

Nyfiken på Internetsäkerhet



Bild från syspeace.com

Detta är dagens minsta textstorlek.

En presentation av och med Johan Murray



Vad tar vi upp idag?

Del 1 13:30 – 14:15

- Internet – en revolution
- Hur vanligt är det med problem?
- Försiktighet, lika viktigt nu som alltid
- Vilka skydd finns det?
- Familjen Gladsurf presenteras

Del 2 14:45 – 15:30

- Praktiska exempel på faror
- Några pekpinningar
- Framtiden med Internet of Things
- Frågor
- Avslutning

Hela presentationen går att ladda ner från och med i morgon, från <http://snso.se/datatrafvar/>

Internet revolutionerar världen

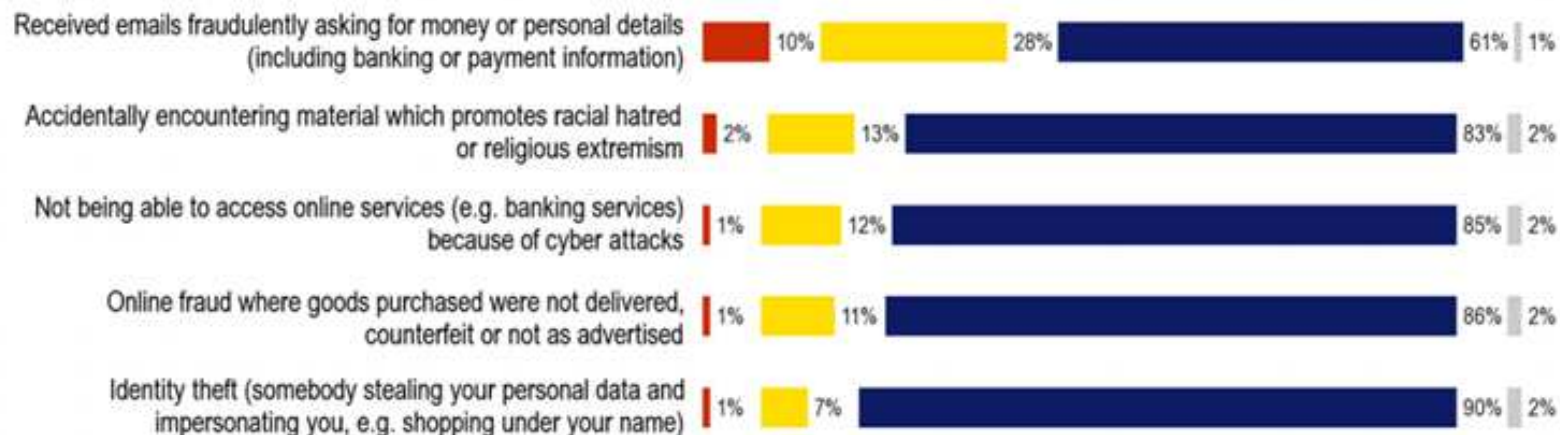


	Fördelar
Handel	Små och stora företag kan erbjuda sitt utbud över hela världen.
Utbildning	Alla får tillgång till en oerhörd mängd fakta. Billig utbildning med hög kvalitet (MOOC)
Arbete	Distansarbete, Vobb Nya kvalificerade yrken
Socialt	Spel och kontakter med släkt, vänner och likasinnade över hela världen genom sociala medier Global omtänksamhet
Sammantaget	Enorm val- och yttrandefrihet Avstånd betydelselöst

Vad upplever man som problem?



QE10. Cybercrimes can include many different types of criminal activity. How often have you experienced or been a victim of the following situations?



Bedräglig e-post

Rasism

Otillgänglighet

Bedräglig handel

ID-stöld

Ofta

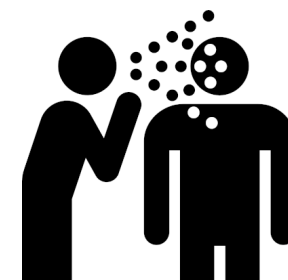
Ibland

Aldrig

Vet ej

Ur EU-rapport om nätsäkerhet från 2012. Ca 1000 utfrågade per land. Ej begränsat till senaste året.

Enligt SCB drabbades 17 % i åldrarna 16-85 av virus/datorinfektion under 2014-5



Är det farligt? – Nej, inte om man aktar sig!

- Förebyggande vård är bättre än kirurgiska ingrepp....
- Har man inget riskbeteende blir man bara utsatt för de hot och smittor som finns i det egna språkområdet och kulturen.
- De riktas ofta mot någon viss målgrupp, sällan svenska pensionärer (Rika, politiska motståndare, industrin, forskare, ungdomar....)
- Ändå skräms vi ofta av media, och det kanske är nödvändigt för att bibehålla försiktigheten

Säkerhetstrender

- Våra datorer blir (med Antivirus) allt bättre på att skydda sig själva
- Vi blir allt mer utsatta för påverkan
- IT-företagen växer och blir mer sociala och lika, men läcker...
- Vi får allt fler smarta IT-prylar i hela samhället som till en början är osäkra

Hur kan man då akta sig själv?

