Digital Protection and Privacy

April 2019

Wojtek Bogusz
Wojtek@FrontLineDefenders.org

Some illustrations: Assi Kootstra
Get this presentation: https://secure.frontlinedefenders.org/soc/201904.pdf

FRONT LINE DEFENDERS
THE INTERNATIONAL FOUNDATION FOR THE PROTECTION OF HUMAN RIGHTS DEFENDERS

Worrying about below digital risks?

- Account (email, social media) hacked, closed.
- Stolen, crashed, destroyed devices.
- Confiscated devices. Being arrested with devices.
- Infected devices. Phishing. Social engineering.
- Surveillance physical/digital. Phone calls/SMS interception. Phone tracking.
- Social media profiling. Using posted information against you.
- Censorship, blocking access to information.
- Your website hacked, blocked, DDoSed, closed.

Risk assessment

Path towards general protection plan

- **What** do you want to protect?
  - Where is your information stored?
  - How do you communicate? With whom?
  - Which devices and services do you use?
- **Who** do you want to protect it **from**?
  - Who can access your information, communication, meta-data? What risks does this bring?
  - Who may be interested in your information and communication?

Risk assessment

Path towards general protection plan

- How **likely** is it that you will **need** to protect it?
- How bad are the **consequences** if you fail?
- How much trouble **are you willing** to go through in order to try to prevent those consequences?

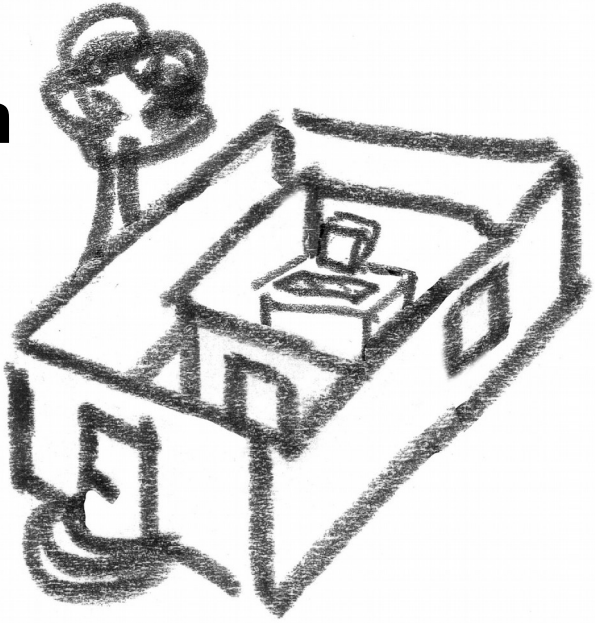
Identifying concrete **threats** to your information and **capacities** to reduce risk. Planing and implementing..

See: https://ssd.eff.org/en/module/introduction-threat-modeling

Integrated (Holistic) Protection plan

- Well-being, medical protection, legal protection, …
- Physical protection of data at work, home, when travelling, ...
- Basic security of computer, phone, operating system, programs, apps, etc.
- Protection of stored information
- How to connect to Internet and communicate securely
- Protection of services, accounts: which to use, what for, how, how are accounts connected between them, etc.

Physical protection of your information
Some questions:



- Where to store information?
  Where communicate from?
  Which devices to use?
- Where and how leave your devices, backup, ..?
  Would you recognise if somebody accessed your devices?
- How do you dispose information?
- Secure you wireless internet or cable network
- Do you connect to public/open wifi?
- Do you plug unknown devices, or plug yours to unknow computers/ sockets?
- Avoid putting portable devices on display, never leave them unattended, avoid obvious laptop bags, ...

