



Velkommen til

IT-sikkerhed med flere enheder

Henrik Lund Kramshøj hk@zencurity.dk

slides are available on Github

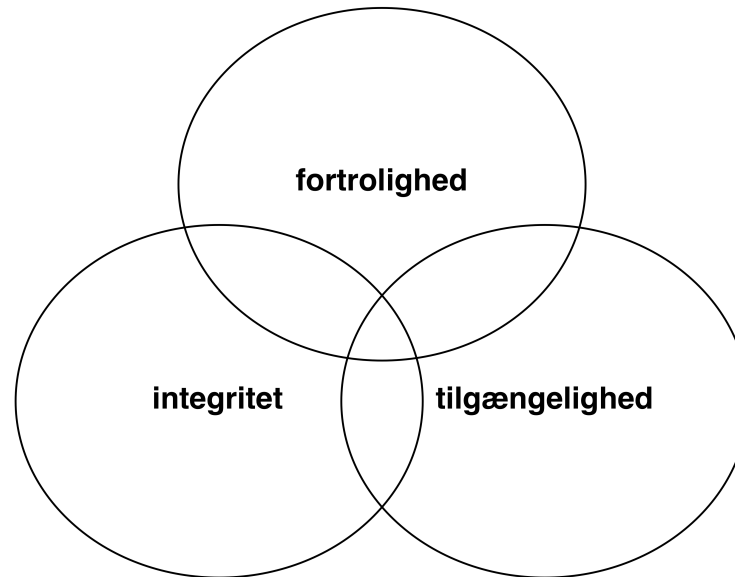
Formålet med foredraget



Don't Panic!

Give eksempler på metoder for at sikre data ved brug af flere enheder

Plan: Vi skal beskytte data



- Nogle enheder er nemme at transportere, mobiltelefon
- Nogle enheder har rigtigt tastatur

Næsten alle enheder idag bør have fuld kryptering af storage

Quick Wins: Opsec Light



Operations security (OpSec, OPSEC), what do you need?

https://en.wikipedia.org/wiki/Operations_security

Use multiple devices, isolate data

Less critical on phone, most critical on laptop with full disk encryption

Using different password for each service, impossible!

One time passwords



YubiKey NEO

Multi-protocol security key with NFC for Android phone, tablet, and Windows, Mac, and Linux computers.



YubiKey 4 Series

Our most popular key. Multi-protocol security key. Multiple form factors for USB-A and USB-C.

OTP One Time Password, sniff one and you can use it, if you have a time machine 😊

I use Google Authenticator and Yubikeys

https://en.wikipedia.org/wiki/Google_Authenticator

<https://www.yubico.com/start/>

Eksempel Mine enheder



- Min private telefon
- ~~Min arbejdstelefon~~ - bruger jeg ikke
- Min primære laptop - private
- Mine andre laptops - private
- Min arbejdslaptop - bruger jeg minimalt til private data
- NB: jeg er ikke religiøs - burde måske være mere kompromisløs
- Vær passende paranoid