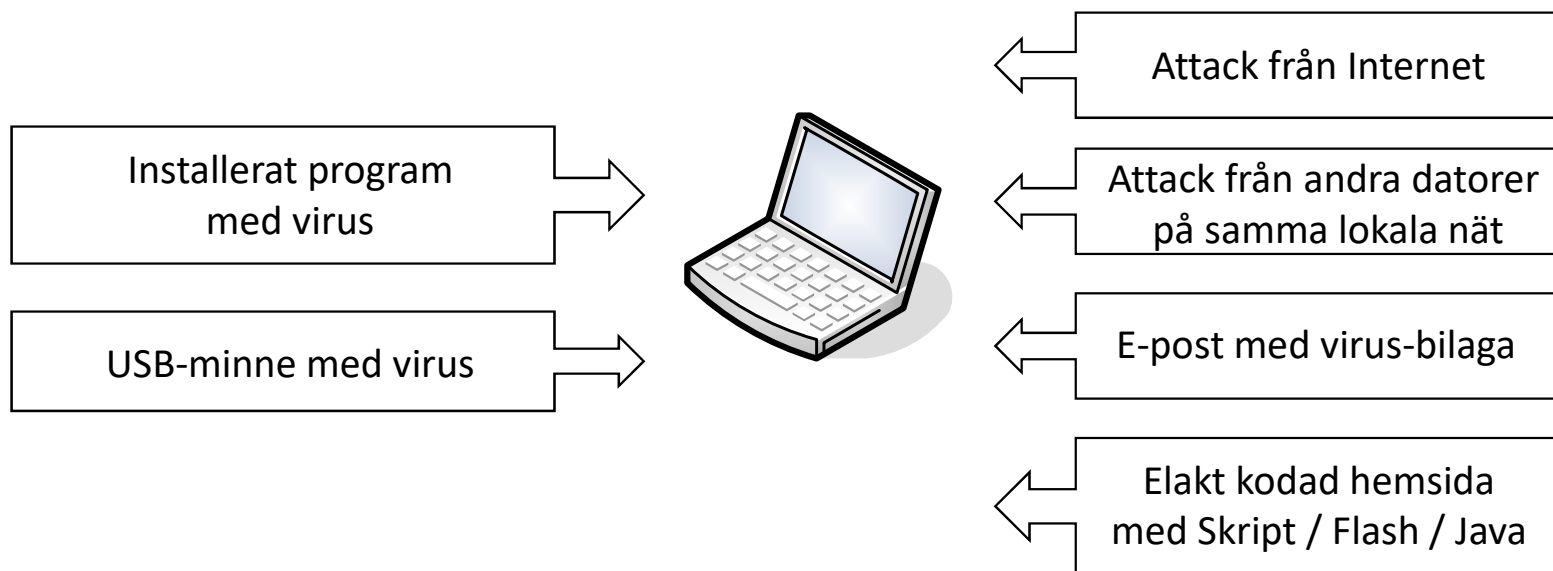


- Människor ligger bakom allt som finns på Internet
- Man får själv bedöma anseendet på dem man umgås med och deras avsikter
- Trovärdigt innehåll duger inte som grund för bedömningen

Förtroendeskapande hjälpmedel på Internet:

- + Oberoende omdömen (Googla!)
- + Elektroniska legitimationer (certifikat)
- + Antal följare och gillanden i sociala medier
- + Webbläsares och Antivirus svarta listor över hemsidor
- + Myndigheters (ARN, Bolagsverket) och pressens svarta listor över företag

Hur kan en dator "akta sig"?



Skydd:

- Brandväggar
- Antivirus
- Uppdateringar
- Sandlådor
- och ändå flera sätt

Datorskydd – Brandväggar



- Måste finnas närmast Internet för att stoppa olämplig inkommande datatrafik.
- Ska inte kunna konfigureras om av andra än ägaren.
- Fungerar bra. Gör att skurkarna använder andra metoder för att ta sig in.
- Är ett absolut nödvändigt program i datorn om man har mobilt bredband.
- I antiviruspaketen ingår ofta ett brandväggsprogram.
- Windows 10 levereras med en bra brandvägg, men som har ett dåligt användargränssnitt.

Datorskydd – Uppdateringar



- Hackare utnyttjar kryphål i datorns alla Internet-program
- Uppdateringar täpper till och minskar avsevärt risken att bli drabbad av intrång
- Men, hackarna ger ändå inte upp

- Mängden och storleken på uppdateringarna har blivit ett problem för att vi vänjer oss vid att datorn ibland har "annat för sig"
- Självuppdaterande program testas inte alls lika hårt före släpp som andra program

Datorskydd – Antiviruspaket

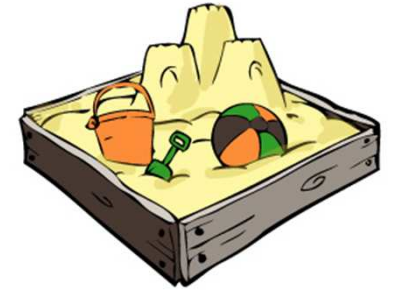


- Ska hindra virusfiler från att skada datorn, men gör även annat.
- Klarar i bästa fall 90% av alla kända virus, *men inga alldeles nya*.
- Det enda sättet att upptäcka att man blir smittad innan det är för sent.
- Engelska Wikipedia har en bra översikt över vad olika Antiviruspaket kan https://en.wikipedia.org/wiki/Comparison_of_antivirus_software

- Inte så fantastiskt säkra som reklamen för Antiviruspaketen påstår.
Likaså överdrivs ofta farorna.
- *En uppdaterad dator med bra antivirus hos en försiktig surfare blir sällan skadad.*

- Windows 10 levereras med ett enkelt antivirusskydd: Windows Defender.
- I Windows kollas dessutom datorn varje månad med Microsoft Malicious Software Removal Tool som ingår i Windows Update.