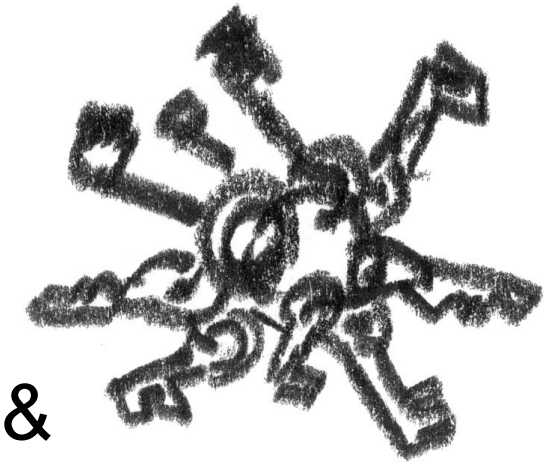
Basic protection computers, phones

- Use **lates version** of operating system
- **Update** operating system and all programs & apps frequently
- **Uninstall** all non essential programs & apps, eg.: Java, Flash, Quicktime, Silverlight, …
- Windows, Mac, Android run **anti-virus** (e.g. Avira.com, AVG.com, Windows Defender / Windows Security Essentials) & anti-spyware software (e.g. Malwarebytes.com)
- Set **user password/PIN** on computer and phone

Basic protection computers, phones

- Consider switching to good Free and Open Source Software: Firefox, Thunderbird, LibreOffice, …
  Consider switching to FLOSS operating system: Ubuntu.com, Tails.boum.org, Qubes-OS.org
- **Windows** some configuration:
  - use Hardentools
  - show file extensions: control panel > appearance > show hidden files
- **Mac**:
  - use: OverSight, BlockBlock, LockDown also maybe LuLu, DoNotDisturb, RansomWhere, KnockKnock and Task Explorer, ReiKey
  - see: The Essential Guide for Mac Security

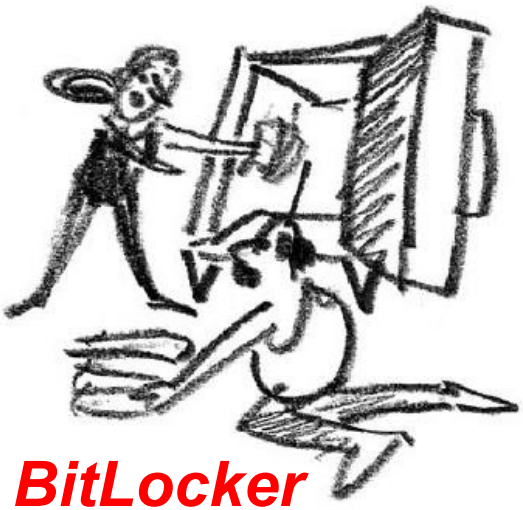
Creating and maintaining good passwords



- Use passphrase: **long and complex or random**
- **Never use the same** password twice
- **Change passwords** from-time-to-time & once it may have been compromised
- Ignore or trick **security questions** for account recovery
- **Never share** passwords and accounts
- Store your passwords securely. **Use password manager** – like **KeePassXC.org**. On phones use **MiniKeePass** and **KeePass2Android**. Maybe use online service bitwarden.com

Protection of stored information

File/Disk encryption



- **Encrypt entire disk** of your computer:
  Windows: *Control Panel* > *System and Security* > ***BitLocker***
  See Security in-a-Box
  Mac: *System Preferences* > *Security & Privacy* > ***FileVault***
  Android: Settings > *Security* > *Encryption*
- Choose **which information** to encrypt for **additional protection**
- Use **VeraCrypt**
- Use **best password skills**. Make sure your **computer is well protected**
- VeraCrypt can **encrypt whole disk** together with Windows system files

Destroying sensitive information
Wiping the traces of work

- Computers store lots of information to help us work:
  browsing history, internet cache, user names, passwords, filled web form entries, cookies, recently-used files/folders, recycle bin, temporary files and documents intermediary versions, document properties, unused space on disk, swap file, slack of clusters
- Learn how to manually wipe traces in each program..
- **Simple delete does not destroy data from disk** – use special programs to destroy unwanted or important information: Install Slim CCleaner from https://www.piriform.com/ccleaner/builds

- Wipe free space regularly (eg. on end of day)
- Wipe and destroy information on equipment you give away or dispose: old computers, disks, diskettes, cd/dvd's, ...
- Make sure you remove meta-data from your files before sending!

