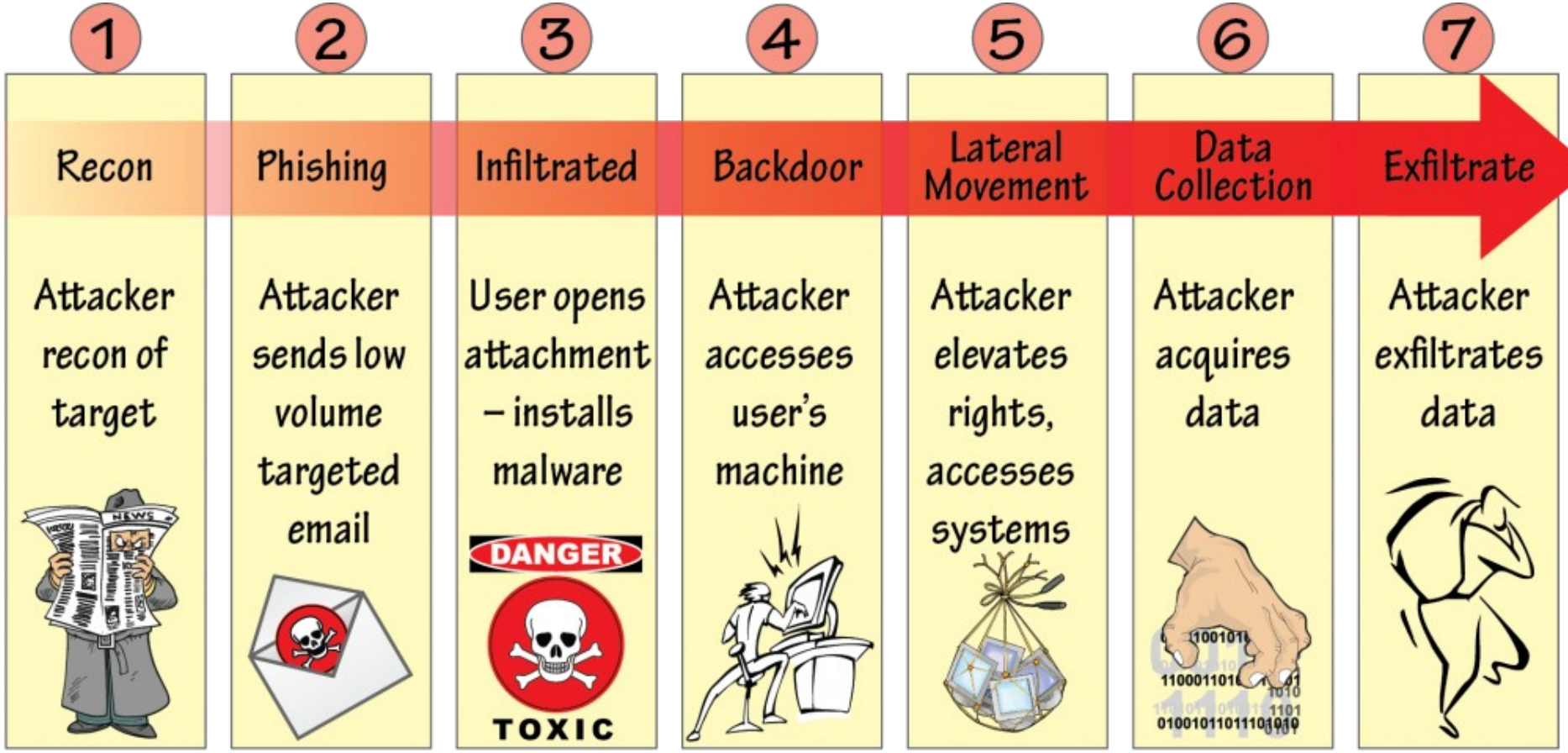
Cyber Kill Chain



Sådan undgår du at andre stjæler dit online-liv

Sådan skal du gøre, hvis du vil undgå identitetstyveri - eller hvis det er gået galt. 73.000 danskere blev ramt sidste år. Du skal nødigt blive den næste.

http://www.computerworld.dk/art/227939/saadan-undgaar-du-at-andre-stjaeler-dit-online-liv

Identitetstyveri dækker både over, at nogen ulovligt tilegner sig en andens oplysninger, og at nogen misbruger disse oplysninger til fx at optage lån, købe ting eller chikanere på forskellig måde.
De personlige oplysninger kan fx være CPR-nummer, adgangskoder, sundhedsoplysninger eller andre følsomme persondata. ”IDENTITY THIEF”

Din PC har VIRUS

1. Hvis skærmen fyldes med mærkelige popups, reklamer i nye vinduer, vinduer, der fortæller, at Pc'en er angrebet af virus mm., er det typisk spyware eller et falsk antivirusprogram.