Datorskydd – Sandlådor



- Ska hindra elaka hemsidor från att skada datorn, men hindrar dem inte från att läsa/stjäla användarens privata filer. Det finns ju hemsidor som kan leta efter virus i datorn!
- Sandlådor kan ställa frågor om hemsidor försöker bete sig "dumt"!
- Sandlådor ingår i webbläsarna.
- Chrome har bäst sandlåda, Edge ligger inte långt efter.
- *Internet Explorer har en riktigt riktigt dålig sandlåda.*
- E-postläsarprogram har inga sandlådor, så e-post i hemsidesformat och bilagor kan skada datorn, men det finns hjälp mot det...



Eget skydd – Sund misstänksamhet

Källkritiskhet är ingen naturlig förmåga, den får man lära sig

Läs gärna "Källkritik på Internet" från Internetstiftelsen (iis.se)

När man får information:

- Är avsändaren pålitlig? (kolla ryktet)
- Stämmer avsändaren? (kolla språket)
- Varför kommer informationen just till mig?
- Om det är verkar (text i bilder-länka ...magor-ziparkiv ...)
- Går innehållet att bekräfta? (För bra/hemskt för att vara sant?)
- Är det fortfarande aktuellt?

Innan man lämnar ut information:

- Kan jag lita på att mottagaren hanterar informationen väl? (kolla vilken mottagare?) (kolla språket, finns kontaktuppgifter)
- Är formuläret professionell ut?
- Varför behöver just jag lämna ut denna information?
- Till vad behövs alla de uppgifter som efterfrågas?
- Är det någon mer uppgift som borde varit med?
- Blir känsliga uppgifter skyddade av kryptering? (https:// eller hänglås)

Vi går igenom detta efter pausen!



Adresser på Internet, URL:er

organisation land
sodermalm.seniornet.se/kanelbullen
avdelning domän kategori

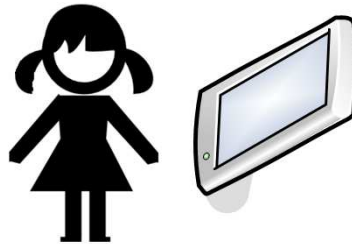
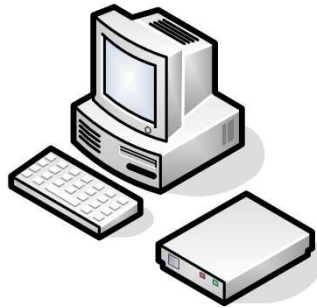
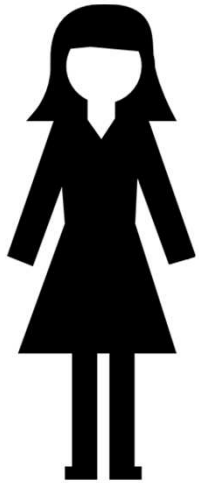
http:// betyder överföring "i klartext", föredras av skurkar

https://
hänglås betyder krypterad överföring med certifikat

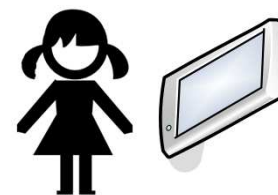
Så, vad betyder det här?

<http://www.citibank.com:ac=piUq3027qcHw003nfuJ2@sd96V.plsEm.NeT/3/?3X6CMW2I2uPOVQW>

Familjen Gladsurf



Tas upp vid något annat tillfälle....



Mirandas värld: Barnvänlighet

Föräldrakontroll (skyddar mot vuxet material och överanvändning)

- Man anger tillåtna hemsidor i Webbläsarna och blockerar otillåtna appar
- Omständligt att sköta, lätt att gå runt, bäst att vara med när barnet surfar
- Alternativ: NetNanny, en speciell webbläsare som kostar pengar
- Man behöver också kolla att Google har "Safe search" inställt

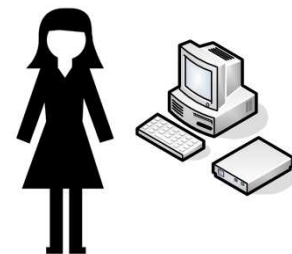
IPad visar inte video med Adobe Flash Player, som är urdålig

Year	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	½2016
# of Flash Vulnerabilities	1	5	10	21	20	60	63	66	56	76	314	200

Hennes MP3-spelare (USB-minnet) är "vaccinerad"

