IT-Workshop 11.2. PROTOCOL

Q= Questions from the group

First off

No phones/devices for high level activites, best to just leave them at home (don't turn them off though, that is suspicious). To connect devices to any Internet/Wifi is high risk and not recommended if there is sensible information to be protected.

Overview - Topics

-Working safely with devices

-Tools for safer browsing

-VPNs

-Signal

-Cryptpad

-Tips for safer alternatives

-Operating system (live system) - Tails

How does the Internet work?

Everything - every activity and content on the Internet is saved on servers, they can be anywhere and everywhere. Most websites are hosted in some datacenters and they are being built everywhere (especially because of AI). Your computer accesses that server and that server sees who is accessing the website. VPNs are the Middle-Person between you and the website. They hide IP-addresses and all information on your person.

What is metadata?

Date, time, location and device information. For example deleting the metadata on pictures (Metadata cleaner) is recommended before uploading a jpeg on websites etc...

Recommendations: Exifcleaner, Exifscrambler, …

1. Safe research - The Tor Browser as VPN alternative

The issue with browsing normally is that websites can track IP-addresses, it is like your Home Address and traces the activities back to your person. Police can raid websites and access logs to find out sensible information. Hiding the IP-address is vital for save browsing. A good browser to use safely is The Tor Browser, it works with Tor nodes, they are little servers people have created and it makes Internet usage very anonymous. It is like a community based VPN and normally very safe to use. Countries have to put in a lot of effort to track information through Tor. Downside: Exit nodes make usage limited, a website knows if it is being accessed through Tor (some companies try to block those immediately - so a lot of Captchas to fill out). Google as search engine will most likely not work. Tor works on most computers.

Installment: Tor Project - Download: www.torproject.org/download/

the programme will ask you to connect manually or automatically, in AT it is fine to connect automatically. For iPhone and MacBooks there is a detailed step-for-step guide on Wikihow.

2. VPNs

VPNs hide your IP-address but they don't hide everything (there is still enough information to find out who is accessing the browser). Mullvad VPN is recommended because they don't save user data and are not based in any country. ProtonVPN is owned by a Trump supporter (also the free version is crap). Important: don't ever use a free VPN. Additional topic: DNS-queries. There is a difference between search engines and browsers!

Recommendations: Mullvad VPN, IVPN.net

Q: How does Wifi play a role in Tor usage?

A: Your Internet provider will know that you access the Tor Browser but they cannot track the content you are consuming.

Q: What is Open Source?

A: Companies produce Softwares, they write the code for a programme. As end consumer you don't see the code of a programme. Open source provides the code for people to access freely and check the code for security risks. Tip: Searching for the Open Source of a programme and check Reddit for discussions about the code. You will most likely find out if there are security risks.

3. Signal

It is not the safest Messanger out there, but it is safer than Whatsapp or SMS. There are some very safe alternatives (Matrix, Element - client for Matrix). Molly is a good workaround for Signal, but only available for Android via F-Droid (f-droid.org). It is best to do individual research and find a workaround that works for you.

Tips for safer Signal: delete Link previews, no profile picture with face on it, no linking of phone number to signal profile, hiding phone number in profile.

Q: what is the Security number on Signal?

A: they change the encryption key every few weeks, that is the security number.

Q: is there a way to use a different code for Signal than the one for the iPhone?

A: research is needed for that answer (some Molly alternative maybe?).

Q: what Information is encrypted and what not (regarding calls and messages) and what is the safe thing to do at protest?

A: normal calls and SMS are not encrypted, it is better to call over Signal or even Whatsapp, but best to not call anyone at a protest. Signal and Whatsapp calls go through the internet (which is different than from the SIM-card). If there is a SIM on you, there is GPS on you.

Q: can Trojans access deleted data on devices?

A: yes, the deleted data can still be accessible through IT-experts. Even encrypted data can be accessed, sensible information should never be saved on a technical device.

4. Cryptpad/Cryptdrive

Good alternative for GoogleDrive, there are standard text-files, documents, presentation, Kanban (interactive to do list), Form (for questionares), Diagram, … it is an open-source programme, so it is definitely safer than GoogleDocs. It is not 100% reliable so you should save important information on external hard drive (encrypted sticks). The interface of Cryptpad is not optimal for users but you can get used to it very quickly (just use a user name and password to safe) otherwise the files will delete themselves after a year.

Tip: If you have to rely on Cloud you can ZIP the files (local encryption and upload on Google for example). You can always encrypt folders on your computer and then upload them to Cloud (safer than just storing the file).

5. Tails

Tails is designed to hide your identity, it uses the Tor network to protect you from surveillance and censorship. There are limitations: you can't hide that you are using Tails or Tor. A Tail stick is a simple USB stick with the Tails operating system on it. By starting the Tails you can transform your computer into a safe(r) device because it can only use the system from the stick. If you remove the stick, the information will be deleted from the device but saved on the Tailstick. Website: tails.net - they have easy to follow manuals and you can try it on your own at home with a step-by-step-guide. It is best to do it yourself and not accept a copied Tailstick (cloning). If the stick is compromised then every copy of it will be aswell. Tails can run on a computer that has a virus, it can protect from it but it has limitations. Tails also deletes Metadata when using it. It is recommended to use Tails for one purpose at a time, because it connects the activities to each other.

Q: what capacity is needed for a Tailstick? is it illegal?

A: it is not illegal, Tails is developed by Tor (used by US government), 8GB is the minimum, that should be enough but more is better (32 or 64 is perfect). It should be a new stick, otherwise it will be slow.

Q: is there a brand you shouldn't use Tails on?

A: it is designed to make every device safer, but don't use it on government devices or already compromised BiOS, firmware or hardware.

Depending on your brand of device, you have to either keysmash or press and hold different keys while starting the laptop with the Tailstick in it. For example:

Mac Intel: Press and Hold Alt

Asus: F2 keysmash

Lenovo: F12 or Str and F12 keysmash or press and hold

Notes and Additional Topics

Tip: Open-Source Email-providers: Riseup, Systemli, Proton (you probably shouldn't for various reasons), Posteo, …

you can encrypt Emails with a PGP-Key (topic for another time)

Tip: Google Maps alternative: Open Street Maps (open source)

Tip: If the government confiscates your device you should destroy it after getting it back, don't use Tails on it or try to get documents off it.