Recovering from information loss

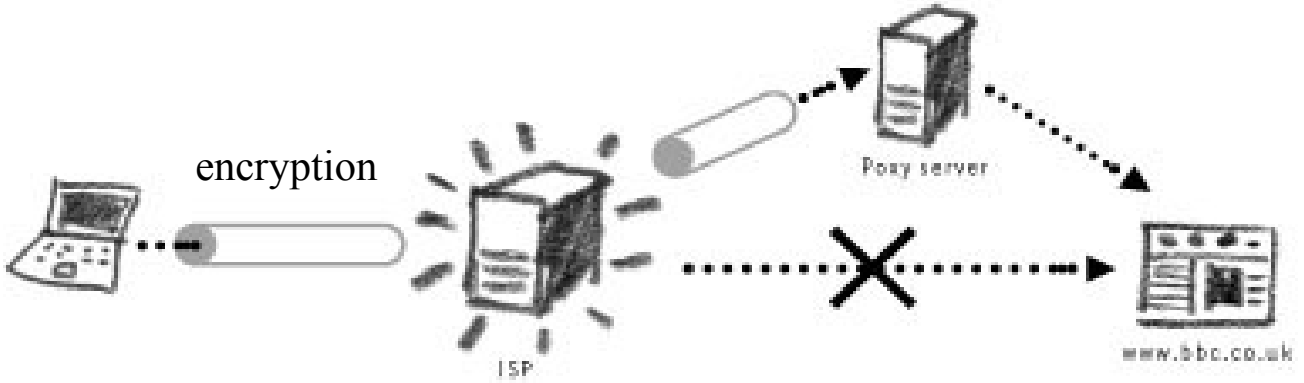
Backup

- **Organise information**
- Decide what to backup
- **Backup on regular basis** and after large work
- Choose **where** to backup
- **Keep backup separate from original files**
- **Protect backup** files, eg. encrypt with VeraCrypt
- Prepare and try in practice backup policy for computers, servers, mobile phones, office, etc.

Use default **Backup** on **Windows 7** or **Windows 10**, or use **FreeFileSync.org**
On Mac use **TimeMachine**

Interesting **zero-knowledge online backup** options:
Tresorit.com/nonprofit, Sync.com, TeamDrive.com, TrustWire.com
try encryption with: **Cryptomator.org** or BoxCryptor.com
Note that online backup brings new risks!

Protecting Internet connection, bypassing censorship, publishing information anonymously – Proxy, VPN, etc.



Proxy: intermediary computer(s) to request information.

- Trust proxy provider, all traffic pass through the proxy.
- You may try:
  - Psiphon3.net, Mullvad.com, expressVPN.com, GoldenFrog.com/vyprvpn, ProtonVPN.com, PrivateInternetAccess.com,
  - Tor Browser, getLantern.org
  - See: https://ThatOnePrivacySite.net/vpn-comparison-chart

Protecting your computer from viruses, malware and hackers

Browser Safety

Firefox :

- Install add-ons: [NoScript], HTTPS Everywhere, Privacy Badger, uBlock Origin, [uMatrix]
- Never remember and clear history (Menu: Options > Privacy, History),
- Don't Remember logins for sites (Menu: Options > Security, Logins, uncheck "Rember logins..", see "Saved Logins", and "Remove All", or at least "Use a master password")
- Menu: New Private Window – to browse without remembering history
- Configure Search Engine (Menu: Options > Search)




Chrome/Chromium :