- Då kan den inte sprida virus bara genom att anslutas till en dator

Gunillas värld: Farliga nerladdningar

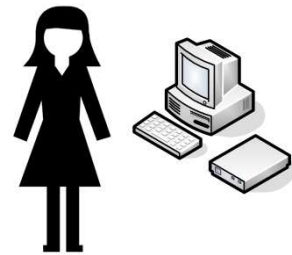


A composite screenshot illustrating a security risk. On the left, a Bing search for 'chrome download' shows a result for 'Google Chrome | Google Chrome Download' with a red arrow pointing to it from the text 'Example of malicious site for downloading legitimate software'. On the right, a Facebook interface is overlaid with a download progress window for 'setup.exe from 75.253.133.137' and a 'Security Warning' dialog box from Internet Explorer stating 'The publisher could not be verified. Are you sure you want to run this software?' with 'Name: setup.exe' and 'Publisher: Unknown Publisher'.

Ladda bara ner mjukvara *direkt* från respektabla tillverkares hemsidor!!!!
Annars kan man få virus "på köpet".

Falsk hjälpsamhet ska man passa sig för!

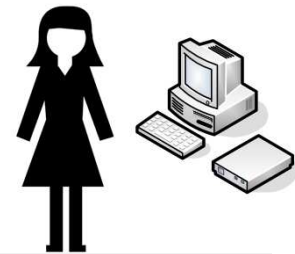
Gunillas värld: Farliga nerladdningar



The screenshot shows the CNET Download.com website for WinRAR (64-bit). The top navigation bar includes the CNET logo, a search bar, and links for Reviews, News, Download, CNET TV, How To, and Marketplace. A prominent green banner at the top of the page reads "3 steps for a faster PC" with a "Start Download" button. Below this, the breadcrumb trail is: Home > Windows Software > Utilities & Operating Systems > File Compression > WinRAR (64-bit). The main heading is "WinRAR (64-bit)" with a "Download Now" button. To the left, there are two rating sections: "CNET Editors' Rating" with five red stars and the word "Spectacular", and "Average User Rating" with five blue stars and "out of 126 votes". The main text describes WinRAR as a lightweight, flexible, and easy-to-use archiving utility. To the right, there is another "3 steps for a faster install & scan" banner with a "Start Download" button and a list of steps: 1. Start Download, 2. Run the quick scan, 3. Fix up to 100 Registry Issues. Below this, there are two award logos: "A top 10 utility on Download.com" and "ARO® 2012". At the bottom, there is an "Ads" section with a "Download Free" link and a link to "Free FLV Player Download Here!".

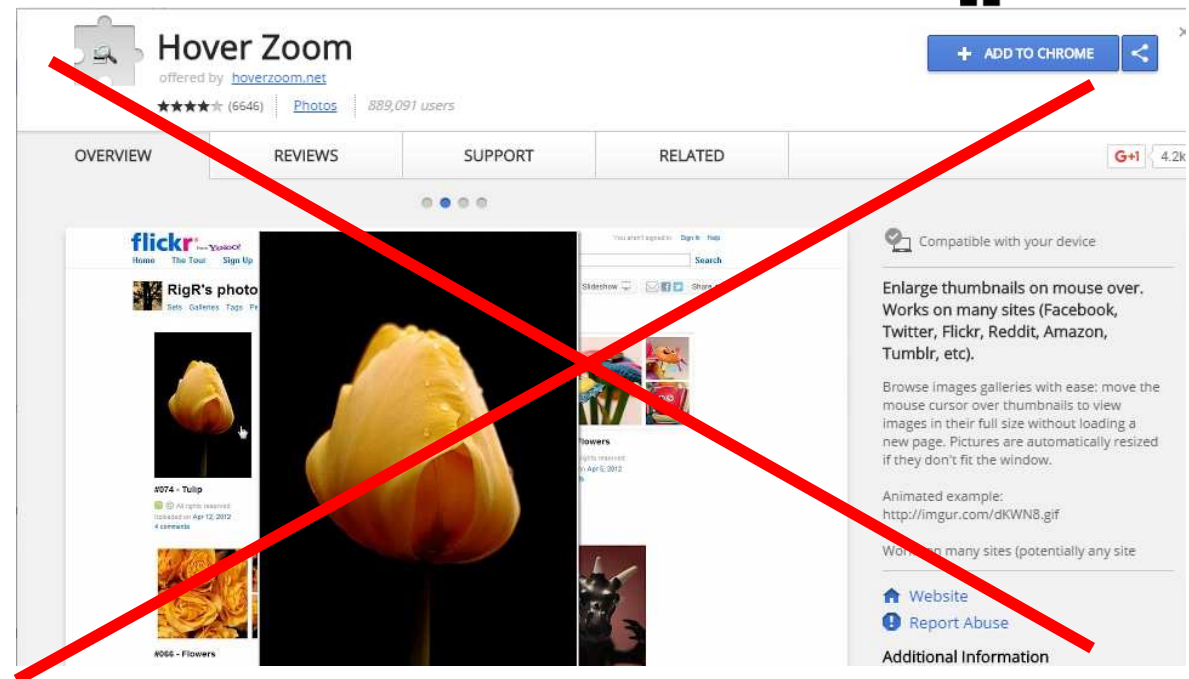
Det är inte alltid så lätt att klicka rätt! Sväva över länkar för att se vart de går!
Har man installerat virus krävs krafttag för att få datorn ren igen.

