används nu i Tyskland för att ta ut pengar (eller köpa smycken). För att stoppa och korrigera det här behöver jag din hjälp nu genast! Hämta din bankdosa eller var beredd med ditt Bank-ID.

Bedrägerier med falska bankmän eller poliser

Hej Lars!
Jag ringer dig från din bank. Det är mycket viktigt!
Ett bedrägeriförsök pågår mot ditt kreditkort.
En person från banken kommer snart hem till dig och hämtar ditt kreditkort (bank-kort) och dina värdesaker så att vi får hjälpa dig att klara upp det här.

Obs! Bankpersonal eller poliser kommer aldrig hem till dig för att hämta ditt kreditkort (bank-kort) och dina värdesaker.

Vanliga bedrägeriförsök och vad du kan göra

- ”vishing” – från **v**oice **f**ishing. En person fiskar efter ditt bank-id och/eller dina bankkoder.

- Bedragaren ringer upp människor från ett fejkat telefonnummer som **ser ut** att komma från deras bank, och förmår dem att logga in med hjälp av sitt mobila bank-id, eller med sin bankdosa. När offret gör det sitter bedragaren beredd med en inloggning till bankens hemsida, vilket gör att det är hen som släpps in på kontot. På så vis kan de göra vilka överföringar de vill.

Vad du kan göra för att skydda dig

- Gå in på **Skatteverket.se** och anmäl att det bara ska vara möjligt att ändra din adress med hälp av legitimation eller Bank-ID.
- Läs på **adressändring.se**
  Välj ”Mitt adresslås”:
  Genom att låsa din adress hos oss kan du enkelt och kostnadsfritt skydda dig mot att någon obehörig adressändrar, lagrar eller eftersänder din post. Är din adress låst kan beställning enbart bekräftas med ditt BankID.

Skydd mot ”hackers” och virus

- Första försvarslinjen: Du själv!
- Klicka inte på länkar eller bilagor från okända avsändare! Om ett erbjudande verkar för bra för att vara sant så är det troligen inte sant!

Skydd mot ”hackers” och virus

- Första försvarslinjen: Du själv!
- Klicka inte på länkar eller bilagor från okända avsändare! Om ett erbjudande verkar för bra för att vara sant så är det troligen inte sant.
- Andra försvarslinjen: Antivirusprogram!
- Gratisprogram eller betalprogram; huvudsaken är att du har ett anti-virusprogram.
  Gratis: AVG Free edition.
  Betal: Norton, Panda, F-Secure, Bullguard.

