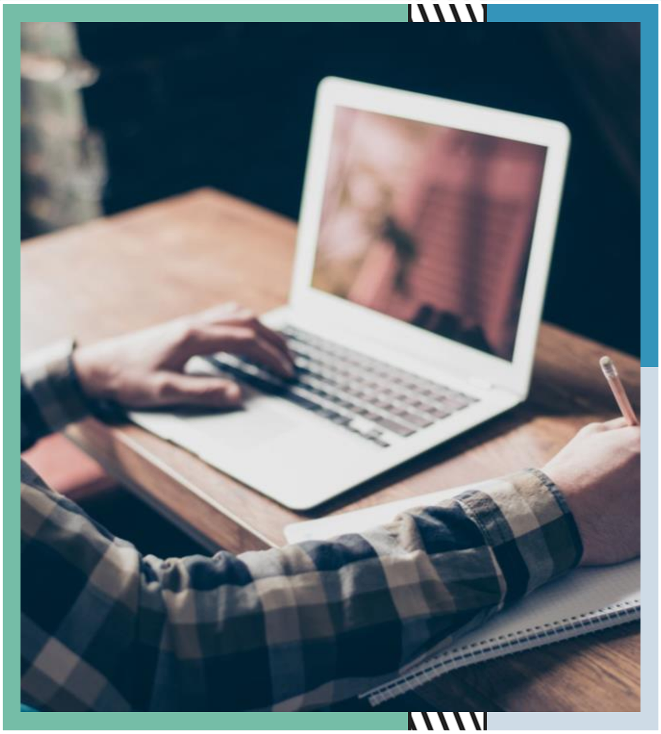
4. Guide for an Ethical, Secure and Non-Biased Behavior in the Digital World



Apply proper measures to keep personal data, information and knowledge safe

Respect property rights on data, information and knowledge

Respect data, information and knowledge confidentiality, integrity and accessibility

Identify your valuable data, information, and knowledge.

- ❑ Ask yourself about potential benefits generated by the data, information and knowledge stored on your devices.
- ❑ Assess potential costs associated to the loss, errors, or unavailability of your files.
- ❑ Can your image be affected if data about you is available to different third parties?

Sort your valuable data, information, and knowledge by importance.

Your data, information and knowledge can be important from at least three different perspectives: their confidentiality, integrity and accessibility.

❑ Decide for each file/message/storage unit you are interacting with what are the needs for its' confidentiality (C), integrity (I) and accessibility (A).

❑ Be sure that the C.I.A. triad is your filtering tool in each stage of data, information and knowledge processing.

Asses your responsibility as data, information, and knowledge owner, co-owner or user.

- ❑ What are your responsibilities for each file/message/storage unit?
- ❑ What rights do you have for each piece of data, information and knowledge?
- ❑ Be careful especially while working with your colleagues in shared documents!

A good understanding of the functioning of the e-learning platforms and other software used during the studies helps a lot – the problems in use will decrease and the learning environment will become more comfy and fruitful.

- □ Read all the instructions provided by the admin and teachers – many answers are already there!
- □ Accept without delays all the suggested periodic updates (of course, after checking that they come from a reliable source).
- □ Identify the contact data of the persons that can help you when you are in trouble with the educational software and use them when in need!
- □ Do not leave any incident or problem you have noticed unreported – maybe it is of interest for your peers.

Take care of your devices!

- ❑ Don’t leave your devices exposed.
- ❑ Block them even for a short absence.
- ❑ Use multiple authentication factors. If your device supports it, use biometric authentication (fingerprint, voice, or face).
- ❑ Change the default passwords. Create a random password or Personal Identification Number (not your birthdate, phone number or other data that can be derived easily by an attacker).

05 - 1

Take care of your devices!

- ❑ Monitor battery usage on your' device and, in the case of suspicious spikes in CPU usage, scan for the presence of spyware or file-based miners (ENISA 2021).
- ❑ Do not connect to unsecured public Wi Fi networks. In any case, do not send sensitive financial data while you use an unsecured Internet connection!
- ❑ Do not connect your device to untrusted PCs or charging stations.

Be careful when installing mobile applications!

❑ Don't rush when installing a new app. Assess its' trustworthiness by identifying and analyzing the developer, in order to sort the genuine from bogus applications. Identify the rating and read the negative comments first.

❑ Read careful the security policies, terms and conditions for every app you use, or you are about to download. If they require an exaggerated access to your data, think twice before installing them!

Be careful while using mobile applications!

- ❑ Regularly update your operating systems and applications.
- ❑ Do not open links received from unknown senders in SMS messages and chats. Even if you know the person suggesting an application, remain vigilant. Never confirm requests for installation of third-party software on your smartphone (positive technologies 2019).
- ❑ Disable automatic execution of code and macros in your applications.

Be careful while browsing!

- ❑ Look only for secure connections. In your browser, check if the URL starts with HTTPS or if a small lock is visible. Check the information about the website by clicking on the small lock.
- ❑ Check the domain name of the websites you visit for typos, especially for sensitive websites (e.g. bank websites).

Use the e-mail with utmost care!

- ❑ Stay vigilant when going through your inbox. Do not click on links or download attachments if you are not absolutely confident about the source of an e-mail.
- ❑ Carefully check links before opening them, even if you are a client of the company that sent the email. If the linked address contains any misspellings, the email is not genuine.
- ❑ Remember that bank employees never ask for full card information (positive technologies 2019).
- ❑ Avoid responding to new links received in e-mails or SMS messages by unknown senders and, most of all, do not enter your credentials when following such links (ENISA 2021).

When you write an e-mail, don’t get confused to a spammer.

1. Before starting, make sure you cannot find the answer by yourself;
2. Use a clear and informative subject line;
3. Use a proper greeting;
4. Structure your e-mail as a formal letter;
5. Include only necessary information;
6. Proofread grammar & tone;
7. Say thank you and sign you e-mail with your full name and any other relevant data (specialization, year of study, ID etc). (Gunner 2022)

Use your academic e-mail only for academic purposes. Create a separate e-mail account for non-academic activities.

Authentication tips & tricks

- ❑ Use a strong and unique password for every online service. Re-using the same password for various services is a serious security issue and should be always avoided. Using a password manager software will make managing of the whole set of passwords easier. (ENISA 2021)
- ❑ Adequately protect all identity documents and copies (physical or digital ones) against unauthorised access. (ENISA 2021)
- ❑ Identity information should not be disclosed to unsolicited recipients and their requests by phone, e-mail or in person should not be answered. (ENISA 2021)

Security software: the basic toolkit

❑ Use only licensed & updated software.

❑ Use an anti-malware solution (antivirus + antispyware …) for every device you are using. Help the antimalware solution with an aware and careful your behavior while using Internet services.

❑ Be sure that you are protected by a firewall. A licensed and updated operating system already has one.

Backup is important. Really important

- □ Backup
- □ Backup,
- □ Backup ...
- □ ...
- □ Implement secure and redundant backup practices!

Keep up with recent cybersecurity trends, developments and advice!

enisa
European Network
and Information
Security Agency

This Photo by Unknown Author is licensed under CC BY-NC-ND

ENISA. 2021. ”ENISA Threat Landscape 2021 - April 2020 to mid-July 2021.” doi:10.2824/324797

Gunner, Jennifer. 2022. ”How to Write a Clear, Polite Email to a Teacher.” YourDictionary. Haettu 3. 3 2022. https://grammar.yourdictionary.com/writing/how-to-write-a-clear-polite-email-to-a-teacher.html

positive technologies. 2019. ”Vulnerabilities and Threats in Mobile Applications, 2019.” positive technologies. https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/

References