Gunillas värld: Webbbläsartillägg-spioner



Gör hemsidor snyggare och skadar inte datorn, men...

- ser och kan ändra allt vad man gör i webb-läsaren och kan dessutom skvallra om det
- kan lägga till vad som helst på hemsidan innan den visas
- kan vara snällt först, och bli styggt genom uppdatering

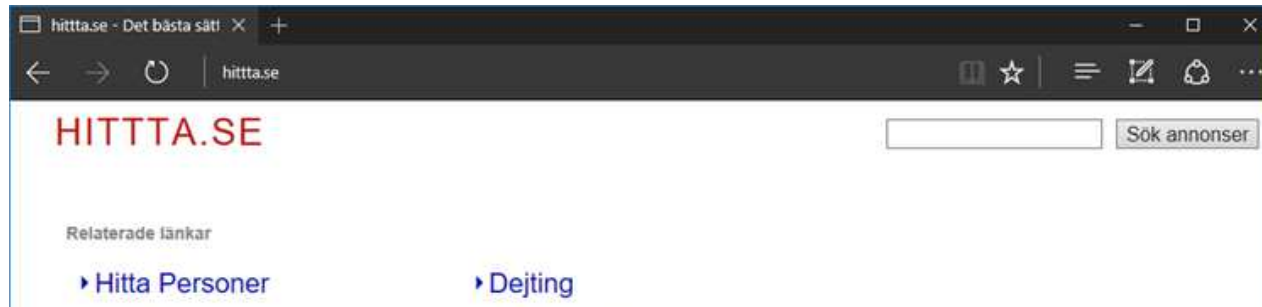
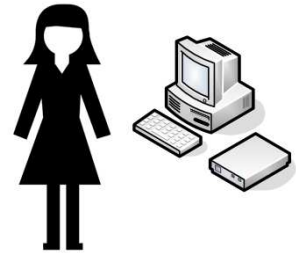


Man behöver köra anti-spion-program för att bli kvitt dessa, och sådana ingår i en del Antiviruspaket.

PAUS
till 14:45



Gunillas värld: Farliga hemsidor

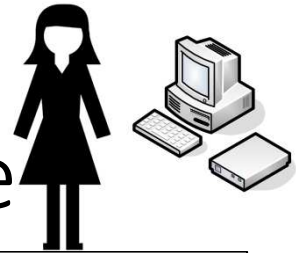


- Man kan nå dem av misstag, eller om man har ljusskygga vanor.
- De kan också locka med kändisskvaller eller något annat populärt.
- Farligheter kan finnas på högst respektabla hemsidor som tillfälliga annonser.

- Hemsidor kan undersöka om datorn är möjlig att bryta sig in i, utifrån.
- De kan undersöka (och stjäla) nästan alla datorns filer.
- De kan skrämmas med fasansfulla (men osanna) meddelanden (sällan på svenska).
Stäng webbläsaren så försvinner meddelandena.

Är man osäker kan man kolla hemsidan på safeweb.norton.com, men det bästa är om man aldrig ens kommer fram till farliga sidor.

Gunillas värld: Hemsidor med dåligt rykte



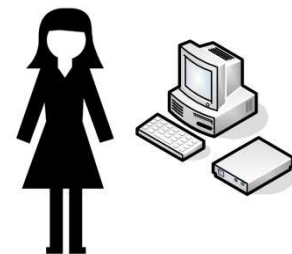
Det finns hjälp:

- Några Antivirus markerar ökända länkar med en röd signal. Grön *ej* = OK!
- Flera webbläsare blockerar länkar: Edge och IE har "Smart Screen Filter", Chrome, Safari och Firefox använder en gemensam "Safe Browsing List".



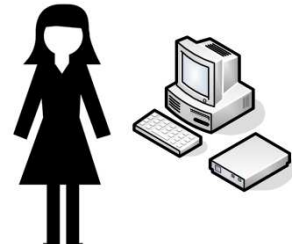
- Man kan alltid bilda sig en uppfattning om hemsidans rykte genom att googla själv
- Källkritik är helt nödvändigt, t.ex. misstänksamhet mot sökmotorns urval

Gunillas värld: Bedrägliga hemsidor

A screenshot of a web browser showing a promotional page for an iPhone 7. The browser's address bar displays the URL: <https://sourceone.prizesfortoday.com/se/?o=145&r=p1q5370322n7se&a=178&sa=4427>. The main heading reads "Få en iPhone 7" with subtext "3D Touch. 12 MP bilder. 4K video." and a note "+ 3 dagars provperiod på 101player.com för obegränsad onlineunderhållning". On the left, there is a form with fields for "Välj färg:", "Förnamn", "Efternamn", "Adress", "Postnummer", "Ort", and "E-postadress", followed by a blue "Fortsätt" button. Below the form is a "Teknisk info" section with bullet points: "Kapacitet 32GB", "Världens mest avancerade mobila iOS 10", "Ny 12 MP dual iSight-kamera", and "3D Touch skärm med OLED-bakbelyst skärm". On the right, a hand holds an iPhone 7 displaying a calendar event "Coffee with Allison" and weather information for Cupertino. A red circular sticker with the text "Promo Pris 10:-" is overlaid on the phone's screen.

