

# Lühidalt infoturbest



# Miks ma peaksin muretsema?

- Mul pole ju arvutis midagi väärtuslikku!
- Miks peaks keegi just minu arvuti vastu huvi tundma?
- Senimaani pole ju midagi juhtunud.
- See on itipoisi mure.
- Ma ei taipa sellest nagunii midagi.
- Sissemurdmine on ju ebaseaduslik!
- Eestis ei ole selliseid kurjategijaid.



# Küberkuritegevuse tendentsid 2007-2010



2009

- Küberkuritegevus professionaliseerub
- Kurjategijaid huvitab pigem raha kui kuulsus
- Rünnakuteks vajalikud tööriistad on üha lihtsamad ja kättesaadavamad
- Rünnakud kodukasutajate vastu (botnet) – kasutaja teeb üht, küberkurjategijad midagi muud tema arvutis.
- Igapäevaellu on murdnud infosõda ehk poliitiliselt motiveeritud küberrünnakud



# Küberkuritegevus



- Küberkuritegevuse käive aastal 2006 oli võrreldav inimkaubanduse ning kasum narkokaubanduse omaga
- 2006. aastal registreeriti 3,24 miljonit arvutikuritegu
- Eksperdid usuvad, et 90% kuritegudest jääb registreerimata
- Allilmas on tööjaotus – need, kes oskavad pahavara kirjutada, ei levita seda kunagi ise
- Nõrgem lüli tavakasutaja
- Tulevik: Pahavara levib rohkem kiirsuhtlusprogrammide (MSN), internetitelefonide (skype), mobiiltelefonide kaudu
- Isegi Mac ja Linux pole enam nii turvaline kui varem ☹



## Parool peaks kaitsma arvutisüsteemi väärkasutamise eest, kuid:

- 1/3 internetikasutajaid jagab salasõnu oma lähedastega
- 40% paroolidest on laialt levinud:  
admin, parool, 1234, enda või pereliikme või lemmiklooma nimi, auto registreerimisnumber...
- 25% salasõnadest on murtavad 65 000 sõna sisaldava sõnaraamatu põhjal
- veel 11% salasõnadest on murtavad miljon sõna sisaldava sõnaraamatu põhjal
- Eesti tähestiku 32 tähest saab kuuetähelise sõnana moodustada 1073741824 kombinatsiooni



# Paroolide varastamine



- 1-2% inimestest annavad oma parooli võõrale sellepärast, et too seda küsib
- 90% arvutikasutajatest on nõus loovutama oma sisselogimisinfot pastaka vms eest
- Enamik kasutajaid ei kontrolli elektronkirja või telefonikõne ehtsust

## Paroole saab:

- Veebibrauseri salvestatud paroolide loendist
- Pealtkuulatud võrguliikluse kaudu
- Klahvivajutuste salvestamisega
- Sisestate need ise vastavasse veebivormi
- Ütlete telefoni automaatvastajale



# Tulemüür

- Tulemüür on esmane kaitse sinu arvuti ja interneti vahel
  - Kaitseb võrgust tulenevate rünnakute eest
  - Kaitseb mõningate tarkvara turvaaukude ära kasutamise eest
  - EI KAITSE viiruste eest
- Operatsioonisüsteemiga kaasatulev või kommertslahendus ?
  - Windows puhul kindlasti kommertslahendus, Linux puhul sobib ka operatsioonisüsteemiga kaasatulev
- Riistvaraline või tarkvaraline ?
  - Kontorivõrgus kas eraldiseisev tarkvaraline või riistvaraline tulemüür
  - Sülearvutil tarkvaraline tulemüür



# Viirusetõrje

- Millist viirusetõrjet valida ?
  - Symantec, McAfee, NOD32, Kasperski, Avira jne.
  - <http://www.av-comparatives.org/>
  - Korralik kohalik tugi
  - Suurema võrgu korral kindlasti korralik tsentraalhaldus
- Kas tasuta ka saab ?
  - Windows platvormil kommertskasutusse ei saa
  - Kodukasutuseks tasuta Avira, Avast, AVG
  - Linux puhul ClamAV tasuta