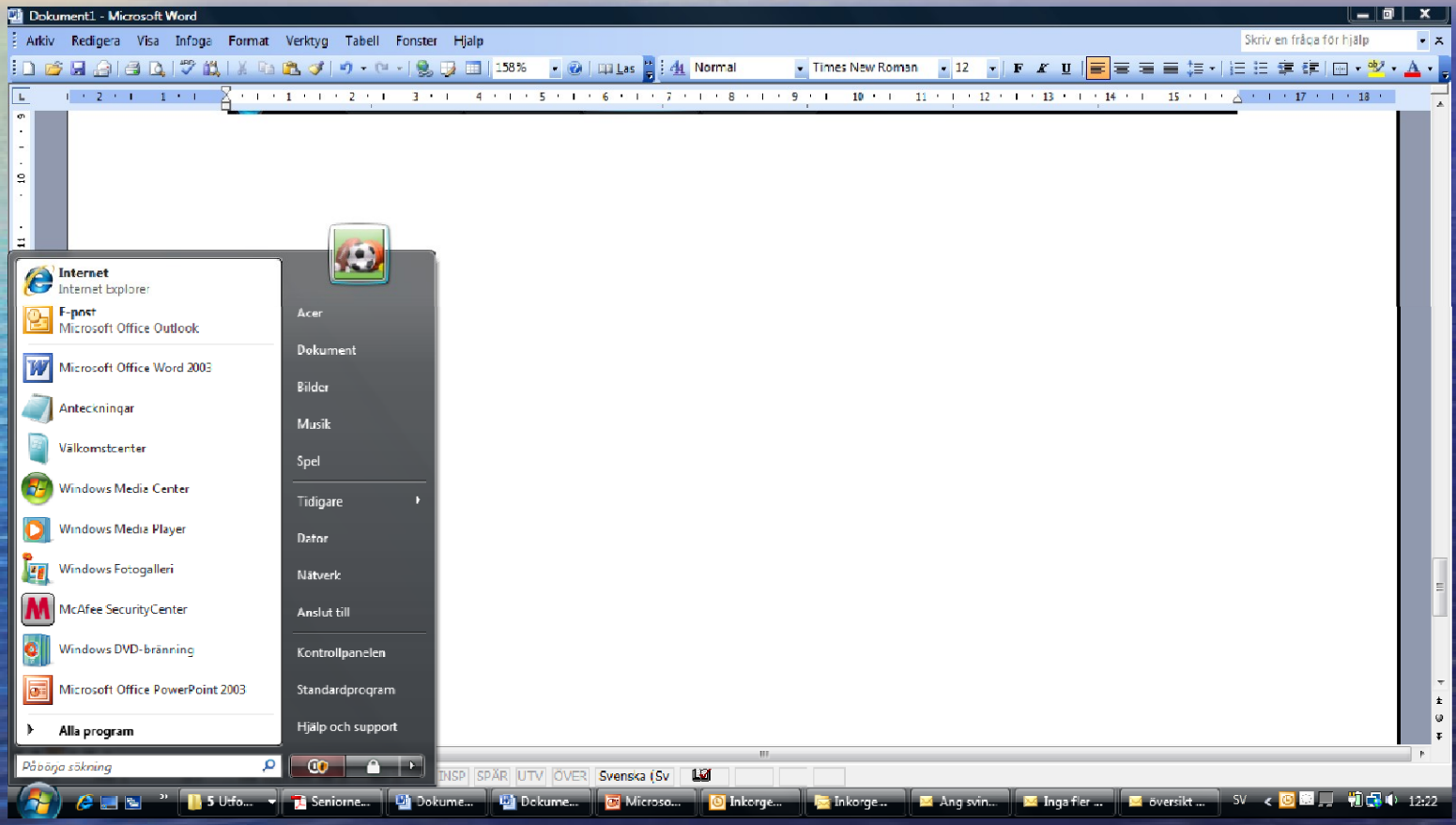
Skydd mot ”hackers” och virus

- Första försvarslinjen: Du själv!
  - Klicka inte på bilagor länkar från okända avsändare! Om ett erbjudande verkar för bra för att vara sant så är det troligen inte sant.
- Andra försvarslinjen: Antivirusprogram!
  - Gratisprogram eller betalprogram; huvudsaken är att du har