Behöver man tillägga att det finstilt kostar 800:- i månaden i medlemsavgift? Källkritik!

Gunillas värld: Bedrägliga/farliga brev



Oönskade brev är mycket vanligt!
Sådana brev kallas SPAM och kan göra harmlös reklam men också försöka luras (= Nätfiske).
Bara släng dem, så är ingen skada skedd.
Påhittigheten är enorm! De är sällan på svenska.
Skickligt gjorda falska brev är svåra att avslöja =>

De kan ha virus i bilagor.
Öppna helst bilagor i molnet, om det går!

Moderna E-postleverantörer och Antivirus lyckas ofta, som väl är, avlägsna såväl spam som farliga bilagor, men inte alltid.

From: Google <no-reply@accounts.googlemail.com>
Date: March 19, 2016 at 4:34:30 AM EDT
To: john.podesta@gmail.com
Subject: Someone has your password

Google



Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:

Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

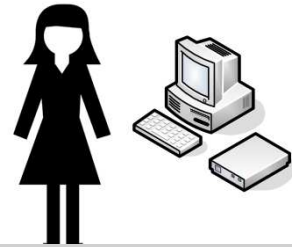
Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](#)

Best,
The Gmail Team

You received this mandatory email service announcement to update you about important changes to your Google product or account.

Gunillas värld: Bedrägliga brev



Här är ett oskickligt gjort falskt brev =>

Dessa frågor man kan ställa sig för att undvika att bli lurad:

- Är avsändaren pålitlig? (kolla ryktet)
- Stämmer avsändaren? (kolla språket)
- Varför kommer informationen just till mig?
- Om det är tillkrånglat – varför? (text i bilder – länkar – bilagor – ziparkiv ...)
- Går innehållet att bekräfta? (För bra/hemskt för att vara sant?)
- Är det fortfarande aktuellt?

”Telefonlur” förekommer också!

From: "donotreply@hmrcupdate.com" <donotreply@hmrcupdate.com>
Date: 4 May 2016 11:32:04 BST
To: Undisclosed recipients;
Subject: Tax Refund

Avs brukar vara falsk!

HM Revenue & Customs

Wednesday, 4 2016

Dear Sir | Madam

We have recently noticed some discrepancies in your tax return for the previous year. You are now due some refunds. We do not hold your payment details on record. [Press here to provide us with your settlement method.](#)

Kindly allow 7-10 working days for refund to appear on your account.

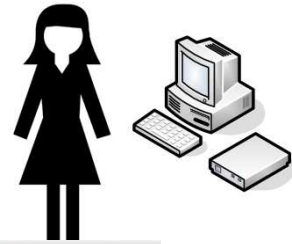
You have 5 working days from the receipt of this email to action the request.

Sincerely
Customer Support
HMRC

Sväva med musen över länken

<http://goo.gl/1qCAsJ>

Gunillas värld: Bedrägliga formulär

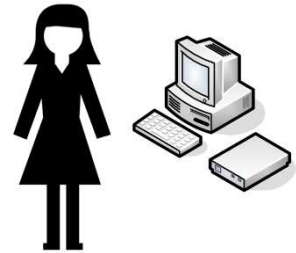


Innan man lämnar ut information:

- Kan man lita på att mottagaren hanterar informationen väl? (kolla villkor och rykte)
- Stämmer mottagaren? (kolla språket, finns kontaktuppgifter)
- Ser formuläret professionellt ut?
- Varför behöver just jag lämna ut denna information?
- Till vad behövs alla de uppgifter som efterfrågas?
- Är det någon mer uppgift som borde varit med?
- Blir känsliga uppgifter skyddade av kryptering? (https:// eller hänglås)

A screenshot of a web browser showing the ANZ login page. The browser's address bar contains a long URL: anz-australia-loginaccount.com/ssl/anz/anz/auth.html?info=4624g80a13c0db1f8e263663d3faee8d195ae. The ANZ logo is visible at the top. A yellow warning box with a triangle icon contains the text: "In order to cancel a payment we need to verify your identity. Please type the requested information in the fields below. This information is used for verification purposes only. Your credit card will not be charged." Below the warning is a form with the following fields: Full Name (with a dropdown menu set to "Exactly as appears on card"), Date of Birth (dd-mm-yyyy), Billing Address, City, Postcode, Mother's Maiden Name, Card Number (four separate boxes), Expiration Date (mm-yyyy), and Cvv (one box). A blue "SUBMIT" button is at the bottom right of the form.