2. Kører Pc'en pludseligt meget, meget langsomt er dette typisk et tegn på en virus, en orm eller en trojaner eller anden malware. (Dette er dog langt fra sikkert, grundet service packs)

3. Hvis et program ikke vil starte, er det oftest et tegn på inficering.

4. Forbindelsen til Internettet er gået eller kører meget langsomt. Sker dette, er det oftest fordi malware på Pc'en bruger forbindelsen til at linke til andre computere i et botnet eller sender mails med vira til brugerens adressebog.

5. Lige pludselig dukker der websider op, som brugeren ikke har skrevet i browserens adressefelt.! Dette er andet tegn på, at Pc'en er angrebet, og her skal brugeren være meget opmærksom på, at der ikke sendes til sider med malware etc. Det er om at få hevet stikket til bredbåndet!

6. Er billederne fra brylluppet forsvundet eller brevet til banken om omlægning af lånet? Lad os ikke håbe det sker, men hvis brugeren oplever det, skal Pc'en undersøges grundigt for virus og anden malware.

7. Antivirusløsningen er forsvundet og firewallen slået fra – et andet meget sikkert fingerpeg om, at Pc'en har software liggende, der slår alle sikkerhedsmekanismer fra.

8. Hvis skærmen bliver "spist" af små insekter eller er fyldt med kinesiske eller russiske tegn er dette meget sikre vink om, at computeren er snigløbet af malware.

9. Hvis en eller flere filer, som kræves for at fx et spil eller et program kan køre, er forsvundet, kan der også være virus på Pc'en, men evt. også på at installationen ikke har kørt helt efter bogen.

10. Computeren har fået sit eget liv! Hvis Pc'en har sendt mails, som brugeren ikke har skrevet, starter programmer, som brugeren ikke har installeret, er der meget stor sandsynlighed for, at der er virus på maskinen.

Virus fri, hvordan.

Kampen mod virus er bestemt ikke afsluttet, i kan til enhver tid få scannet jeres private udstyr, under formodet mistanke, om virus.
HVIS i konstaterer virus, så husk omgående at melde det til jeres IT ansvarlige!
Vil i selv forsøge jer, så anbefales følgende procedure ved formodet virus.

1. Scan/rens jeres udstyr med Kaspersky online scanner/BOOT CD. Webroot Spysweeper (Der findes dog andre, men disse er effektive) Download evt. trial version til scanning.
2. Red data, altså tag Backup af dokumenter, billeder osv. på Ekstern Harddisk (Ikke på USB nøgle)
3. Whipe disken (Altså en fuldstændig sletning af data på jeres Harddisk)
4. Whipe alle USB nøgler/Eksterne HD/SD-MMC hukommelseskort osv.
5. Geninstaller operativsystem (Microsoft, Linux eller Mac)
6. Scan Backup data, med nedenstående produkter. (Før de indlægges på PC)
7. Installer/indkøb Antivirus, Webroot Spy Sweeper (Internet Security), Kaspersky
Kaspersky: Super fuldtids beskyttelse,
SpySweeper: Super scanner.
8. Før Backup data tilbage på den nyinstallerede PC.
9. Kontroller Firewall er aktiveret.
10. Først nu kobles PC igen på internettet.
11. Lav nye passwords på PC, Mailkonti, Netbank, Live messenger, Facebook osv
12. Noter jer "normalbilledet" for den nyinstallerede PC. (Hvor hurtigt loader den, falder PC til ro osv.)

Kontakt familie, venner, kolleger osv. - de vil sikkert sætte pris på info omkring jeres konstaterede virus..

Certifikater, demo

Webbrowser

I T S I K K E R H E D

IE10

- NEM ID
- Digital Signatur
- Net Bank
- Webshop

Firefox

http://lifehacker.com/turn-on-tracking-protection-in-firefox-to-make-pages-lo-1706946166

Chrome

- Gmail
- Hotmail
- Live Messenger
- Streaming video
- Browsing
- Websider

Husk ÅBN kun ”1 vindue” ved LOGIN på Netbank eller Webmail ect.