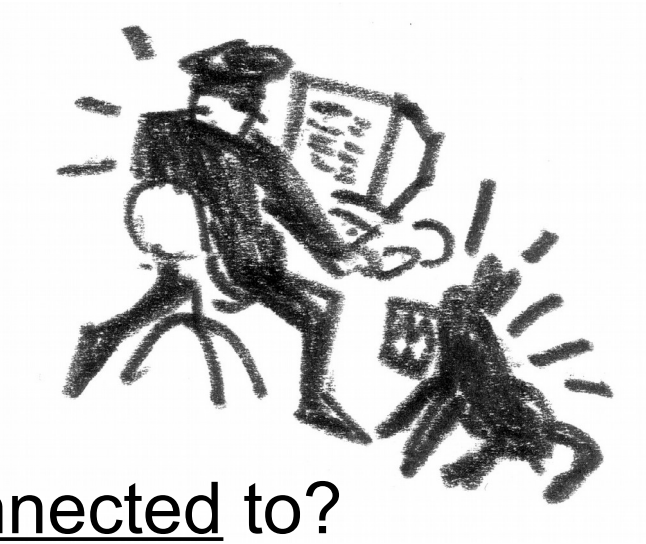
- Install extentions: uMatrix, uBlock Origin, HTTPS Everywhere, Privacy Badger
- Clear history (Menu: Settings > Show advanced settings... > Clear browsing data...)
- Don't remember login passwords (Menu: Settings > Show advanced settings... > Passwords and form, uncheck "Enable Autofill.." and "Offer to save your web passwords", see "Manage Autofull.." and "Manage passwords")
- Menu: New incognito window – to browse without remembering history
- Configure Search Engines (Menu: Settings > Search)




See https://riseup.net/en/better-web-browsing

Keeping your Internet communication private

Protect (all) accounts



- How do I change my account password?
- How do I reset the password?
  What information is needed to rest it?
- Which other accounts this account is connected to?
- What information about my real idenity is available on this account? How can I delete all stored information?
- Who has access to information on this account?
  How can I restrict access?
- What are other security options on this account (account activity; 2-factor authentication; spam filter; ...)?
  Which of those I want to use? How?

Keeping your Internet communication private

2-Factor Authentication

- Helps protect your account
- Require you to enter single use code, in addition to your password when you log in (SMS, OneTimePassword, U2F, ...)
- Google: “2-step verification”; Facebook: “login approvals”; Twitter: “login verification”
- www.twofactorauth.org - services that supports 2FA
- www.turnon2fa.com - guides how to implement it
- Best to get codes generated from an app like FreeOTP or Google Authenticator, AndOTP, Duo Mobile
- Store backup codes or QR code safely!

Social Engineering

- Social skills and human psychology manipulation used to collect information or gain an advantage.
- Starts with information gathering, moves onto relationship development and exploitation
- Some types: (spear) phishing, vishing, pretexting, baiting, tailgating, quid pro quo, etc.

See:

https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/
https://www.amnesty.org/en/latest/research/2018/12/when-best-practice-is-not-good-enough/
https://fossbytes.com/what-is-social-engineering-types-techniques/
https://www.datto.com/blog/5-types-of-social-engineering-attacks
https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering
https://www.amnesty.org/en/latest/research/2019/03/phishing-attacks-using-third-party-applications-against-egyptian-civil-society-organizations/

Social Engineering - Things to look out for

- Requests for sharing personal information
- Sense of urgency in requests / incoming messages
- Language used / Context / Content of online messages or email communications
- Offer or claim too good to be true

See: https://www.wired.com/story/resist-phishing-attacks/

https://phishingquiz.withgoogle.com/

Social Engineering - Quick Fixes

- *Be aware of the situation and context*
- *Control impulsive reactions. Curiosity, trust, and fear. Be in touch with your instincts and emotions*
- Navigate to the site separately, log in, and check what's actually going on. Or contact sender through other channel to confirm.
- Treat attachments with suspicion, avoid opening, particularly if you didn't ask for them or didn't have a pre-arranged plan to receive them
- Backup your data
- Enable multifactor authentication on every account that offers it
- Close accounts you don't use anymore
- Set up a password manager to keep track of unique, strong passwords
- *Attitude: 'my information belongs to me. I decide who I share it with, how, when'*
- *Think before you click*

Social Networking

- Who has **access** to the shared information?
- Who controls and **owns** the information once it is on a social networking site?
- What **information about me** could my contacts pass to other people?
- Would my contacts be concerned if I **share** information about them?
- Do I **trust** everyone I am connected to?
- Metta-data, Settings, Groups (public | closed | secret)