ett anti-virusprogram. Gratis: AVG Free edition. Betal: Norton, Panda, F-Secure.
- Tredje försvarslinjen: Uppdatera!
  - Microsoft Windows uppdateras gratis, acceptera det! Gärna automatiskt!
  - Antivirusprogrammet skall uppdateras regelbundet!! Gärna automatiskt!

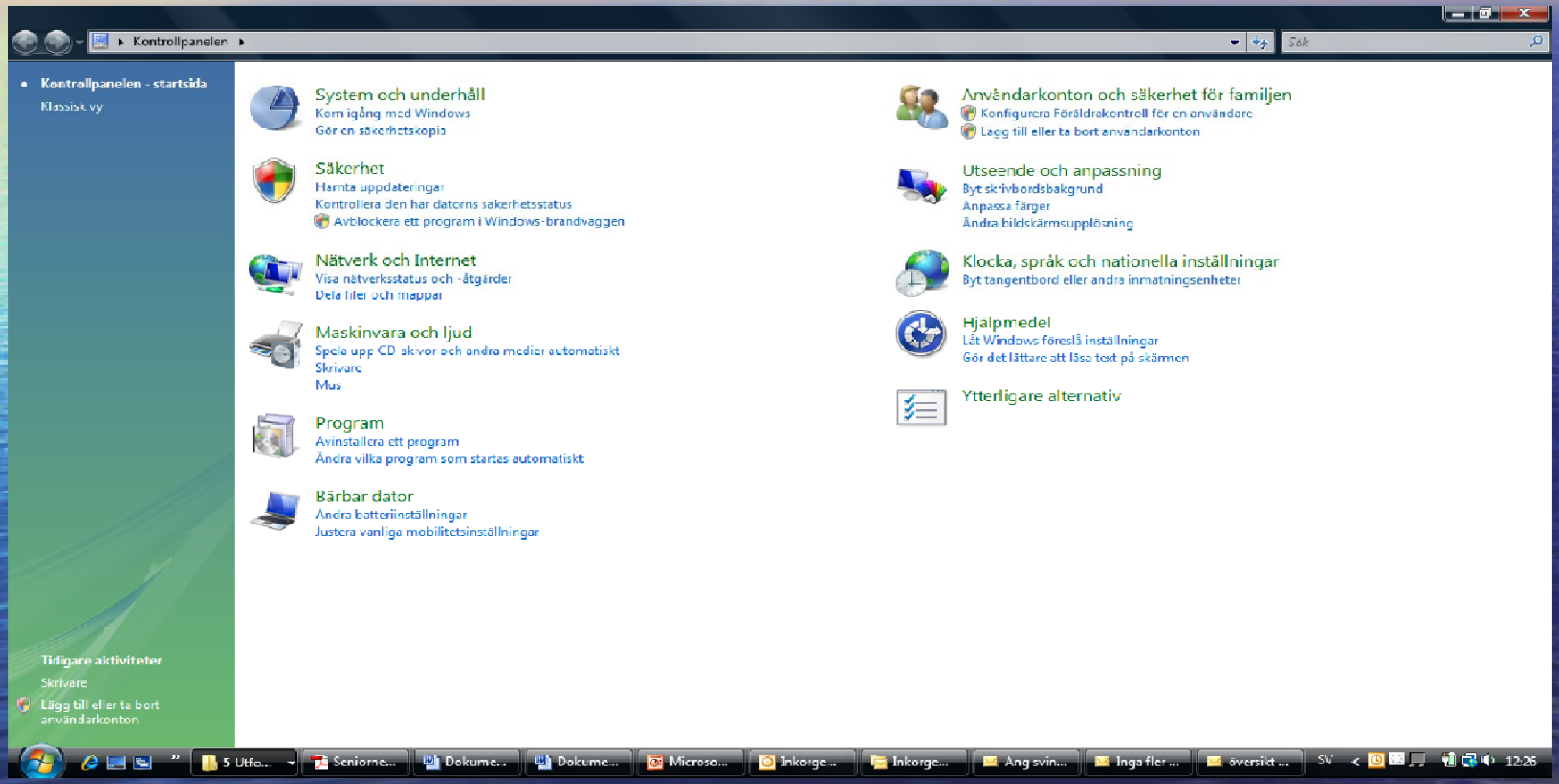
Bästa sättet att anmäla till polisen?