Første afpresnings-software på dansk

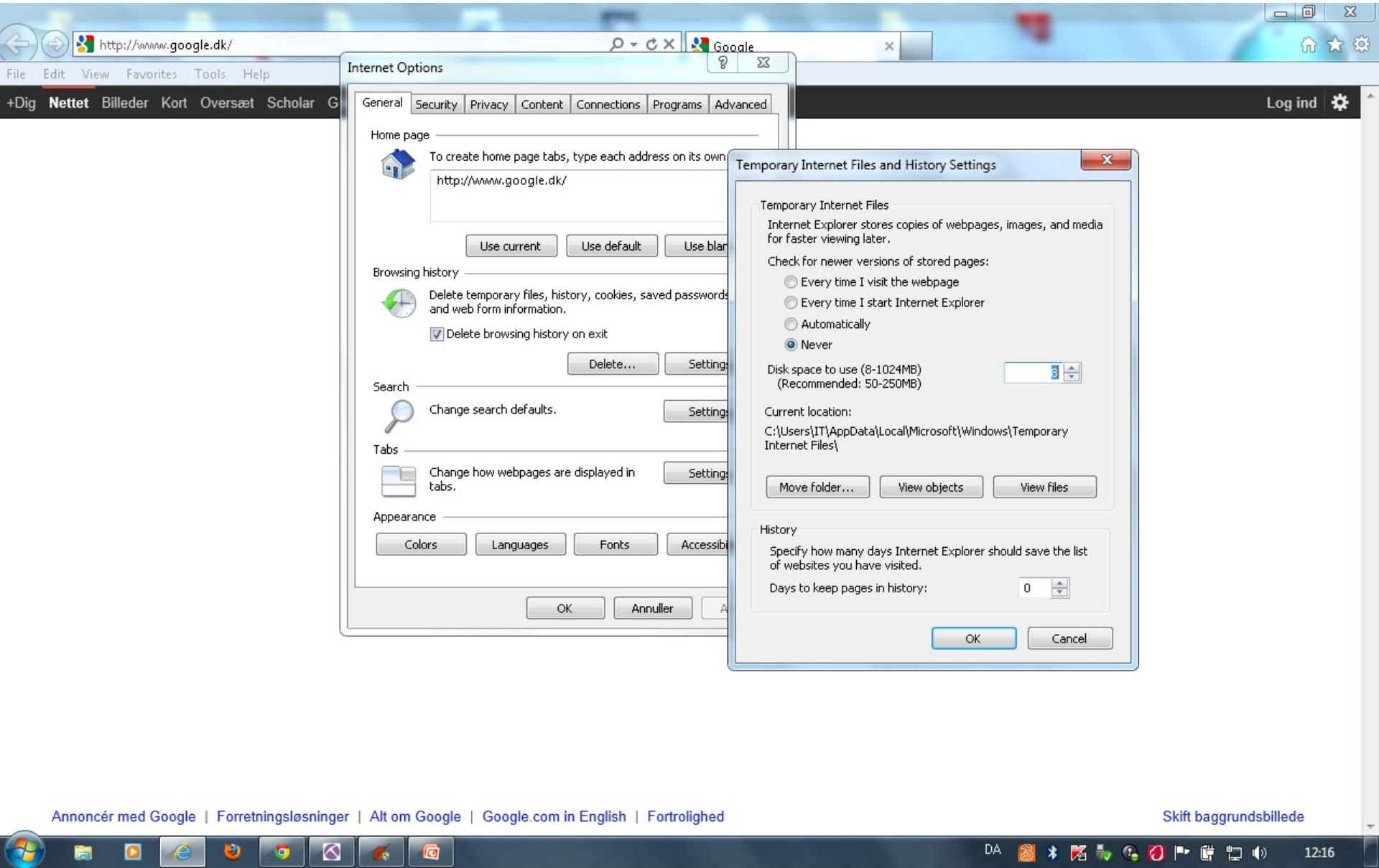
(Ransomware)

http://www.computerworld.dk/art/220175/her-er-den-foerste-afpresnings-software-paa-dansk

AdBlock + Ghostery Tilføjelser

1. **Demo EtherApe – Ekstrabladet.**
2. **Installer Mozilla Firefox**
3. **Installer AdBlock**
4. **Start Ekstrabladet.**
5. **Bloker elementer.**
6. **F5, opdater Ekstrabladet.**
7. **Fjern Blokering**
8. **Installer Google Chrome,**
9. **Installer Ghostery.com**
10. **Kør Wizard…**
11. **I Options Enable Bug og Coockie protection – Save.**
12. **F5 Opdater Ekstrabladet,**

