Computer Security for Activists

Protecting yourself and others

Who am I to talk about computer security?

- no technican
- involved in free software outreach
+ long term activist
+ experienced the animal protection trial

What do I mean with "computer security"?

Privacy and Autonomy: A system that only does what I want it to. It neither collects/sends data without me telling it to do so, nor does it deliberately limit my possibilities.

Mindless servants

Computers do not have their own agenda. They simply carry out instructions they are given. Regardless of where those instructions come from, whether they make any sense or are disadvantageous to us.

Who is in control?

Personal computers and mobile devices are sold as pre-configured systems. We usually only have a very limited knowledge of or influence over whose commands they follow and what really happens inside.

Why are the most commonly sold systems problematic?

With "proprietary" (= non-free) systems we are not allowed to investigate or change internal processes. We can't adjust them to our needs.

Various security aspects

All layers of computer security need to work together. If any aspect is disregarded we shouldn't trust our working environment. Most security holes are invisible.

The four security layers:

1) Hardware
2) Software
3) Network
4) Social interaction

1) Hardware

Dangers:

- unauthorised access
- limitations through crippled components
- data loss due to broken hardware

1) Hardware

Solutions:

- old devices (< Multicore/ME), Libreboot Bios
- active internet connection only when needed
- protecting against unauthorised access
- creating frequent backups

2) Software

Dangers:

- unauthorised access through back doors
- deliberately limited functionality
- data loss resulting from updates

2) Software

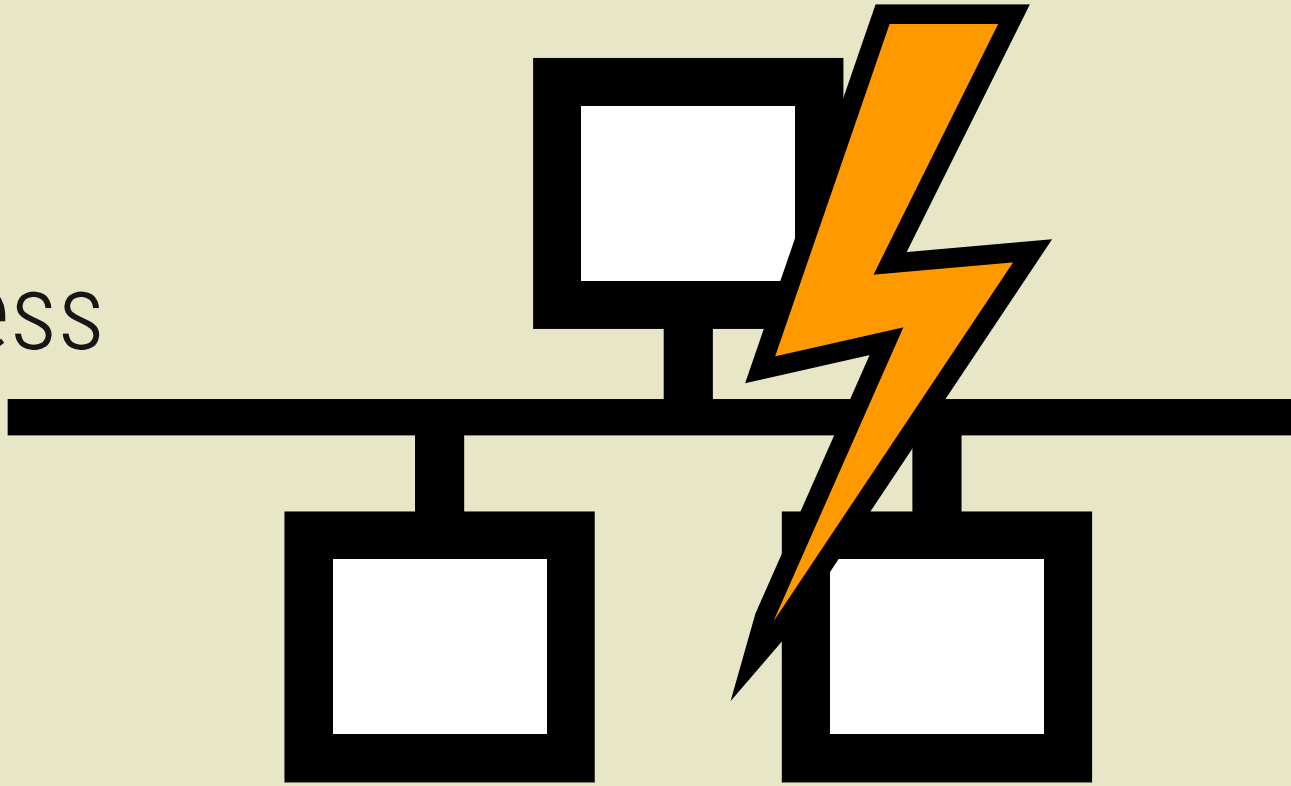
Solutions:

- free software
- encryption
- open standards (exchange formats)
- frequent backups

3) Network

Dangers:

- unauthorised access
- limitations
- surveillance
- unavailable remote data



3) Network

Solutions:

- encryption
- "de-centralised" networks
- network solutions only where necessary
- independent local backups

VGT.at
VEREIN GEGEN TIERFABRIKEN

4) Social interaction

Dangers:

- unauthorised access
- weak or disclosed pass phrases
- malicious software via sticks or downloads
- closed file formats (cooperation)

4) Social interaction

Solutions:

- use strong pass phrases
- keep access information secret
- watch devices, employ user profiles
- insist on open standards

About pass phrases 1

- at least 14 characters long
- letters, digits, punctuation
- nothing you can find in a dictionary!
- for example: „i!_tit1P*id?au347/18t“

important**! _ t**his **i**s **t**he **1 P**hrase* **i d**id**? a**ctually **u**se **347/18 t**imes

About pass phrases 2

- typing, no password manager (forgetting ...)
- no multible times and/or indefinitely usage
- secret system instead of single phrases
- no noting down without serious changes
- always change after (possible) disclosure

Mobile phones

Mobiles are always insecure. Encryption does help a little but never consider mobile phones to be trustwothy! You should view them as surveillance devices on steroids.

Aim: independence

Using free software and open standards is not only a political statement for independence. Even if free software can be less convenient at times it is still our only chance for systems that are not controlled by others.

Contact for further questions:

franz.gratzer@vgt.at

Useful links:

directory.fsf.org, emailselfdefence.org,
tehnoetic.com, duckduckgo.com, torproject.org