Vi glemmer netværket og underholdning som Chromecast m.v

Smart Girl's Guide to Privacy

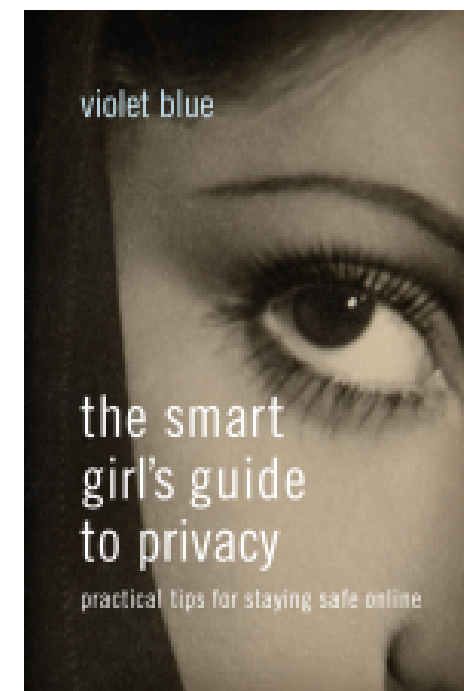


<https://www.nostarch.com/smartgirlsguide>

Practical Tips for Staying Safe Online by Violet Blue

August 2015, 176 pp. ISBN: 978-1-59327-648-5

Kan varmt anbefales! Rød, gul og grøn information



Analyse: Hvilke data



- Emails, SMS og korte tekstbeskeder, hvor er du, skal vi mødes, køb mere vodka
- Billeder - gamle, pinlige, Coffee shop?, nøgenbilleder
- Lokationsdata - hvor er du, hvor skal du hen, Google maps location history
- Breve, egne noter, private dokumenter under udarbejdelse
- Sikkerhedsinformation - inkl pentest af andres systemer
- Projekter - egne og med andre
- Koder og logins ... og data der skal nedarves

Generelle regler for mig selv



Følsomme data skal være krypterede, under transport og gemt

Følsomme data opbevares bag stærke kodeord, dvs ikke telefon pinkode

Backups skal være krypterede, Apple krypteret disk, Duplicity eller Qubes backup

Begræns mere data - brug mere Tor

Adskil applikationer og browsing mere


New 2018: Data der skal nedarves til min søn lægges på Dropbox, eller ukrypteret disk.
Worst case får politiet eller en tyv adgang til billeder fra hans barndom





A reasonably secure operating system


<https://www.qubes-os.org/>


“ WHAT THE EXPERTS ARE SAYING





"If you're serious about security, Qubes OS is the best OS available today. It's what I use, and free." 
— Edward Snowden, *whistleblower and privacy advocate*




"Happy thought of the day: An attacker who merely finds a browser bug can't listen to my microphone except when I've told Qubes to enable it." 
— Daniel J. Bernstein, *mathematician, cryptologist, and computer scientist*



"When I use Qubes I feel like a god. Software thinks that it's in control, that it can do what it wants? It can't. I'm in control." 
— Micah Lee, *Freedom of the Press Foundation, The Intercept*



"Donated a % of my consulting company's last year revenue to Qubes OS. I rely on it for all my work, and recommend it to clients too." 
— Peter Todd, *Applied Cryptography Consultant*

[More From The Experts](#)

Qubes OS er en central del af mit setup

Qubes OS eksempel



The screenshot shows the Qubes VM Manager interface. At the top, there's a menu bar with 'System', 'VM', 'View', and 'About'. Below it is a toolbar with various icons for VM management. A search bar is present. The main area is a table listing VMs with columns for Name, State, Template, NetVM, and MEM. The VMs are listed in descending order of memory usage.

	Name	State	Template	NetVM	MEM
	dom0	●	AdminVM	n/a	2924 MB
	AMSVN	●	StandaloneVM	sys-firewall	447 MB
	anon-whonix	●	whonix-ws	sys-whonix	542 MB
	backup	●	fedora-26	sys-firewall	559 MB
	Browsing	●	debian-9-plus	sys-firewall	1494 MB
	Dropbox	●	StandaloneVM	sys-firewall	1263 MB
	KaliVM	●	kali-template	sys-net	458 MB
	Mailreader	●	StandaloneVM	sys-firewall	602 MB
	Media	●	StandaloneVM	sys-firewall	1091 MB
	NMS-VM	●	StandaloneVM	sys-firewall	931 MB
	Personal	●	debian-9-plus	sys-firewall	780 MB
	Projects	●	debian-9-plus	sys-firewall	1817 MB
	sys-firewall	●	fedora-26	sys-net	424 MB
	sys-net	●	fedora-26	n/a	301 MB
	sys-usb	●	fedora-26	n/a	301 MB
	sys-whonix	●	whonix-gw	sys-firewall	516 MB
	Twitter	●	debian-9-plus	sys-firewall	630 MB
	ubuntu	●	StandaloneVM	sys-net	513 MB
	Zencurity	●	debian-9-plus	sys-firewall	355 MB