IE10, indstillinger



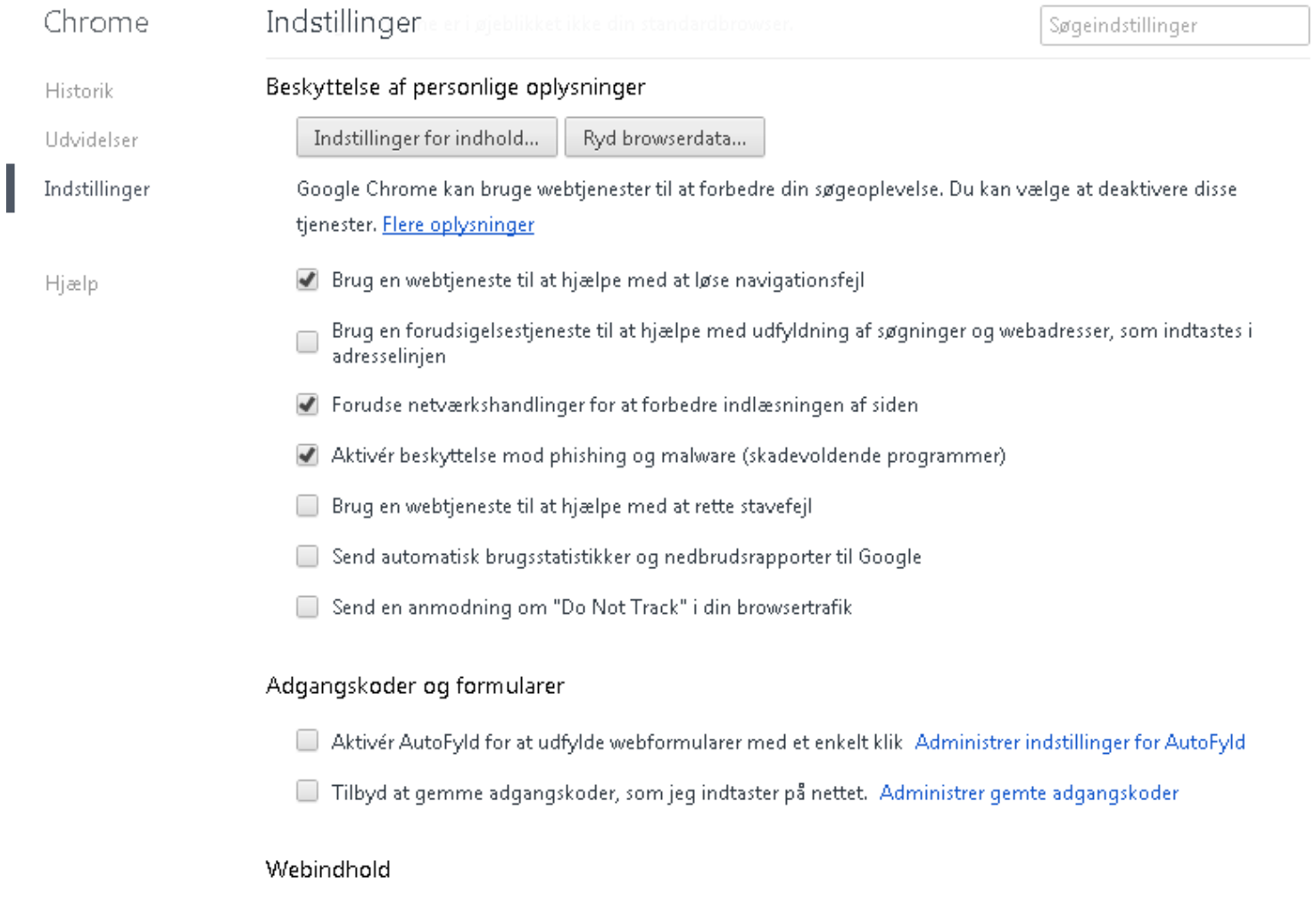
Lille opgave.

1. Indstillinger
2. Tilbyd at Gemme adgangskoder
   (Fjern markering)
3. Indstillinger for indhold,
   Cookies

– ”Alle Cookies og Websitedata” kontroller,,

4. Tillad ikke sporing af fysisk placering.
5. Brug Virtuelt tastatur

Chrome



Sletning af Cookies

Foreningen for Dansk Internet Handel (FDIH) anbefaler, at du sletter dine cookies jævnligt. Nedenfor finder du links til, hvorledes du kan slette de cookies som er sat i din computer.

Sletning af cookies er afhængig af, hvilken browser du benytter.