- Gå in på www.polisen.se och fyll i deras formulär! https://polisen.se/om-polisen/kontakt/polisens-adresser/ Ange t.ex. Region Stockholm!
- Ring 112 om akut pågående brott!
- Du kan ringa 11414, men du kanske blir sittande och får vänta i ett par timmar i värsta fall.
- Bättre att fylla i polis-sidans formulär. Då har du också anmält skriftligt. En skriftlig anmälan är bättre om det blir ett rättsligt efterspel!

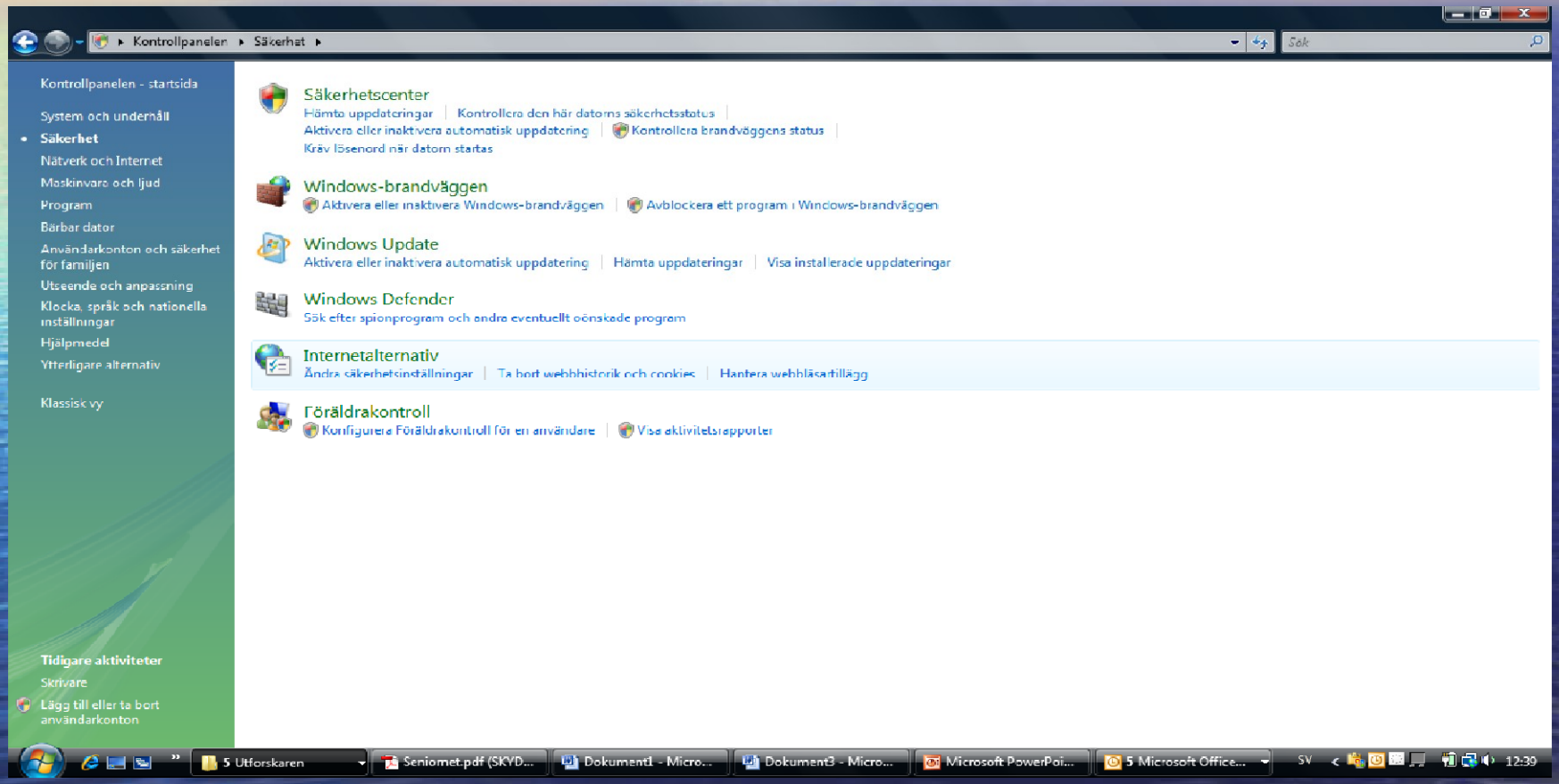
Hitta Inställningar, Kontrollpanelen



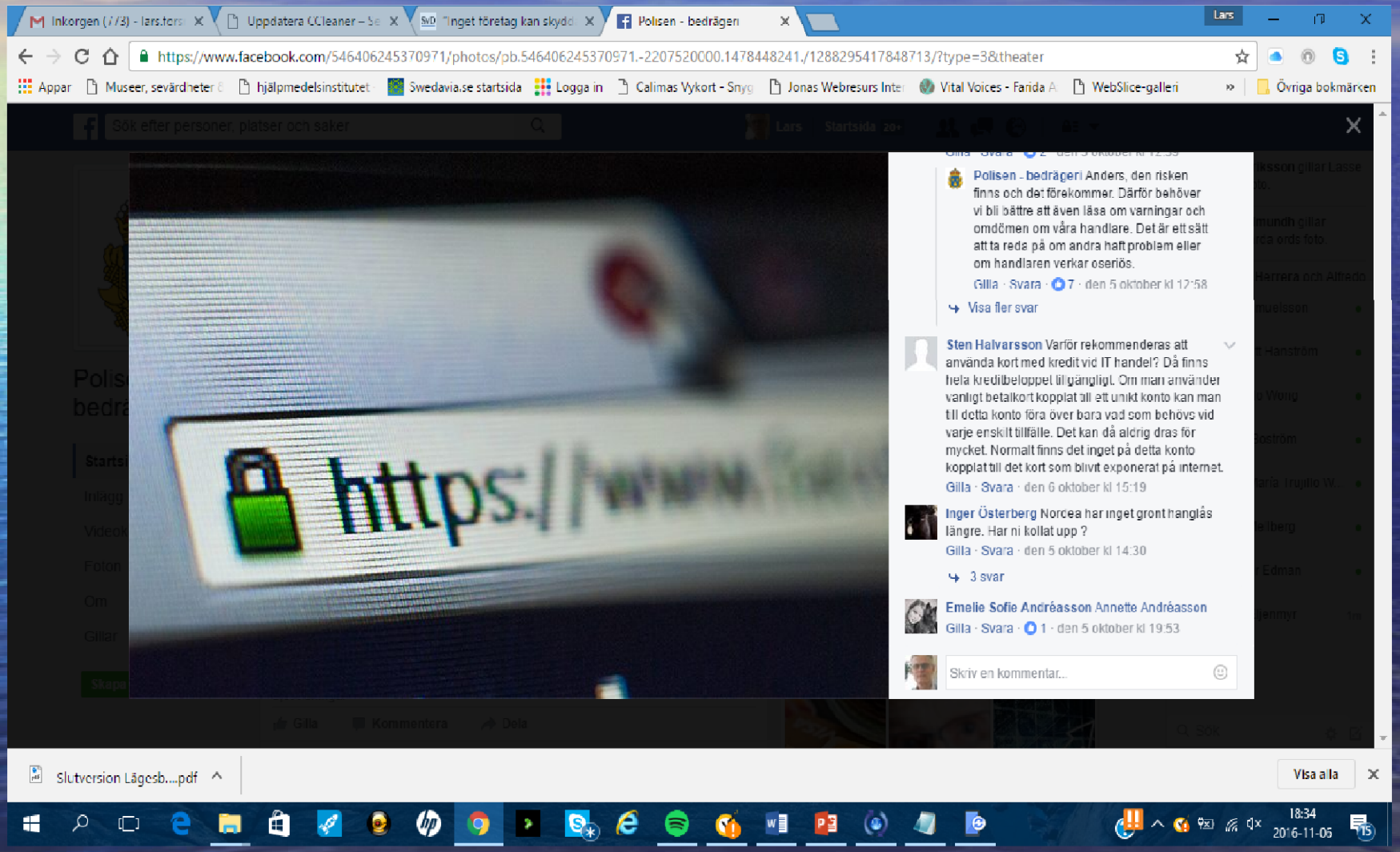
Hitta ”Säkerhet”, ”Status” i Kontrollpanelen/Inställningar