Communication apps/programs

Criteria

- **Program code available for inspection (Free and Open Source)?**
- **Transport encryption?** (https, SSL/TLS with POP, IMAP, SMTP, ..)
- **End-to-end encryption?**
- Verify contacts' identities?
- Are past communications secure if your encryption keys are stolen?
- Are information stored on the device encrypted independently?
- **What is stored on the server?** Previous conversations, contacts, ..?
- Can messages self-destruct? Can you redact/remove the messages?
- Can you use program without access to your (phone) address-book?
- Do you need to give your phone number to communicate?
- **Who's provider?** Do you trust them? Where are servers? Jurisdiction?
- Is security design properly documented? What is **experts opinion**?
- Is 2-factor authentication available?
- No need to pay for the program?
- Are meta-data protected?

Text/Voice/Video Communication

Which communicator app/service is best depends on your and your contacts situation, precautions.. but consider:

- **Signal**
- **Wire**
- Meet.jit.si

- What about: WhatsApp, Threema, Wickr, iMessage, ~~Telegram, Viber, Skype, FB Messenger, etc. etc.~~

Keeping your Internet communication private

Secure Web Mail

Choose your email server carefully:

- **Encrypted connection** (https, pop/ssl, imap/ssl, smtp/ssl)? **End-to-end encryption**..?
- Under which **jurisdiction** is it, where is the server **geographically**, where is company running server registered?
- Do you **trust** administrators? Do you **trust** management?
- 2-Factor Authentication, Spam protection, Phone App, ...
- Does it speak your **language**?
- Are you the only person in your country using this server or you **hide in the crowd**?

Keeping your Internet communication private

Secure Web Mail

- **Connection encryption**: Communication between client/browser and server is encrypted:
  - **www.riseup.net**
  - mail.google.com
- **End-to-end encryption:** communication & all emails stored on the server are encrypted. Email provider does not have access to your email:
  - **GPG/PGP (see Mailvelope.com or Thunderbird+Enigmail)**
  - www.tutanota.com or www.protonmail.com

Mobile phone network infrastructure & risks

- Phone indicate precisely geographic location to the operator at any given time
- Phone is an excellent listening device and can be used to transmit any sound (and video) within an earshot without you knowing
- For practical reasons consider mobile phone conversations not encrypted
- Do not rely on SMS messages services to transmit sensitive information securely. SMS can be intercepted, modified, stored by phone operator, blocked
- Phone can be infected with spyware, using USB, Internet, bluetooth, NFC, WiFi, etc.
- Phones are easily lost, confiscated, stolen
- Operator (& “friends”) has full access to your calls, SMS, Internet connections

.. http://www.zeit.de/datenschutz/malte-spitz-data-retention
.. https://apps.opendatacity.de/vds/index_en.html
.. https://www.youtube.com/watch?v=ucRWyGKBVzo

Mobile Phone Security – General protection

- **Never leave your phone unattended**
- Switch phone off and disconnect the battery. Use signal blocking bag. Or leave it with somebody trustful
- If you need new identity change SIM card and phone device
- Switch off: Bluetooth, NFC and WiFi if not using. Switch them on only when needed. Use them only in trusted locations.
- Do not accept and install unknown and unverified programs that originate from an unexpected sources – may contain viruses/malware.
- Connecting phone to a computer may pass malware infection.
- If you use your phone to browse the Internet, follow similar safe practices as those you use when you are on the computer.
- Observe your phone's behaviour and functionality.

Resources and help:

- **www.SecurityinaBox.org**
- https://ssd.eff.org - Surveillance Self-Defense
- https://www.digitaldefenders.org/digitalfirstaid
  - Digital First Aid Kit
- https://hygiene.digitalpublicsquare.com/
  - Hygiene in Digital Public Square
- https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide
  - The Motherboard Guide to Not Getting Hacked
- http://www.tcij.org/resources/handbooks/infosec
  - Information Security for Journalists
- **Get help! See:**
  https://www.digitaldefenders.org/digitalfirstaid/sections/investment-committee/

Get this presentation:
https://secure.frontlinedefenders.org/soc/201904.pdf