- Viser et mix af mine VMs, ikke alle
- Derudover findes Disposable VMs
- og nu tid til demo

Egen mailserver

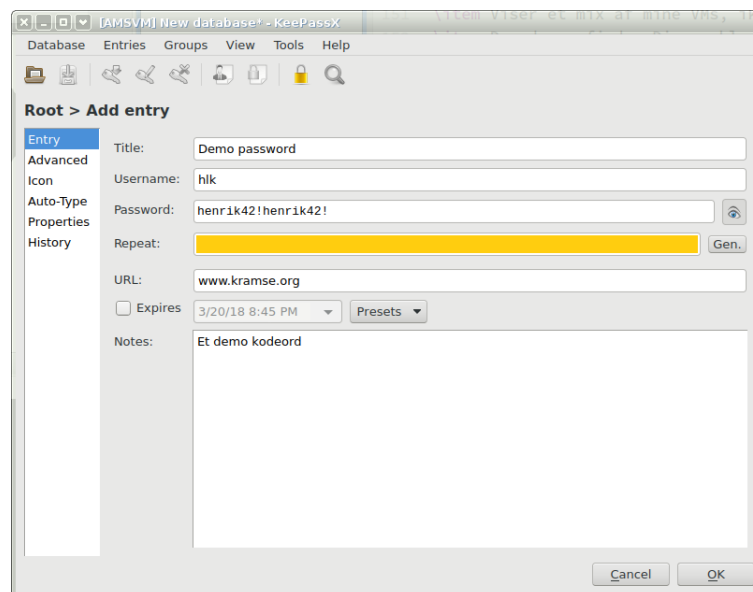


- Lidt bøvlet - specielt anti-spam
- Post modtagelse Postfix <http://www.postfix.org/>
- IMAPS <https://www.dovecot.org/>
- Anti-spam Bogofilter <http://bogofilter.sourceforge.net/>

Men har også en Google mail konto, som bruges til

- Sende data til folk direkte fra telefonen
- Modtage og opbevare koncertbilletter
- *Unclassified information*

Password safe



Kodeordshuskere er nødvendige idag

Jeg har prøvet KeePassX, LastPass, 1Password, Apple Keychain

Jeg bruger idag primært Lastpass \implies KeePassX



Følgende slides er tiltænkt som oversigt og eksempler

Tor project anonym web browsing



Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

[Download Tor](#)

- ➔ Tor prevents anyone from learning your location or browsing habits.
- ➔ Tor is for web browsers, instant messaging clients, remote logins, and more.
- ➔ Tor is free and open source for Windows, Mac, Linux/Unix, and Android

<https://www.torproject.org/>

Der findes alternativer, men Tor er mest kendt

Why use Tor?



- Your public IP is **Red Information**, often lead directly to you
- You like to browse things, without telling your ISP, the government, your teacher, ... everyone, Avoid censorship
- You want to avoid stalkers
- You are an investigative journalist or high school student researching Al Qaeda, Daesh, ISIS for school
- Consider getting the book *The Smart Girl's Guide to Privacy*
<http://smartprivacy.tumblr.com/>

Shameless plug: we are starting up danish information page and more <https://www.torserver.dk/>

Pic from <https://www.torproject.org/>

Who Uses Tor?



Internet.

Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the



accountability.

Businesses

Businesses use Tor to research competition, keep business strategies confidential, and facilitate internal



on corruption.

Activists

Activists use Tor to anonymously report abuses from danger zones. Whistleblowers use Tor to safely report



Media

Journalists and the media use Tor to protect their research and sources online.