”Säkerhet” i Kontrollpanelen, leta upp **säkerhets-status** eller liknande.

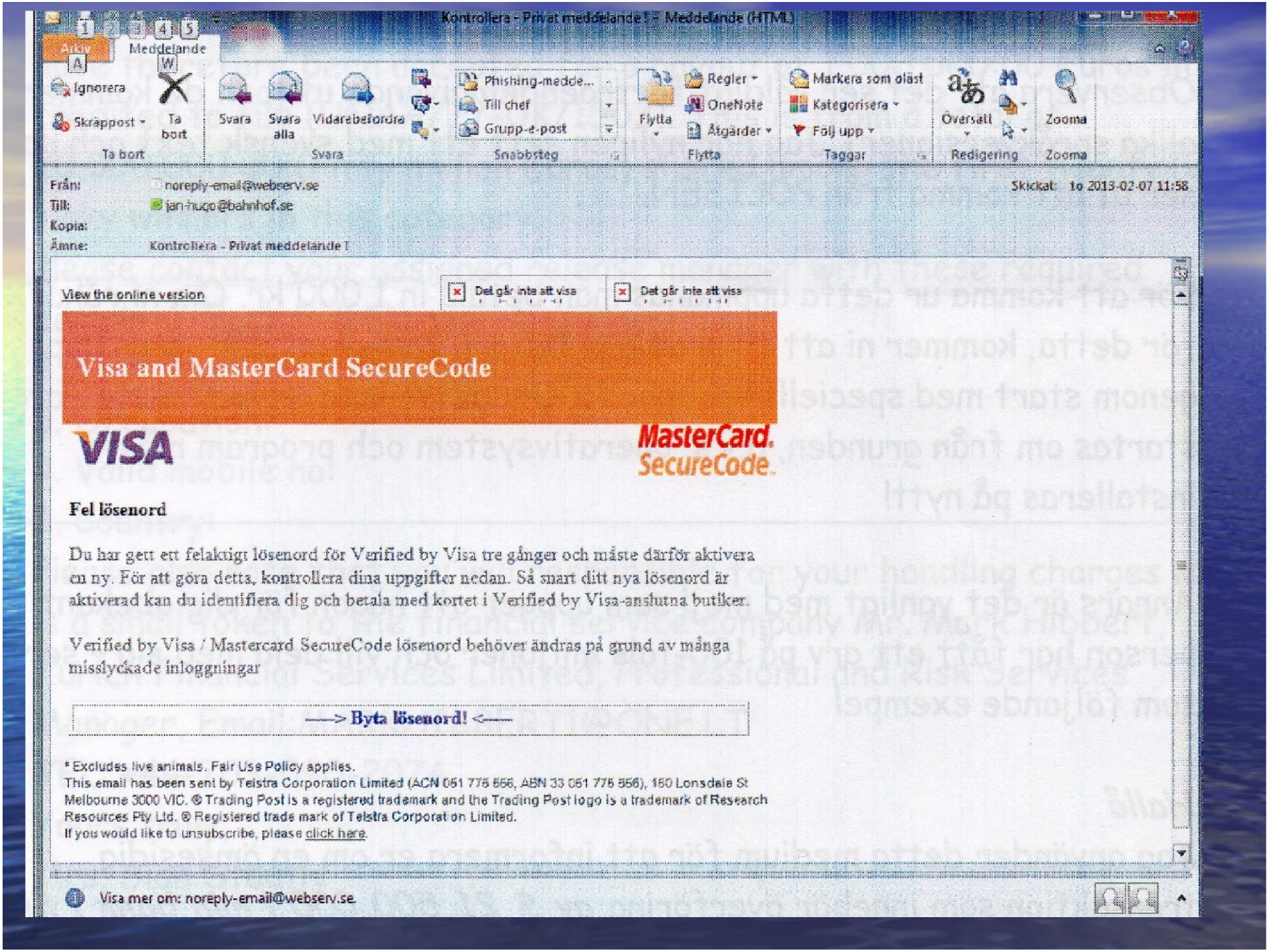


https://www.dinfinabank.se



ID-kapning, ID-stöld

- Bedragaren tar reda på ditt **personnummer** genom att söka i din brevlåda, eller i soprummet eller på nätet.
- Bedragaren tillverkar en falsk legitimation i ditt namn, ett falskt körkort ett falskt pass, ett falskt ID-kort.
- Bedragaren går till en annan bank än din och beställer ett Bank-ID i ditt namn. Banktjänstemannen märker inte att den legitimation som presenteras är falsk och inrättar därför ett Bank-ID i ditt namn.
- Bedragaren kan nu ta lån eller beställa varor i ditt namn och/eller ta ut pengar från dina konton i din bank, ändra din adress eller eftersända din post.


Kontrollera - Privat meddelande ! - Meddelande (HTML)
Arkiv
Meddelande
Ignorera
Skräppost
Ta bort
Svara
Svara alla
Vidarebefordra
Phishing-medde...
Till chef
Grupp-e-post
Regler
OneNote
Åtgärder
Flytta
Markera som oläst
Kategorisera
Följ upp
Översätt
Zooma
Ta bort
Svara
Snabbsteg
Flytta
Taggar
Redigering
Zooma
Från: noreply-email@webserv.se
Till: jan-hugo@bahnhof.se
Kopia:
Ämne: Kontrollera - Privat meddelande !
Skickat: to 2013-02-07 11:58
View the online version
Det går inte att visa
Det går inte att visa
Visa and MasterCard SecureCode
VISA
MasterCard SecureCode
Fel lösenord
Du har gett ett felaktigt lösenord för Verified by Visa tre gånger och måste därför aktivera en ny. För att göra detta, kontrollera dina uppgifter nedan. Så snart ditt nya lösenord är aktiverad kan du identifiera dig och betala med kortet i Verified by Visa-anslutna butiker.
Verified by Visa / Mastercard SecureCode lösenord behöver ändras på grund av många misslyckade inloggningar
----> Byta lösenord! <----
* Excludes live animals. Fair Use Policy applies.
This email has been sent by Telstra Corporation Limited (ACN 051 775 556, ABN 33 051 775 556), 160 Lonsdale St Melbourne 3000 VIC. ® Trading Post is a registered trademark and the Trading Post logo is a trademark of Research Resources Pty Ltd. ® Registered trade mark of Telstra Corporation Limited.
If you would like to unsubscribe, please click here.
Visa mer om: noreply-email@webserv.se

Lars Forsmark

Till: webupdating@email.ch
Ämne: SV: Din webmail kvot har · verskridit den fastst· llda kvoten som · r 2GB. du k· r p· 2,3 GB.

-----Ursprungligt meddelande-----
Från: COMHEM Admin / Webmaster / lokala värden [mailto:gunnareriksson@glocalnet.net]
Skickat: den 10 maj 2011 21:13
Till: undisclosed-recipients:
Ämne: Din webmail kvot har verskridit den fastst llda kvoten som r 2GB. du k r p 2,3 GB.

Din webmail kvot har överskridit den fastställda kvoten som är 2GB. du kör på 2,3 GB.
För att åter aktivera och öka din webmail kvot du kontrollera och uppdatera din webbmail konto
För återaktivera och öka din webmail kvot genom att sända nedan.

Fyll i och skicka följande information för kontroll
* Email Adress: .....
* Lösenord: .....
* Bekräfta lösenord: .....

Underlåtenhet att göra detta kan leda till en uppsägning av din webbmail konto.
Tack, och om ursäkt för besväret
Comhem Admin / Webmaster / lokala värde

Varning för konstiga meddelanden!

”Kära Kontrollera med Visa / Mastercard SecureCode medlem

Du har ett privat meddelande!

Klicka här för att läsa meddelandet
http://aussietrackers.org/update.php ”

Detta är ett typexempel på ett meddelande som inte kommer från den/det företag som nämns i texten

VARFÖR, skulle en bank, ett kontokortföretag skicka epost med en länk till något som är mig fullständigt främmande? VAD ÄR AUSSIETRACKER.ORG?

Läs hjälp- och supportsidan!