Benytter du en PC og med nyere browsers kan du slette dine cookies ved at bruge genvejstasterne: **CTRL + SHIFT + Delete**

Virker genvejstasterne ikke og/eller benytter du en Mac skal du starte med at finde ud af, hvilken browser du anvender og klik herefter på de relevante links:

Sletning af cookies i Internet Explorer
Sletning af cookies i Mozilla Firefox
Sletning af cookies i Google Chrome
Sletning af cookies i Opera
Sletning af cookies i Safari 6
Sletning af Flash cookies

http://www.fdih.dk/cookies/slet-dine-cookies

Tool - Test Port Forwarding on Your Router - Windows Internet Explorer

http://www.yougetsignal.com/tools/open-ports/

Favoritter Funktioner Hjælp

Open Port Check Tool - Test Port Forwarding on ...

PortScanning

you get signal

Port Forwarding Tester

your external address

95.209.228.194

open port finder

Remote Address 95.209.228.194 Port Number 80 Check

Use Current IP

Check a port's status by entering an address and port number above.

about

The open port checker is a tool you can use to check your external IP address and detect open ports on your connection. This tool is useful for finding out if your port forwarding is setup correctly or if your server applications are being blocked by a firewall. This tool may also be used as a port scanner to scan your network for ports that are commonly forwarded. It is important to note that some ports, such as port 25, are often blocked at the ISP level in an attempt to prevent malicious activity.

This tool should work on any system connected to the Internet, even on latest mobile phones equipped with mobile broadband.

For more a comprehensive list of TCP and UDP ports, check out this Wikipedia article.

If you are looking for a software solution to help you configure port forwarding on your network, try using this powerful Port Forwarding Wizard.

common ports

21 FTP
22 SSH
23 TELNET
25 SMTP
53 DNS
80 HTTP
110 POP3
115 SFTP
135 RPC
139 NetBIOS
143 IMAP
194 IRC
443 SSL
445 SMB
1433 MSSQL
3306 MySQL
3389 Remote Desktop
5632 PCAnywhere
5900 VNC
6112 Warcraft III
Scan All Common Ports

Open Port Check To... IT Sikkerhed Microsoft PowerPoin... DA

Hvordan snyder de os..

- Scam # 1: ***Din computer er inficeret*** **, Den største kriminelle trussel er de (FAKE) antivirus produkter!**. De forsøger at overbevise dig om, at din computer er inficeret, så du installerer og betaler for "antivirus beskyttelse" - det er reelt ikke beskyttelse. - I det øjeblik du ser en falsk alarm, stop alt, hvad du laver, - dræb browseren, og udføre en fuld scanning med de legitime antivirus produkter.

- **Scam # 2:.?!** ***Tjek dette cool link*** **Din vens e-mail eller Facebook konto** er kapret, og du modtager en kort besked med en kort URL til at se en video eller tjek noget lige så "cool". Linket fører rent faktisk til en ondsindet side med en malware download. De fleste shortlink tjenesteydelser har en funktion, der lader dig se, hvor shortlink vil gå hen, bruge det. Hvis du aldrig har hørt om webstedet, skal du kontrollere faktiske destination område med, f.eks

- **- - - - -http://www.ip-adress.com/ip_tracer**

- Scam # 3:.? ***Peter Hansen ønsker at være din ven*** - via populære sociale netværkssider.. I stedet for at linke til "venneanmodning," tager den dig til en ondsindet side . For at undgå dette, uden at klikke noget, **skal du flytte musen hen over linket i din e-mail, så se på statuslinjen for at se præcis, hvor linket fører hen**, Hvis meddelelsen hævder at komme fra ét specifikt selskab, men webadressen peger på et domæne, du aldrig har hørt om, skal du ikke klikke på linket.

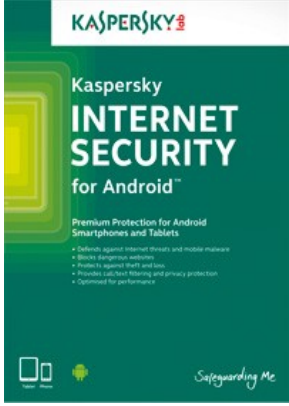
Hvordan snyder de os..

- **”Drive by” Omrute banklogin, *”Vi har registreret dit psw os skal opdat. Sikkerhedsindstillinger, dette kan tage op til 10 min på en langsom internet”***
- **Spear fishing attack,** http://www.computerworld.dk/art/116931/hackernes-nye-vidundervaaben-spear-phishing
- Targeted malware https://media.blackhat.com/bh-eu-10/presentations/Carrera_Silberman/BlackHat-EU-2010-Carrera-Silberman-State-of-Malware-slides.pdf
- Targeted malware: ”Online spil for børn” Google søgning.
- Virus på Printere: CPU og HDD
- SpamBot: http://en.wikipedia.org/wiki/Spambot
- PDF Stream dumper: http://blog.zeltser.com/post/3235995383/pdf-stream-dumper-malicious-file-analysis
- Buffer Overflow: Hvad er det ? http://en.wikipedia.org/wiki/Buffer_overflow
- Honey Pot:
- Penetration test, bestilles af diverse større virksomheder – hvorfor ??
- DataMining: Automatiseret søgning efter skjulte mønstre, Bruger info om færden på internettet, gruppere enheder, relationer mellem databaser.
- Fuzzy Logic: Problemløsning automatiseret control system.
- Cloud Computing: Hvad er det ? Hvorfor ? (Trusted computing base) hvem kigger med ?
- **http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/**