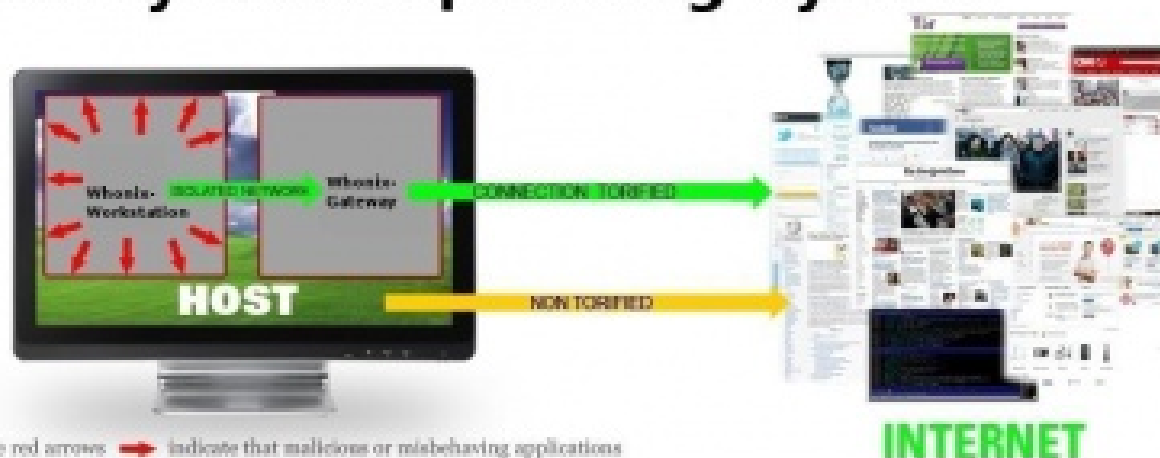
Military & Law Enforcement

Militaries and law enforcement use Tor to protect their communications, investigations, and intelligence

gathering online.



Whonix Anonymous Operating System



The red arrows → indicate that malicious or misbehaving applications can't break out of the Whonix-Workstation.
All network connections → are forced to go through Whonix-Gateway, where they are torified and routed to the Internet.

Whonix is an operating system focused on anonymity, privacy and security. It's based on the Tor anonymity network[5], Debian GNU/Linux[6] and security by isolation. DNS leaks are impossible, and not even malware with root privileges can find real IP.

<https://www.whonix.org/>



Brug flere browsere



Firefox



chrome



TorProject.org



Allow active content to run
only from sites you trust



ScriptBlock 1.0

A smart extension that controls javascript, iframes, and plugins



HTTPS Everywhere

whonix
PRIVACY & ANONYMITY OS

Fordele ved flere browsere



Flere browsere giver højere sikkerhed

Data kan ikke flyde mellem flere browsere, cookies m.m.

Mit forslag:

- En browser til *sikre sites* banken, intranet
- En browser til generel internet surfing
- En browser med alle mulige plugins, web udvikling eksempelvis

Installer gerne plugins til højere sikkerhed i allesammen:
HTTPS Everywhere, NoScript/ScriptBlock m.fl.

Det anbefales at disse installeres og vedligeholdes fra IT-afdelingen

Alle browsere har mange fejl!