# Andmete varundus

- Paljudes ettevõtetes ei pöörata andmete varundamisele piisavalt tähelepanu.
  - Mõnikord arvatakse, et andmete säilimise tagamiseks piisab katkematu vooluallika olemasolust
  - Usutakse, et serverid ja töökohaarvutid on nii usaldusväärsed, et andmekadude pärast pole vaja muretseda.
- Millist meediat eelistada varukoopia salvestamiseks?
  - Väline kõvaketas
  - DVD
  - Lint
- Varundusteenust on võibolla hoopis tark sisse osta
  - Eestis pakub antud teenust näiteks MikroLink

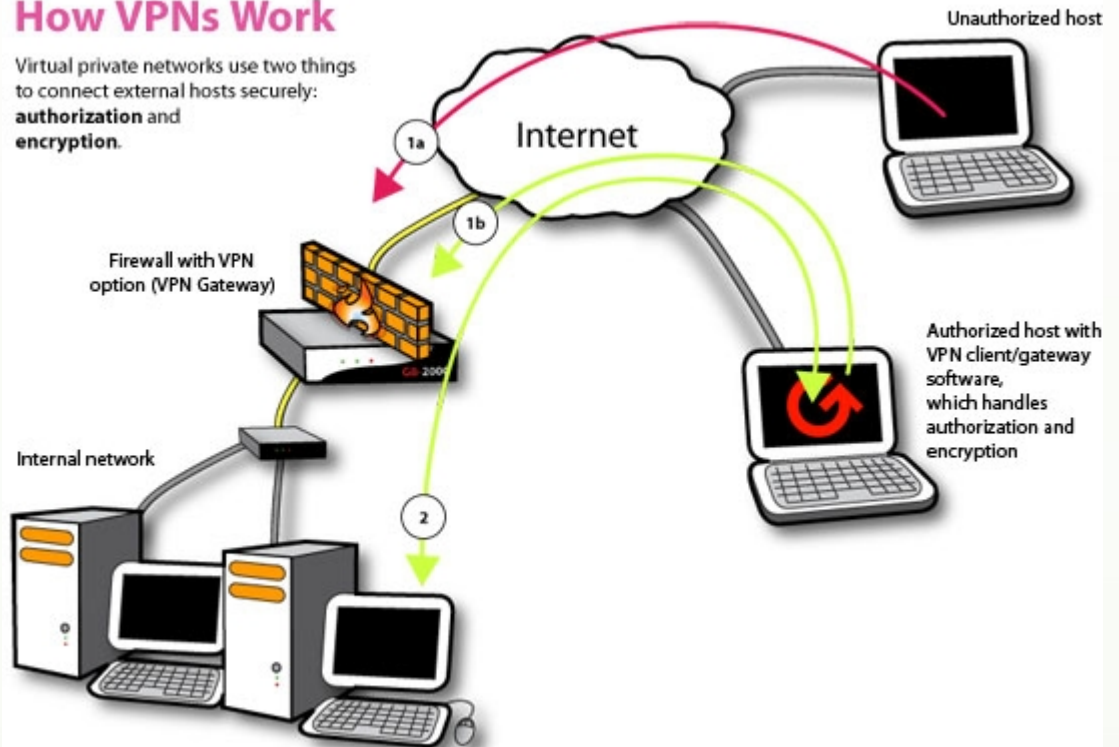


# VPN

- Virtuaalne privaativõrk (inglise keeles Virtual Private Network, VPN) on privaatne ja turvaline arvutivõrk, mille loomiseks kasutatakse avalikku telekommunikatsiooni infrastruktuuri.

## How VPNs Work

Virtual private networks use two things to connect external hosts securely: **authorization** and **encryption**.





# Üldised soovitused



2009

- Kasuta tulemüüri
- Hoia viirustõrje värskes
- VPN ühendused kontori/töötaja, kontori/kontori vahel
- Vaata et tarkvara oleks uuendatud
- Loobu administraatoriõigustest
- Varunda varakult, varunda tihti
- Ära ava kõike, mida sulle näidatakse või saadetakse
- Kasuta ID-kaarti ja Mobiil-ID´d veebiteenustesse sisenemiseks