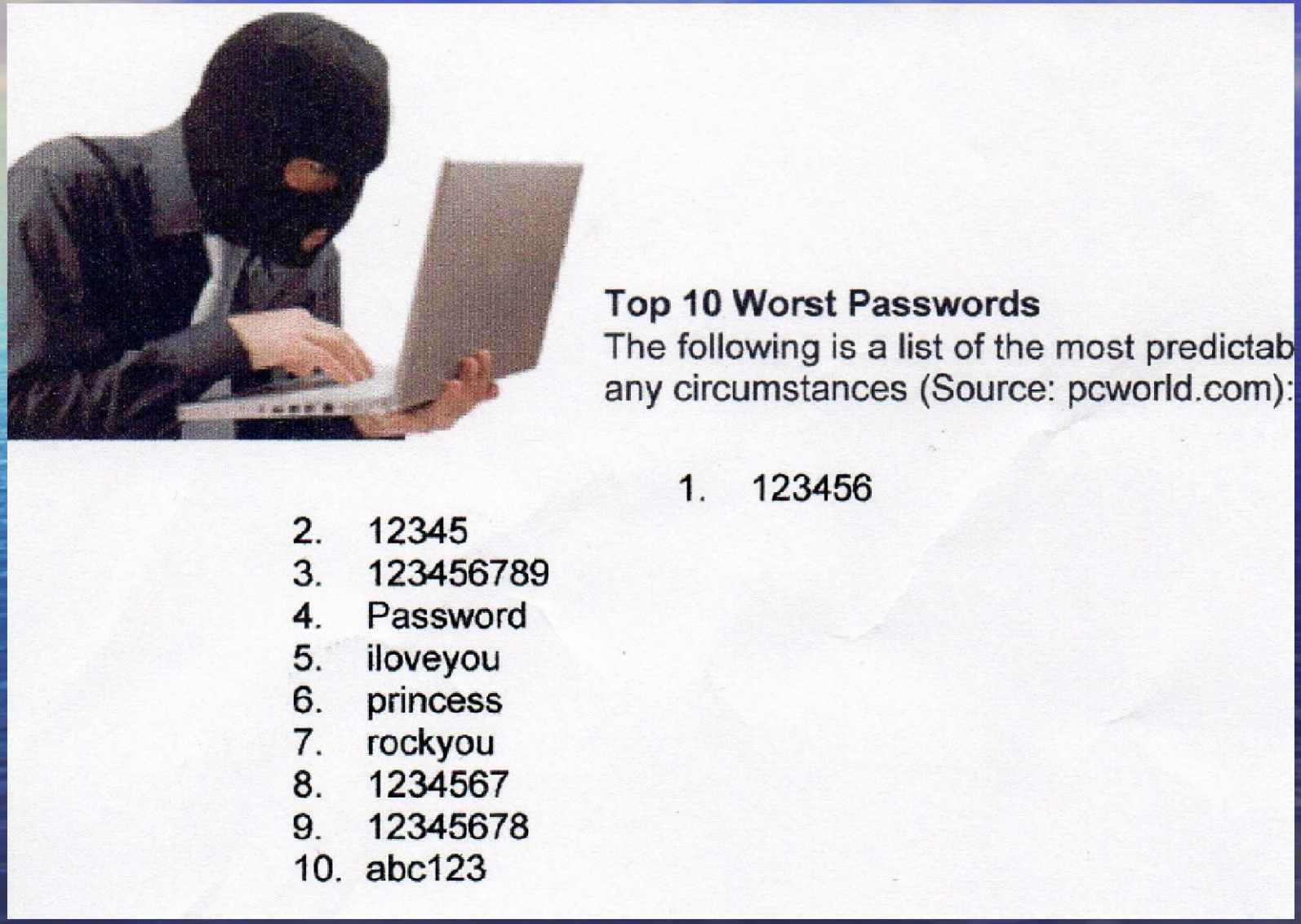
Om du får epost av denna typ – ta bort meddelandet omgående!!! Klicka under inga omständigheter på ”länken”
– om du gör så kommer förmodligen ett ”spionprogram” att installeras på din dator, som sedan skickar information om dig till någon som vill åt dina privata uppgifter

En bank/kontoföretag kontaktar aldrig sina kunder på detta sätt – vill de att du ska göra något för att skydda dig – kommer du att få ett brev, alternativt läsa på deras hemsida, då du gör ex. betalningar att de utsatts för någon forma av bedrägeri och de vill i så fall att du byter kort – men att du gör det vid ett personligt besök på banken

Vad du själv kan göra för att skydda dig

- Lämna inte ut ditt personnummer utan att veta vad det kommer att användas till. Födelsedatum räcker oftast.
- Håll koll på din post t.ex. bekräftelse om adressändring eller t.ex. Postnord: ”Paketet du beställt kan hämtas nu”, om du faktiskt inte beställt något.
- Byt till låsbar brevlåda (om du har brevlåda utomhus).
- Skriv inte om din resa på Facebook, etc.
- Om du tappat bort en ID-handling så anmäl till polisen och kreditupplysningföretagen och till Transportstyrelsen om du förlorat ditt körkort.
- Kolla dina kontobesked! Har DU gjort alla köpen?