APPS
”Blacklist”

Top 10 Blacklisted Apps: iOS Devices	Top 10 Blacklisted Apps: Android Devices
1. Dropbox	1. Dropbox
2. SugarSync	2. Facebook
3. Box	3. Netflix
4. Facebook	4. Google+
5. Google Drive	5. Angry Birds
6. Pandora	6. Google Play Movies & TV
7. SkyDrive	7. Google Play Books
8. Angry Birds	8. SugarSync
9. HOCCER	9. Google Play Music
10. Netflix	10. Google+ Hangouts

Tablet/ Phone



- **Ad injector. Inficeredt Adware.**
- **APP integration, 2 APPs samarbejder om tyveri,**
- **Kryptering. Data gøres ulæselige for hacker.**
- **2 Factor auth. Login gøres sikker.**
- **Wrapping. Et ekstra sikkerhedslag på APPs**
- **SecuTablet Hårdt opsat Blackberry Tablet.**

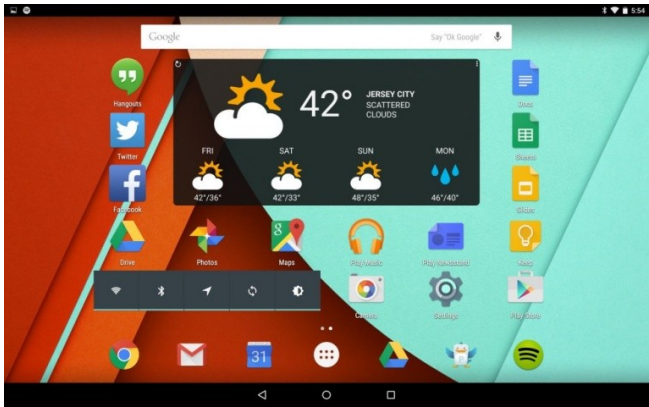
Anbefaling

1. Anvend adgangskoder
2. Aktiver kryptering
3. Hold styresystemet på din smartphone opdateret
4. Åbn ikke ukendte filer, som du modtager med mms, mail eller Bluetooth
5. Installer kun applikationer du har tillid til
6. Aktiver mulighed for at fjernslette alt indhold
7. Lås SIM-kortet til telefonen
8. Sluk for Bluetooth, når det ikke benytte
9. Når din smartphone anvender Wi-Fi, skal det trådløse net være krypteret
10. Brug antivirus, (Kaspersky/Webroot/Lookout)

Kilde: http://borger.itst.dk/sikkerhed

IOS
ANDROID

- IOS/Android
- Kryptering af OS
- Antivir.
- APPS
- Browser.
- 2 Fact. Auth på mail/FB ect.



"Jeg har brug for din hjælp".

Situation:

- Gmail hacket,
- Oversat til arabisk,
- Alle mails slettet og
- Alle mails videresendt til samme mailnavn@yahoo.de,
- Alle kontakter fjernet men kopieret,
-

  Indstillinger:
- 1. Slet: videre-sendelse af mail, og slet videresendelses mailkonto.(husk gem ændringer under hvert faneblad)2. Fjern alternativ mobil nummer til gendannelse. - Indsæt eget mobil nr., aktiver "2 factor autentifikation"
- 3. Ændre sprog, hav Gmail åben på alternativ PC, således at stien ind til sprog kan visuelt kopieres. (ikke samme mail konto)
- 4. Ændre: "sletning af mail i inboks". til "kopi af mails i inboks"
- 5. Genskab mails i inboks.
  6. Genskab mails fra papirkurv. max 30 dage.
- 7. Genskab kontaktpersoner max. 1 år.
-

  Password og sprog kunne ændres, men efter kort tid var konto tilbage på arabisk.
  2 gange under gendannelse, (ca 2 timers varighed) tog hacker kontoen tilbage, først da alternativ mobilnummer var fjernet kunne hacker ikke længere gendanne psw og sprog.

DNSChanger Malware

DNS Malware: Is Your Computer Infected?

DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse web sites, send e-mail, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

Lille Øvelse .

w.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

Erfaringer, optimering…

- Formater USB hver gang der er flyttet data! (Fuld formattering)
- KUN anvende USB medier til data flytning, ikke til backup eller som lagerplads.
- Brug externe HD/Cloud til opbevaring fremfor USB sticks.
- Scan alt inden det bliver tilknyttet PC, med Webroot Spysweeper/Kaspersky. (evt. TRIAL) USB, CD, DVD, SD/MMC kort, Mobiltlf, Kamera, GPS o.s.v.
- BOOT scanne private PC med Kaspersky RescueDisk.
- ”Fange” alt der kommer ind fra gæster, på jeres sweeper/scanner PC.
- Deaktivere Autorun i WIN
- Vise ”skjulte filer og mapper” (hvis det er windows).
- Slå ”skjul beskyttede operativsystemfiler” fra.
- Slå ”skjul filtypenavne for kendte filtyper” fra.
- BlueTooth, deaktiver både på Mobil og Bærbar når det ikke anvendes.
  (Bluesnarfing, simpel og hurtig måde at tilgå og skade både PC samt mobil)

HUSK vi bliver overvåget!

Erfaringer, optimering

- LINUX til IT driftcenter. Ved hårdnakkede Vira.
- Flere Vira som gratisprogrammer IKKE detekterer .
- Log ALDRIG ind på et åbent trådløs netværk, Hverken hjemme, job, Lufthavn.
  (MAN in The Middel ATTACK **Erfaring fra KIEV uge 10 med WIFI hookup.**
- Minumum WPA-PSK kryptering på trådløse netværk. WEP eller WPA tager ca. 5 min at brute-force !!
  http://www.tacnetsol.com/news/2011/12/28/cracking-wifi-protected-setup-with-reaver.html
- http://lifehacker.com/5873407/how-to-crack-a-wi+fi-networks-wpa-password-with-reaver
  https://www.cert.dk/nyheder/nyheder.shtml?12-01-04-11-11-24
- **Airodump: 802.11 packet capture program**
- **Aireplay: 802.11 packet injection program**
- **Aircrack/Reaper: static WEP and WPA-PSK key ”brute force” cracker**
- **Airdecap: decrypts WEP/WPA capture files**
- **John The Ripper, Free Password Crack.**
- **Cain and Abel, WIN password Recovery tool (Brute force)**
- **Rainbow Crack, (Password Crack software)**
- **Brutus (Online Password Crack, HTTP, FPT, POP3, TELNET)**
- **Netværks Printer, vira på HDD. Der er CPU i nye netværks printere**

