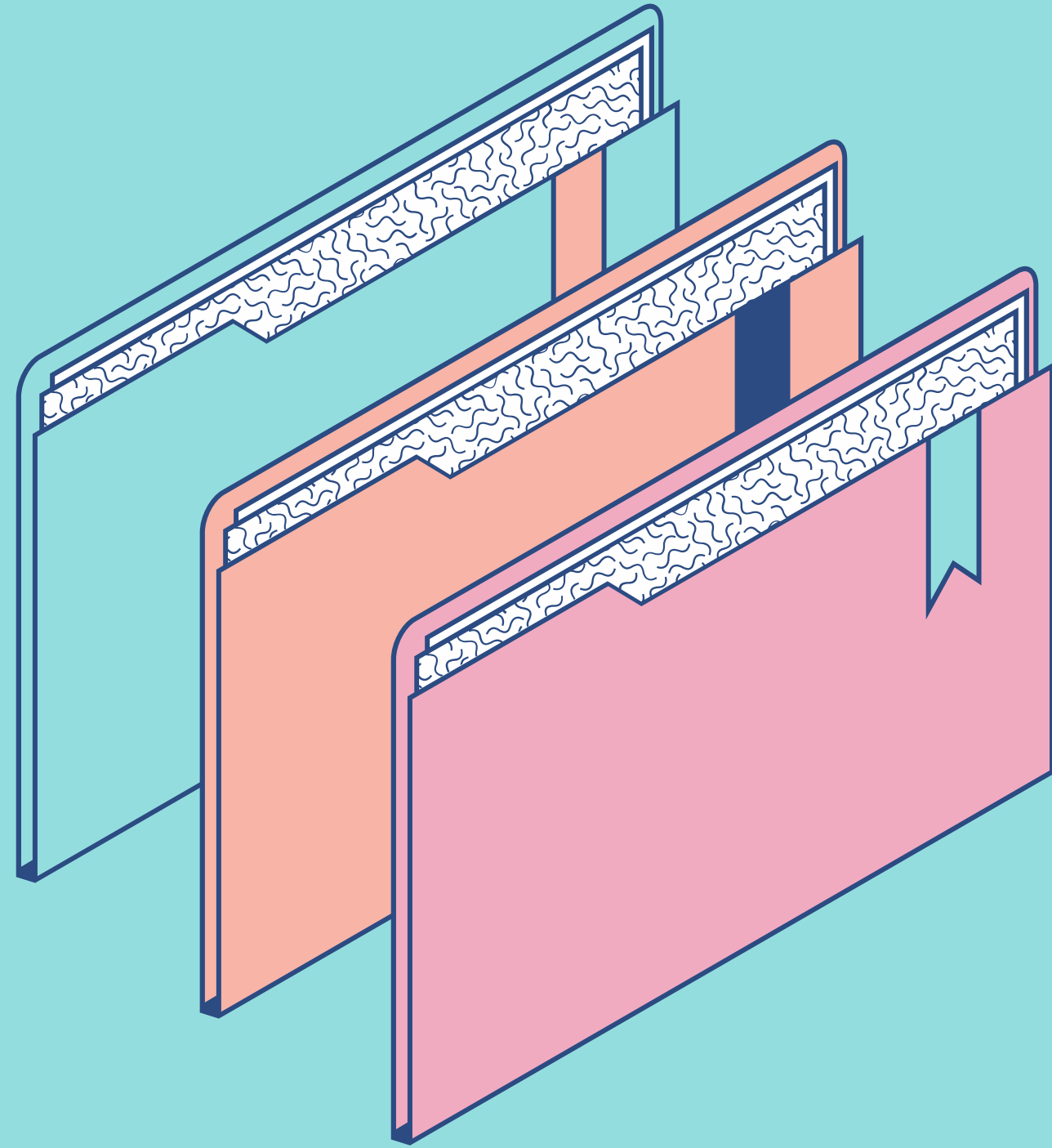




# PERSONAL DATA

Data Protection



# What are considered personal data?

Personal data is any information that allows the identification of a specific person. This can include name, address, phone number, email, photograph, date of birth, social status, medical records, financial data and others.