Generelt indstillinger for browsere

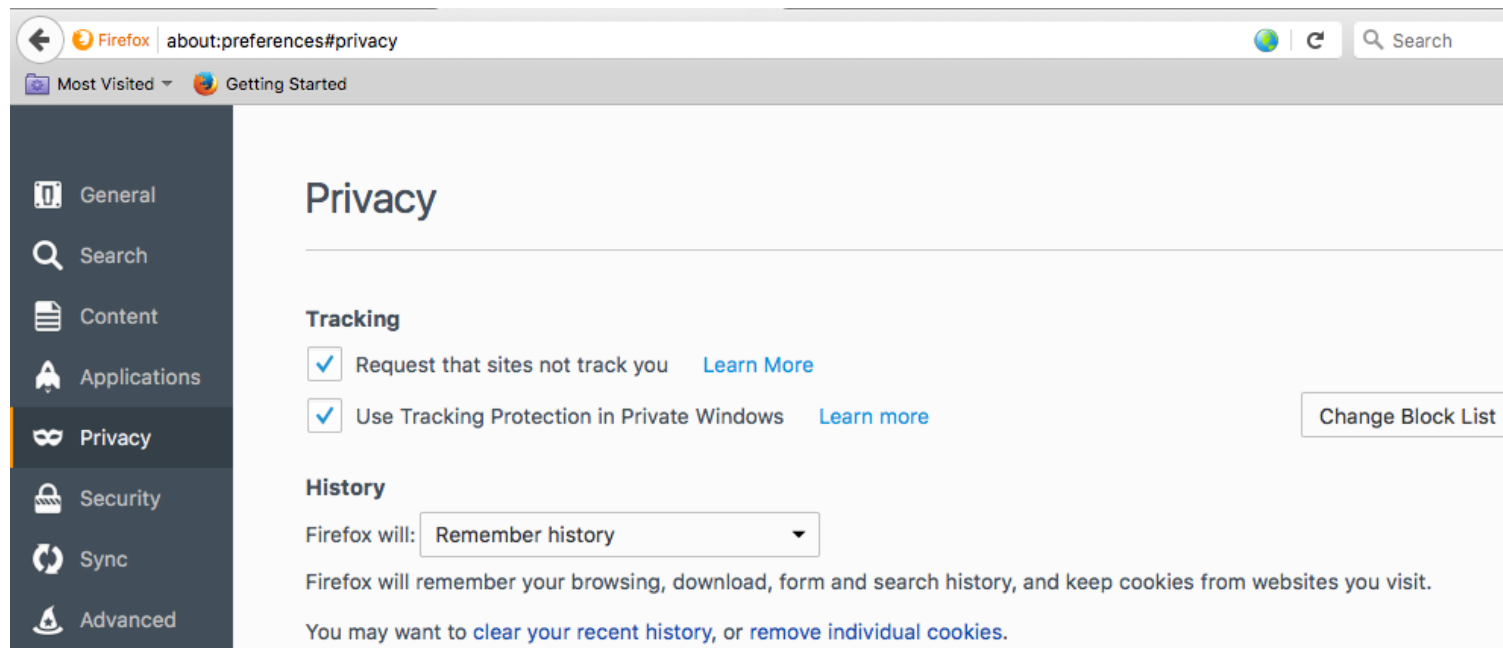


Skal være indstillet på den sikre browser til generel surf

- Slå JavaScript fra generelt med NoScript/ScriptBlock
- Slå click-to-play til for aktivt indhold
- Slå "Do Not Track" til
- Slå Java helt fra, afinstaller evt. Java helt fra computeren
- Installer en AdBlocker - jeg bruger AdBlock

Vigtigt: servere der viser reklamer er ofte mål for hacking

Hvor ændrer man indstillingerne



De fleste findes under:

- Chrome `chrome://settings/` og `chrome://extensions/`
- Firefox Indstillingerne og for enkelte ting: `about:config`