Internet Of Things

Consumer & Home

Smart Infrastructure

Security & Surveillance

Healthcare

Network

Transportation

Retail

Industrial

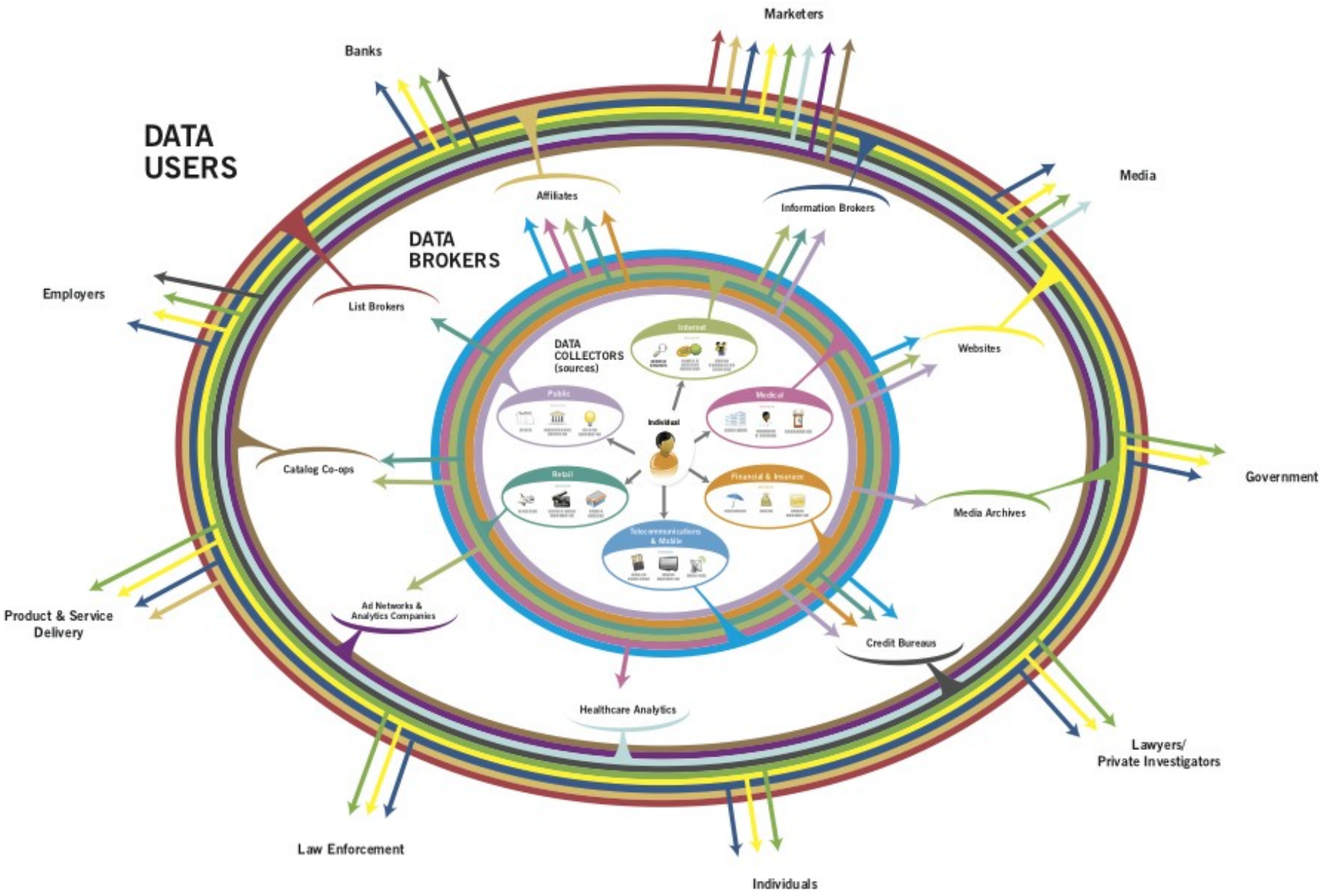
Others

Mobil sikkerhed

Sådan undgår du virus:

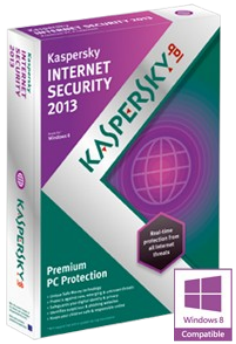
- Deaktivere: Bluetooth-forbindelsen,WIFI og Netværk - når det ikke anvendes.
- Synlighed til ”skjult” under Bluetooth-indstillinger.
- Åbn ikke ukendte filer, som du modtager med mms, mail eller Bluetooth.
- Hvis mobiltelefonen pludseligt tilbyder et eller andet, som du ikke selv har startet eller kan gennemskue 100 %, så skal du altid vælge ‘NEJ’.
- Hvis du har en Smartphone (med operativsystem, JAVA, internetadgang, BlueTooth med videre), så skal du installere et antivirusprogram og huske at holde det opdateret.
- URL/Link scanner anbefales.

Personal Data Ecosystem



Links

http://www.threatexpert.com/
https://www.virustotal.com/
http://www.kaspersky.com
http://mobil-sikkerhed.dk/
https://www.whitehatsec.com/
http://www.csisdk/dk/artikler/artikler.asp
https://www.securitymetrics.com/portscanlogic.fadp
http://kriminalitet.dk/
http://www.computerworld.com/
http://www.f-secure.com/en_EMEA/security/tools/online-scanner/
http://www.spywarefri.dk/
http://www.ubuntu.com/
http://seclists.org/pen-test/
http://www.version2.dk/sikkerhed
https://www.govcert.dk/
https://www.ghostery.com/
http://linuxmint.com/
https://www.torproject.org/
http://ec.europa.eu/justice/data-protection/index_en.htm
http://www.datatilsynet.dk/
http://www.ice.gov/cyber-crimes/



Antivir Programmer

THREATEXPERT: Godt site med update på hack, BOTNET osv.
SPYWAREFRI.DK: Diverse kendte Trusler osv.
KASPERSKY – Internet Security.
WebRoot – Bedste bud lige nu på software til fjernelse af Spyware, Trojans. (Givet i Licens til LAN).
Linux: Mint, Backtrack, DEFT, Ubunto, Fedora.

Underdover blev der virus testet med:
Avast,
Bitdefender,
Avira,
AVG,
McAfee,
F-Secure,
NOD32,
Security Essentials,
Norton,
Comodo,
Bullguard,
Panda ,
G-Data.