# Why is data protection important?

- **Confidentiality**

If data falls into the wrong hands, it can lead to identity theft, fraud or other problem.

- **Personal safety**

Disclosure of data can pose a threat to personal security.

- **Legislation**

Violation of legislation can lead to fines or other legal consequences.

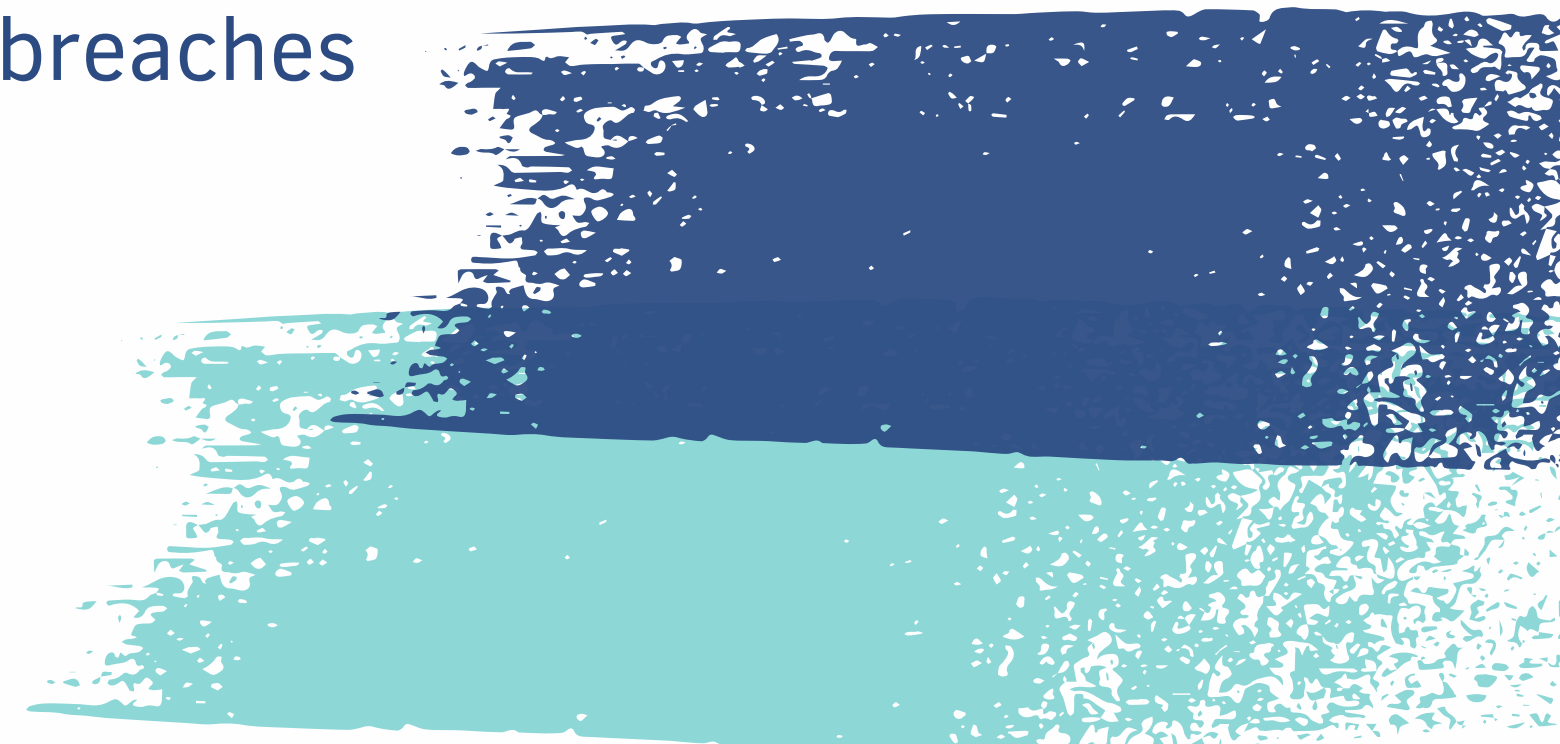
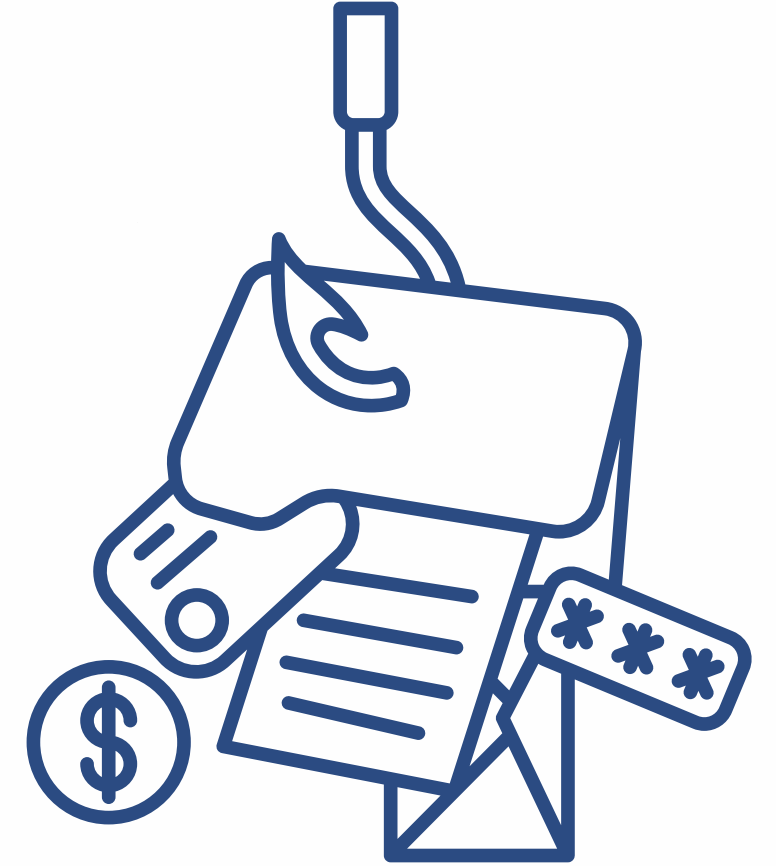


