Fact Sheet 1: Ransomware

What is it?

Ransomware is a type of malicious software (malware) that encrypts your files or blocks access to your computer. To regain access, the attackers demand the payment of a "ransom", usually in cryptocurrency.

Example

Imagine that you receive an email with a suspicious invoice attached. When you open the file, your screen freezes and a message appears demanding money to unlock your documents, photos, and work.

Prevention

1. Don't open attachments or click on links from unknown senders.
2. Keep your antivirus and operating system up to date.
3. Back up regularly, to an external disk or to the cloud.
4. Be wary of messages that misspell or push for immediate action.

Cultural Note

"Prevention is better than cure."

Funded by
the European Union

Fact Sheet 2: Phishing

What is it?

Phishing is a digital fraud technique that tries to trick you into stealing personal data, banking or passwords. Typically, criminals send fake emails, SMS, or messages that appear to come from legitimate companies such as banks or online services.

Example

You receive an email that looks like it's from your bank. The logo and styling are identical to those of the real seat. The email says that you need to update your details urgently and includes a link. You click and are immediately redirected to a fake website... and your data goes directly to the attackers.

Prevention

1. Never click on links or open attachments to suspicious messages.
2. Confirms the sender: a strange or erroneous address is a red flag.
3. Do not share personal data by email or message.
4. Enable two-factor authentication (2FA) on your accounts.
5. If you have any questions, please contact the official entity directly.

Cultural Note

"All that glitters is not gold."

Funded by
the European Union

Sheet 3: Identity Theft

What is it?

It consists of the misuse of personal data (such as name, tax number, address or bank details) to commit fraud or crimes, without the victim's consent."

Example

A person uses your data to open a bank account, hire services or apply for a loan in your name.

Prevention

1. Do not share personal data on unsecured websites or social networks.
2. Use strong and different passwords for each account.
3. Enable two-factor authentication whenever possible.
4. Regularly check your bank statements and communications from financial institutions.
5. Be wary of suspicious contacts who ask for personal data or security codes.

Cultural Note

"Caution and chicken broth never hurt anyone."

Funded by
the European Union

Fact Sheet 4: Social Engineering

What is it?

Social engineering is a psychological manipulation technique used by cybercriminals to trick people into revealing sensitive information (such as passwords, bank details, or security codes).

Example

You receive a call from someone who introduces themselves as a technician from your internet provider. The person seems to know your name and says there's an urgent problem with your account. To solve it, ask for your password or MB WAY code.

Prevention

1. Never reveal passwords, PINs or codes to anyone.
2. He is suspicious of urgency, pressure or threats in the speech.
3. Always confirm the person's identity through official channels.
4. Remember: serious companies never ask for sensitive data by phone, email or message.

Cultural Note

"When the alms are too much, the poor are suspicious."

Funded by
the European Union