Kig også gerne på Safari eller Internet Explorer indstillingerne

HTTPS Everywhere

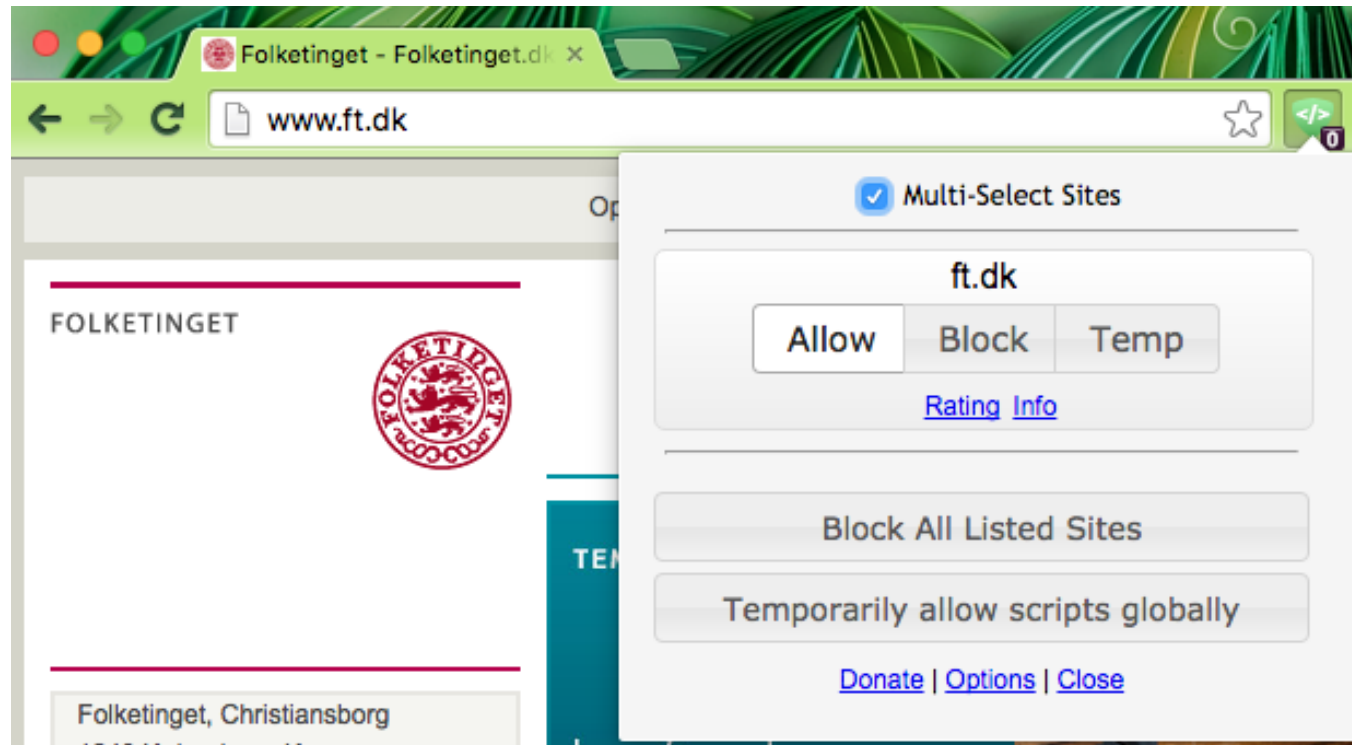


HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

`https://www.eff.org/https-everywhere`

Also in Chrome web store!

NoScript Firefox and ScriptBlock Chrome



NoScripts for Firefox eller ScriptBlock for Chrome
Tillader kun JavaScript på sider hvor det er OK