## What can be the consequences of personal data breaches?

- Identity theft risk
- Reputation loss risk
- Violation of legislation

## What methods do criminals use to access personal data?

- Phishing
- Malware
- Social engineering
- Data security breaches



# Measures to Protect Personal Data

**1**

Do not respond to emails or messages that request your logins and passwords.

**2**

Install antivirus software and update it regularly.

**3**

Use complex passwords and do not use the same password for different accounts.

**4**

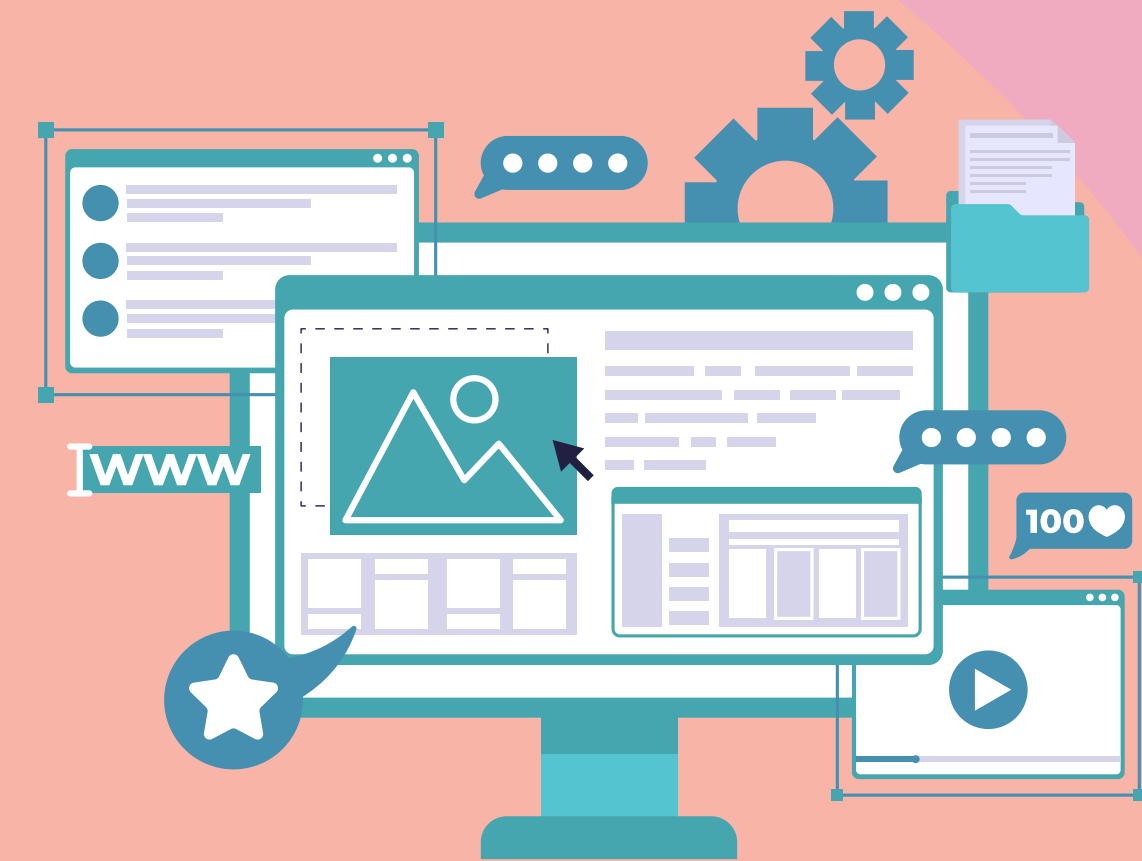
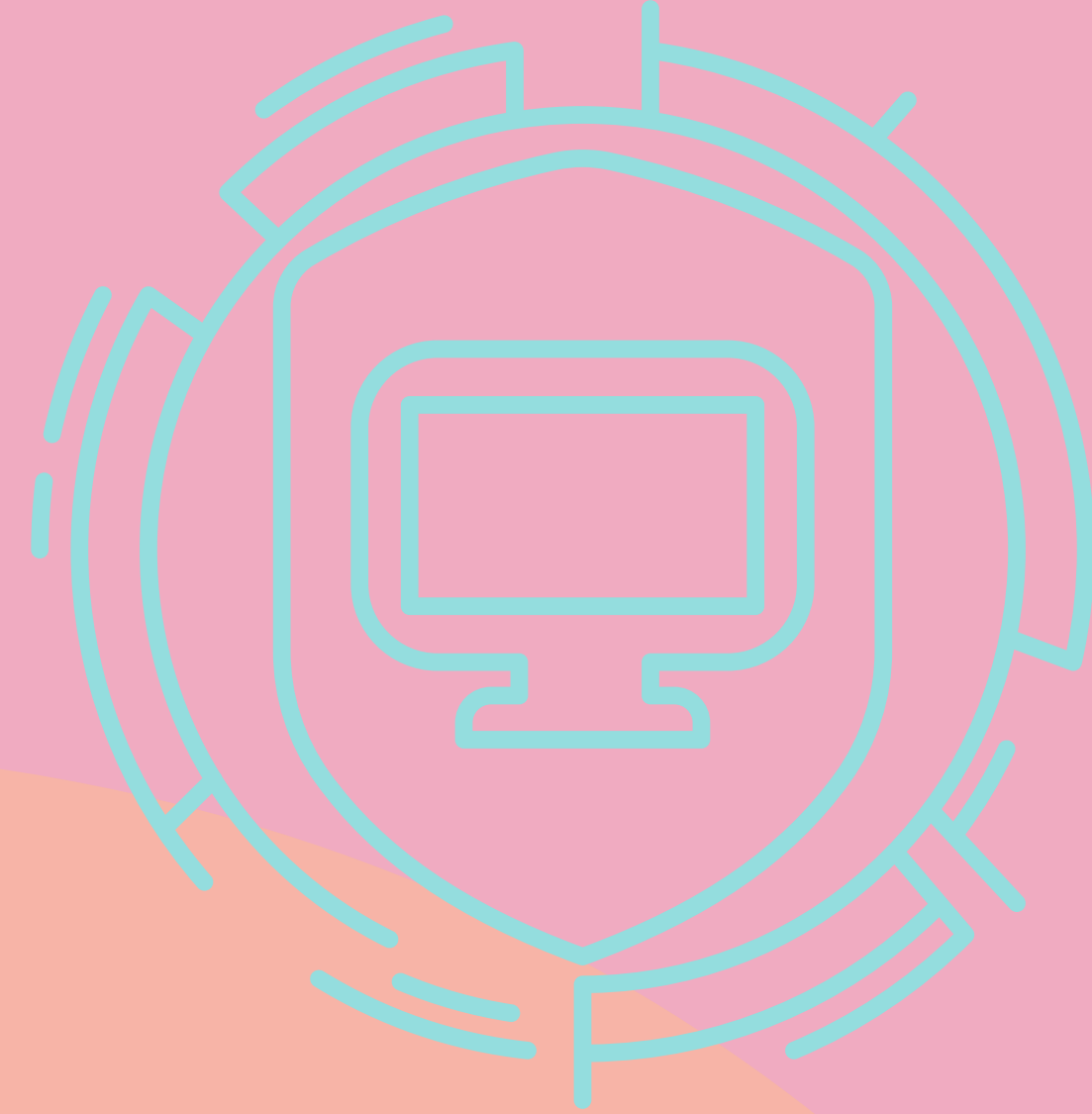
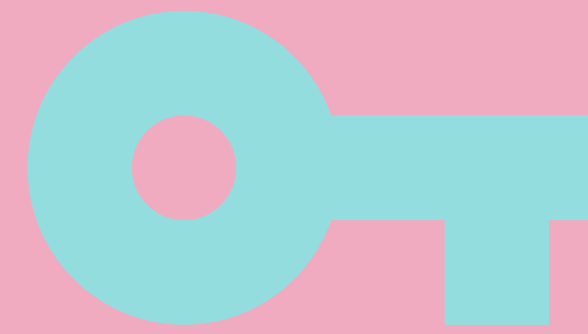
Use two-factor authentication where possible.