Gunillas värld: ID-stöld



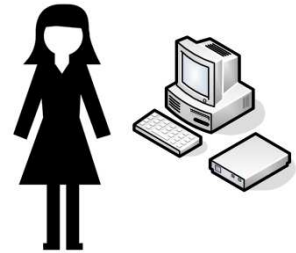
Användarnamn, lösenord och personnummer går att stjäla genom att

- Fråga
- Gissa lösenorden
- Virus stjälar dem från webbläsarens ifyllnadsförslagsminne
- Virus stjälar s.k. sessionskakor
- Ta dem från kundregister (Yahoo, Spotify m.fl. har läckt)

Det finns många andra sätt som all möjlig privat information kan stjälas på

- Att någon skapar konton i andras namn och låtsas vara dem
- Att man glömmer bort att logga ut på Internet-caféer.
- Att skumma Internet-caféer kan ha virus som stjälar kontonamn och lösenord.

Gunillas värld: Lösenordens tyranni!



Två bra principer:

- I want to go to Paris next year
= !w2g2Pxy
- Fyra orelaterade vanliga ord
= KurortSelleriVaddAstrid

Lösenordshanterare i molnet är en lösning
Se t.ex. <https://identitysafe.norton.com/sv>
men kom ihåg hanterarens lösenord!!!
(Ve användarna om tjänsten hackas.)

Banker har betydligt säkrare inloggningar!

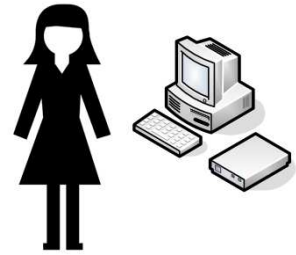
Lösenord ska vara

- Hemliga
- Lätta att hitta på *själv*
- Lätta att komma ihåg
- Svåra att gissa
- Svåra för datorer att knäcka
- Olika överallt (stomme + dekor)
- Så som hemsidan kräver
- Utan åäö om man vill kunna använda dem utomlands

Undvik påminnelsefraser som gör lösenorden för lätta att gissa!

Gunillas värld: Shopping på nätet

Internet är globalt och man vet inte var företagen finns och vilka lagar som gäller



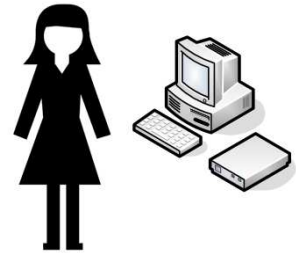
Handlar man på Internet kan det hända att

- Varan kanske inte levereras i gott skick, eller alls
- Kontokortnummer och CVC stjäls ur hemsidans kundregister eller stjäls av ett (virus)installerat tillägg till Webbläsaren

Man kan skydda sig genom att

- Kolla att förbindelsen är krypterad vid betalning (https:// eller hänglås)
- Undvika tillägg i Webbläsaren
- Bara handla från respektabla hemsidor
- Bara öppna kontokortet tillfälligt för Internethandel
- Använda PayPal, så att hemsidan aldrig får reda på kontokortet
- Kontrollera kontoutdrag och fakturor noga (även när man inte e-handlat)
- Köpa via postförskott eller faktura

Gunillas värld: Sociala medier



- Homo Socialomedicus är en ohämmad natur, för i sociala medier råder
 - en snabb marknadsföringskultur (klickfiske, nödvändigt med källkritik)
 - en bevakningskultur (den globala byn)
 - en populäriskultur (gynnar populism)
 - ett mobbarnas eldorado (laglöst vilda västern)
- Åsiktsgrupper man är med i kan kapas och byta till andra åsikter
- Informationen man lämnar ut om sig själv eller andra kan ryckas ur sitt sammanhang, spridas okontrollerbart och aldrig dö
- ID-stölder förekommer, dvs konton kapas eller dubblettkonton skapas
- Gillar man festliga frågesporter och spel kan man få mycket spam efteråt

Några goda råd om hur man klarar sig

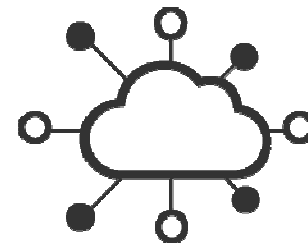


- Ladda ner och shoppa bara från respektabla hemsidor!
- Undvik tillägg i Webbläsaren!
- Använd bra Antiviruspaket som även är begripliga!
- Håll datorn uppdaterad!
- Ta backuper ibland!
- Var misstänksam mot konstiga hemsidor och meddelanden, även från vänner!
- Se till att e-post innehåller frågor!
- Använd långa lösenord!
- Håll hårt i lösenord och kontokortsuppgifter!
- Chansa inte! Fråga hellre någon du litar på först.
- Var inte ute i sista stund!