Fuld Disk Kryptering: Bitlocker

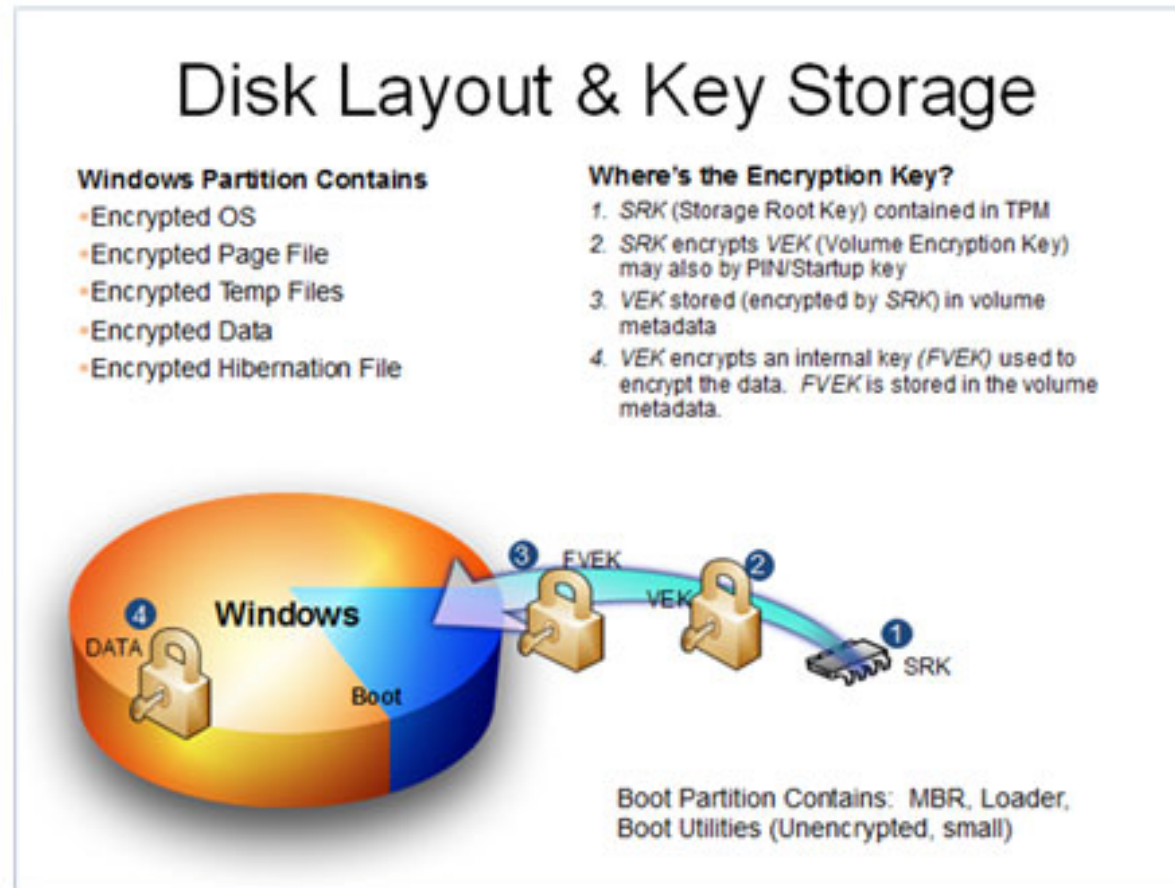


- Microsoft tilbyder Bitlocker fuld disk kryptering
- Åbnes med dit Windows kodeord
- Meget transparent - data krypteres når det skrives ned
- Nedsætter ikke hastigheden mærkbart, ofte forbedres den endda
- Genetableringsnøgle - er slået til på FT computere
Giver mulighed for at IT-afd kan åbne din computer hvis du glemmer koden
- Fungerer på både roterende diske og SSD,
men pas på SSD kan have data fra før kryptering slået til