Dåliga lösenord



Top 10 Worst Passwords

The following is a list of the most predictab
any circumstances (Source: pcworld.com):

1. 123456
2. 12345
3. 123456789
4. Password
5. iloveyou
6. princess
7. rockyou
8. 1234567
9. 12345678
10. abc123

Lösenord

- Minst 8 tecken,
  blanda stora och små bokstäver,
  siffror och specialtecken, t.ex. * &
- sdlvu*41Z
- blsd39*hjuvdR
- jvgdonkB&37

Lösenord, forts.

- sdlvu*41Z
  sov **d**u **l**illa **v**ide **u**ng *41 Z
- blsd39*hjuvdR
  blinka lilla stjärna där 39* hur jag undrar var du ärrrrR
- jvgdonkB&37
- ja visst gör det ont när knoppar brister & 37

Lösenord, forts.

- Obs!
  När du hittar på eller skriver in lösenord är det viktigt att hålla reda på STORA och små bokstäver. Kolla att ”Caps lock” inte är påslagen/nedtryckt. Den funktionen ger STORA bokstäver. (På gamla skrivmaskiner heter den tangenten ”Skiftlås”.)
  Obs! Aldrig mellanrum (eller å, ä, ö, ü, é) i lösenord!

Varning för falska samtal - skydda dina koder och BankID

Det finns bedragare som utger sig ringa från t. ex. banken eller en myndighet. Tänk på:

- Lämna aldrig ut några koder eller annan känslig information.

- Använd aldrig din kortläsare, bankdosa eller Mobilt BankID på uppmaning av någon annan oavsett orsak.

Varningar, forts.

- - Logga aldrig in på Internet- eller Mobilbanken på uppmaning av någon annan.
- - Lägg på luren om någon ringer och ber dig göra något av ovanstående. Är du minsta osäker, ring (eller mejla) din banks kundservice.
- - Lägg på luren om någon ringer och ber dig göra något av ovanstående. Är du det minsta osäker, ring Nordeas kundservice 0771 – 22 44 88, öppet alla dagar 08-20.

Hjälp- och support!

- MSB – Myndigheten för Samhällsskydd och Beredskap www.msb.seMSB – Myndigheten för Samhällsskydd och Beredskap www.msb.se och www.dinsakerhet.se
- www.polisen.se eller mobil.polisen.se Tel.: 114 14 www.bra.se Brottsförebyggande Rådet
- NBC – Nationellt Bedrägericentrum (Polisen) Facebook Windows hjälp- och supportsida finner du under Start eller Windows-knappen eller ”Sök” och Hjälp!
- **Seniornets** medlemssidor, **Datorbiten** inom **Forum**.
- www.fi.se Finansinspektionen, för tips om bedrägliga (finans)firmor.
  Tidningen PC för alla på bibl. el. https://pcforalla.idg.se/

Hjälp- och support, forts.!

- www.bestrid.nu för att bestrida misstänkta fakturor.
- www.nomoreransom.org om utpressningsvirus.
- Seniornets medlemssidor, **Datorbiten** inom **Forum**.
- www.fi.se för tips om bedrägliga (finans)firmor.
- Internetkunskap.se
  Tänk säkert
- Boktips: ”Bara bluff”, S. Ardelius, G. K. Näslund, 2018, förlag Kärnhuset.
- Lycka till!

Hjälp- och support, forts.!

Lycka till!
Efter bedrägliga/oönskade telefonsamtal, blockera numret som ringde upp. På så sätt slipper du ytterligare samtal från det numret. Detta bör du göra varje gång du får ett nytt oönskat samtal.

Hjälp- och support, forts.!

Om du vill ringa polisen, kom ihåg att du kan få vänta väldigt länge!

Ett bra tips:
Använd denna kontaktväg in till polisen via e-post och kontaktformulär.

https://polisen.se/om-polisen/kontakt/polisens-adresser/

- välj polisregion Stockholm

Trick vid Bankomaten!

Om din mobiltelefon blir stulen: *#06#

Checklista – klipp ut och lägg i plånboken!

- ☐ Börja med att ringa telefonen. Någon kan ha hittat den.
- ☐ Använd telefonens lokaliseringsfunktion för att se var den är.
- ☐ Om det inte går – försök radera den på distans. (För du har väl löpande gjort säkerhetskopior?)
- ☐ Ring polisen på 114 14 och gör en anmälan. (Är det ett rån ringer du förstås 112).
- ☐ Byt för säkerhets skull lösenord till ditt mejl-konto, tjänster för lagring, Facebook osv.
- ☐ Mitt IMEI-nummer är: _____
- ☐ Ring och spärra sim-kortet och mobilen hos operatören. Telefonnummer (se sid 59):