**5**

Update software and operating systems on your computer and mobile device.

# Technologies for protecting personal data.

- Data encryption
- Firewalls
- Antivirus software
- VPN
- Biometric authentication
- Multifactor authentication



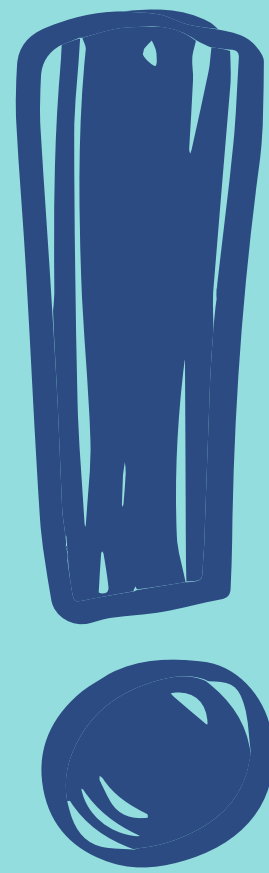


# Data Protection Legislation

Key provisions of data protection legislation include:

1. Consent to the processing of personal data.
2. Purpose of collecting and processing personal data.
3. Ensuring the security of personal data.
4. Data subject rights.
5. Responsibility for violating data protection legislation.

**Protecting  
personal  
data is very  
important.**



Protecting personal data is an extremely important task in the modern world, where more and more information about us is stored digitally. Unauthorized access to this information can lead to serious consequences such as theft of personal funds, fraud, identity theft, etc. Additionally, compromising personal data can damage the reputation and trust in companies and organizations that store this data. Therefore, protecting personal data should be a top priority for anyone who works with digital information.



# Do you have any questions?

We hope you  
learned something new.