Kilde: mere information om Bitlocker

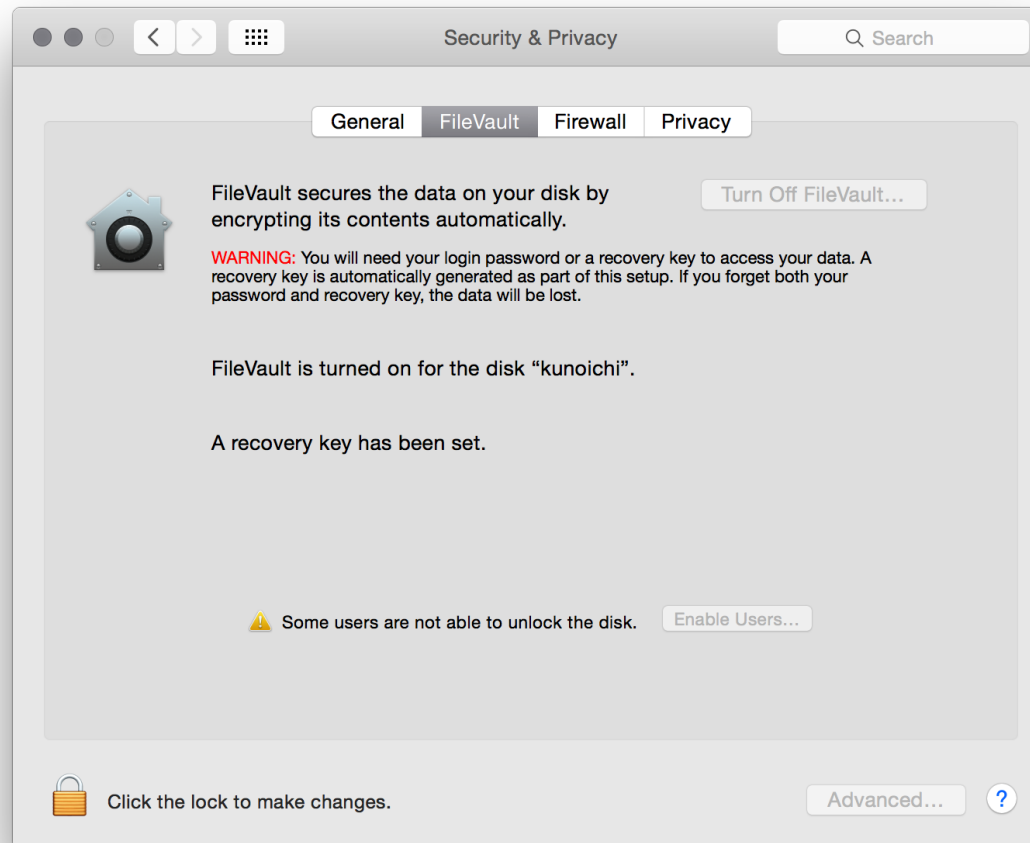
<http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview>

Microsoft Bitlocker



Kilde: <https://technet.microsoft.com/en-us/library/cc512654.aspx>

Apple FileVault Full Disk Encryption Mac OS X



Indbygget, gratis, stærk - slå det til når I kommer hjem

Keeping backup duplicate your data - sample Duplicity



What is it?

Duplicity backs directories by producing encrypted tar-format volumes and uploading them to a remote or local file server. Because duplicity uses librsync, the incremental archives are space efficient and only record the parts of files that have changed since the last backup. Because duplicity uses **GnuPG** to encrypt and/or sign these archives, they will be safe from spying and/or modification by the server.

<http://duplicity.nongnu.org/> duplicity home page

<http://www.gnupg.org/> The GNU Privacy Guard

Dont forget to DELETE data also, write over or physically destroy

Surveillance Self-Defense EFF



Tips, Tools and How-tos For Safer Online Communications

Modern technology has given the powerful new abilities to eavesdrop and collect data on innocent people. Surveillance Self-Defense is EFF's guide to defending yourself and your friends from surveillance by using secure technology and developing careful practices.

Source: <https://ssd.eff.org/>



Husk følgende:

- Husk: IT-sikkerhed er ikke kun netværkssikkerhed!
- God sikkerhed kommer fra langsigtede initiativer
- Hvad er informationssikkerhed?
- Data på elektronisk form, USB drev
- Data på fysisk form, køb en makulator
- Lav backup af data I vil gemme! Køb en ekstern USB disk til offline
3-2-1 backup 3 kopier i 2 programmer med 1 offline/slukket

Informationssikkerhed er en proces

Questions?



Henrik Lund Kramshøj hlik@zencurity.dk

Need DDoS testing or pentest, ask me!

You are always welcome to send me questions later via email

Did you notice how a lot of the links in this presentation use HTTPS - encrypted