# Miks ID-kaart?

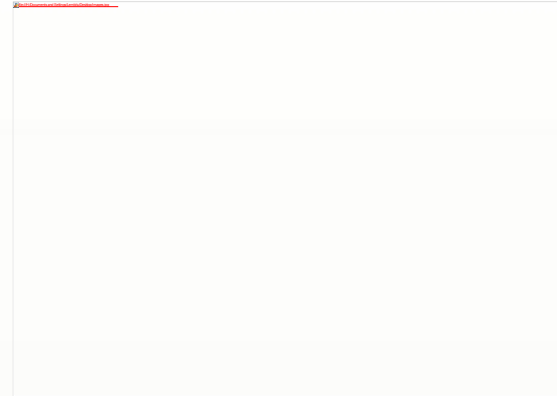


- **Turvaline** – kahetasandiline isikutuvastus (vajalik ID-kaart ning PIN-koodid)
- **Mugav** - üks kaart igale poole sisenemiseks, lisaks digitaalalkiri (ametiasutuste, ID-sõbralike asutustega suheldes)
- Palju kasutusvõimalusi
- Kuna ID-kaart on kohustuslik isikut tõendav dokument, peab see inimesel niikuinii olemas olema.
- Kaardilugeja soodsam – võimalik saada tasuta või max 100kr, PIN-kalkulaatori hind jääb 200 krooni kanti.



# Kaks sõna kaardilugejatest

- Kodukasutusse sobib tavaline kaardilugeja
- Jagatud kasutuse korral kindlasti PIN sõrmistikuga kaardilugeja koos seda toetava tarkvaraga

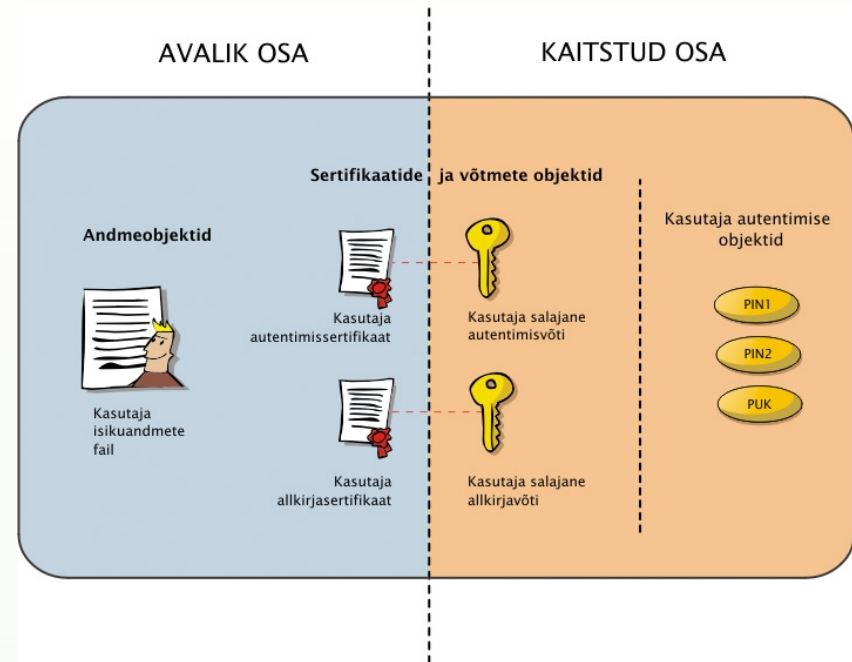




Kiipkaart – nagu väike arvuti  
ID-kaardi kiibil on nii palju  
infot kui hädapärast  
vajalik:

- ✓ Isikuandmete fail
- ✓ Sertifikaadid
- ✓ Võtmed

Ligi saab ainult PIN-idega!





# Turvariskid



- Koode hoitakse koos ID-kaardiga samas rahakotis (muidu läheb meelest)
- Koodi sisestatakse võõras arvutis (pahalasega nakatunud sõbranna arvutis)
- ID-kaart antakse liiga kergekäeliselt võõra inimese kätte
- Algsed koodid jäetakse vahetamata ja turvaümbrik varastatavasse kohta



# Kust saad abi ja infot?



- <http://www.arvutikaitse.ee> - Arvutiturvalisus
- <http://www.infosecurity.ee> - Arvutiturbest vene keeles
- <http://www.id.ee> - ID-kaardi abi