Basic security practices regarding passwords and online identities

End Users

- Do not to reuse the same password for multiple accounts (attackers often try to re-use compromised passwords to access other services).
- If a password is stolen, it must immediately be changed (also get in contact with the respective online service).
- Use complex passwords longer than 8 characters, which contain alphanumeric and special characters.
- A long password does not mean it is hard to remember: four random common words mixed with special characters make a password strong and easy to remember.
- Change passwords for online services regularly.
- Make use of passwords managers.
- Prefer service providers that offer two-factor authentication.

Service Providers

- Never store a password in plain text; store only cryptographic versions of the passwords.
- In addition, a used password hash algorithm should contain further security measures by implementing salt and multiple iterations over the initial hash (i.e. Salted SHA-256.)
- Keep your systems updated and patched, and apply common hardening principles in order to avoid attacks like SQL injections and XSS.
- Every password-based authentication must enforce a proper password policy for things like minimum length, complexity, renewal frequency, etc.
- Deploy two factor authentication where possible
- Use additional tools like CAPTCHA or similar in order to prevent automated attacks
- When providing access to sensitive or critical information, service providers should implement two-factor authentication schemes.

For any further question and information, please get in contact with your nearest CERT[1]!

[1] https://www.enisa.europa.eu/activities/cert/background/inv