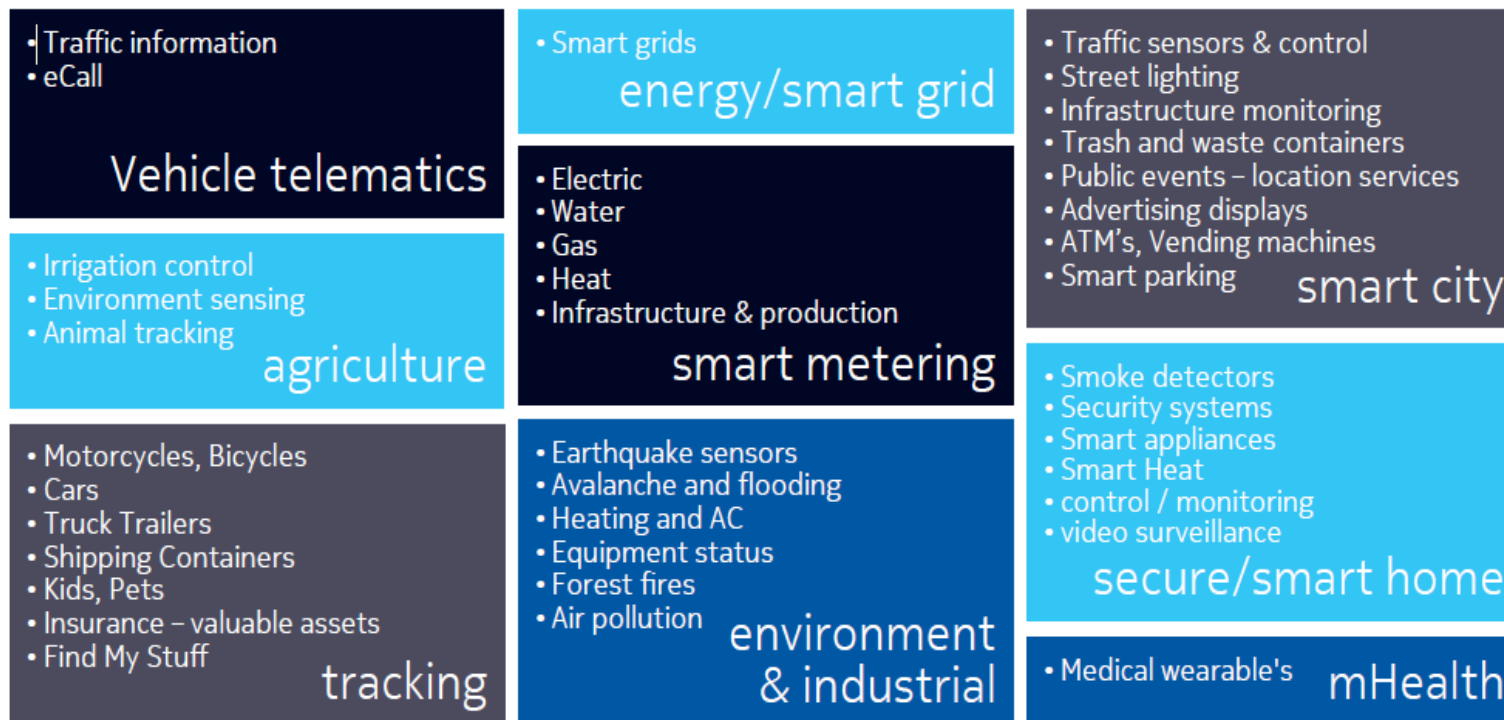


Bra info för den som vill läsa mer

- <http://www.iis.se/>
- <http://www.dinsakerhet.se/>
- <http://www.usa.gov/online-safety>
- <http://computer.howstuffworks.com/10-forms-online-harassment.htm>
- https://en.wikipedia.org/wiki/Internet_vigilantism
- <http://www.av-test.org/en/test-procedures/test-modules/>
- https://en.wikipedia.org/wiki/Comparison_of_antivirus_software
- <http://www.wikihow.com/Be-Safe-on-the-Internet>
- <http://www.internetmuseum.se/>
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
- <https://support.google.com/mail/answer/1366858>
- https://en.wikipedia.org/wiki/Mobile_security
- <http://www.konsumenteuropa.se/sv/amnesomraden/bluffar-och-bedragerier/>

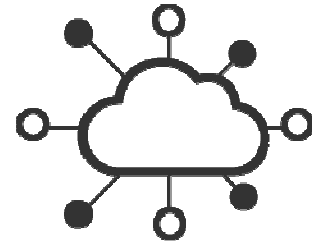


Framtiden: Internet of Things (IoT)



Kan t.ex. ge bättre kunskaper, möjligheter till fjärrstyrning och betaltjänster/reklam
Lägre försäkringspremier och tekniska molntjänster väntas driva på utvecklingen

Framtiden: Internet of Things (IoT)



- 5G-teknik behövs för att ansluta alla nya digitala ”prylar” direkt till Internet
- Den kopplar upp snabbare och säkrare, och har högre kapacitet än idag
- För att inte bli kapade behöver prylarna
 - Ha robusta brandväggar
 - Unika lösenord
 - Uppdateras regelbundet

Framtiden blir mycket spännande.

IT-industrin behöver skärpa sig, för prylsäkerheten idag är dålig. Den provar normalt ut sina ofärdiga produkter i verkliga livet på ett ansvarsbefriat sätt som traditionell industri aldrig skulle våga sig på att göra.

Frågor?

Kommande dataträffar?



Vi planerar fyra nya intressanta dataträffar under vårterminen.

Mer information om dem kommer på hemsidan efter nyår.

Se <http://snso.se/datatraffar/kommande-traffar/>

Kontakta oss gärna på: datatraffar@snso.se

Slut för idag!

Tack för idag!

Surfa lugnt!