

Elementary data security checklist

Checklist for the most basic security rules students have to follow when working on a data project.

8 things to check in regard to the data security within your business:

- Ensure your Operating System is up to date:
 - Updates are important to keep your computer secure from hackers.
- Ensure you periodically check for malware:
 - Malware opens your IT systems up for attack and data theft.
- Ensure your antivirus software is up to date:
 - New computer viruses emerge every day, make sure your antivirus software knows to detect and remove them before they cause harm.
- Ensure your router and networking options are set correctly:
 - Ensure your network is safe and secure, check for open ports.
- Ensure your personnel is aware of cybersecurity issues:
 - Users are the biggest threat to security, ensure they know the best practices and company policy.
- Ensure you periodically backup your data:
 - Use automated backup services like OneDrive, IDrive, and Dropbox Business to prevent loss of business-critical data.
- Ensure you choose unique and complex passwords and store them securely:
 - Use multi-factor authentication when available.
- Consider getting cybersecurity insurance:
 - As a precautionary measure, consider insurance that covers cyber damages and recovery.

7 precautions to take when working with data in a project:

- Always be aware of the confidentiality of data and be careful with how you work with, share, and save data.
- Save data of a project in a special folder for the project;
- Work on the data locally, not in the cloud, so don't use Dropbox/Google Drive/Onedrive etc;
- Send data in a zipped file (with a password) on the web. Send the password via an sms, whatsapp message or any other channel;
- Bitlock your harddrive, so it is not accessible when stolen;
- Make sure your computer has a password;
- Don't share your code on Github;
- Delete data after the termination of the project.