Finabel

Food for thought paper

10 Cyber security Tips
to avoid being hacked & to keep your data safe

AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953

FINABEL
European Army Interoperability Center

This text was drawn up with the help of **Mr Fabien Galle**, trainee, under the supervision of the Permanent Secretariat.

SOCIAL ENGINEERING

- Be prudent like in the real world: clicking…
- Always keep an eye to email & website address.
- Do not open attachment or link you didn't expect: even PDF, .doc or images can be fake.
- Check physically the virtual demands, do phone check, especially when urgent request!
- Consult emails from people you do not know on a webmail interface rather than on the application installed locally on your device.
- Do not answer polls requesting personal data.

ANTI-MALWARE

- Install anti-spy/malware program in addition to your antivirus (like Spybot or Malwarebytes).
- Regularly vaccinate and scan all your devices.
- Be aware to unknown or strange file names.

ANTIVIRUS (AV) & OS UPDATES

- Paid antivirus are not necessarily the best, check https://www.av-test.org to compare. Diversify!
- Do not trust your seller: any device needs AV.
- Configure auto-update every-day in background for antivirus & operating system.
- Auto-scan all devices & drives once a week.

FIREWALL

- Configure built-in Firewall very sharply, on Windows: https://www.howtogeek.com/school/windows-network-security/lesson5/all or through the antivirus settings (Avira allows it).
- Deactivate all incoming connections or authorise only the applications you are using regularly (and use a furtive mode on MacOS).
- Configure router's firewall advance settings.

PASSWORDS

- Choose different passwords for every website.
- Use a (free) safe app capable of destructing all data in case of intrusion attempt to stock all your password with encryption (min. AES 256) in a document with the longest but memorable personal P@ssw0rd-V3ry_S&f3! of your choice, composed of series of unlinked words.
- Change only passwords when signs of hacking.
- Never give your password to someone else or change it immediately if no other solution.
- Put a code directly on all connected devices.

DEMILITARISED ZONE

- Create a separate network on which you put your private data, with no internet access, or connect with an ethernet cable your demilitarised network to your internet connected switch.
  Do not share all files.
- Encrypt sensitive data, work offline if decrypted.
- Double backup your data offline & off-site daily.
- If any breach or infection suspected, do not connect any backup disk, disconnect cloud backups, and call a cybersecurity specialist!
- Obsolete machines should be disconnected.

IDENTIFICATION

- Do not put your personal information on the internet, like your date of birth, email, address.
- Do not use your biometrics to identify because you will not be able to change it if hacked.
- Do not put any health data on the internet.
- Use different email addresses for purpose, ads.
- Never allow geolocalisation if not vital.
- Do not put personal HD photos of you or your family on the internet, or wear sun glasses.
- Do not communicate your banking information.
- Do not say when traveling before coming back.
- Destroy all your papers with a proper machine.

NETWORKS

- Never try to connect to non-protected network, public network, or too easily passworded one, without changing your firewall configurations to hard protection for in and outcoming traffic.
- Change network default password, choose long one, use WPA2 protocol, hide its name (SSID).
- Use a (free but safe) Virtual Private Network (VPN) that neither keeps logs nor sells your data, like Windscribe, with all your devices.
- Whitelist MAC addresses of your apparels.
- Limit WiFi range to your area; update firmware.
- Use Tor as internet browser to end being traced.

AUTHORIZATION

- Create a normal session in addition to your administrator one and work/surf with the first.
- Only allow people access to the less they need to work and have some control on their activity.
- Deactivate non-essential confidentiality app authorisation: contact access, camera or micro.

AUTHENTICATION

- Activate 2 factors authentification but never use SMS: always use app like Google authenticator, on a secured internet connection.
- Disconnect all your internet account at closing.
- Use different ID to log & never use real name.

Created in 1953, the Finabel committee is the oldest military organisation for cooperation between European Armies: it was conceived as a forum for reflections, exchange studies, and proposals on common interest topics for the future of its members. Finabel, the only organisation at this level, strives at:

- Promoting interoperability and cooperation of armies, while seeking to bring together concepts, doctrines and procedures;
- Contributing to a common European understanding of land defence issues. Finabel focuses on doctrines, trainings, and the joint environment.

Finabel aims to be a multinational-, independent-, and apolitical actor for the European Armies of the EU Member States. The Finabel informal forum is based on consensus and equality of member states. Finabel favours fruitful contact among member states' officers and Chiefs of Staff in a spirit of open and mutual understanding via annual meetings.

Finabel contributes to reinforce interoperability among its member states in the framework of the North Atlantic Treaty Organisation (NATO), the EU, and ad hoc coalition; Finabel neither competes nor duplicates NATO or EU military structures but contributes to these organisations in its unique way. Initially focused on cooperation in armament's programmes, Finabel quickly shifted to the harmonisation of land doctrines. Consequently, before hoping to reach a shared capability approach and common equipment, a shared vision of force-engagement on the terrain should be obtained.

In the current setting, Finabel allows its member states to form Expert Task Groups for situations that require short-term solutions. In addition, Finabel is also a think tank that elaborates on current events concerning the operations of the land forces and provides comments by creating "Food for Thought papers" to address the topics. Finabel studies and Food for Thoughts are recommendations freely applied by its member, whose aim is to facilitate interoperability and improve the daily tasks of preparation, training, exercises, and engagement.

FINABEL
Quartier Reine Elisabeth
Rue d'Evere 1
B-1140 BRUSSELS

Tel: +32 (0)2 441 79 38
GSM: +32 (0)483 712 193
E-mail: info@finabel.org

You will find our studies at
www.finabel.org

Responsible publisher: Mario BLOKKEN - Finabel Permanent Secretariat - QRE - Rue d'Evere,1 - B-1140 Brussels - +32 (0)2 441 79 38