60 Anos Setronix desde 1966

OCTOBER
2026
SECOND HALF | PREVENTION



CYBERSECURITY
STOP AND CHECK

An urgent message still needs to be checked.

1. Hazards and risks

Hazards: Fake messages, suspicious attachments and links.

Risks: Data theft, fraud and unauthorised access to accounts.

2. Before you start

- Check the sender's full email address.
- Verify requests using a contact you already know.
- Use only approved applications and channels.

3. Stop and report

- Requests for a password or access code.
- Urgency, secrecy or changes to bank details.
- Already clicked or shared data? Report immediately.

4. What to do: four prevention steps

1 

Read
Check the sender and context.

2 

Verify
Use an independent contact.

3 

Protect
Do not share credentials or codes.

4 

Report
Use the relevant internal reporting channel.

5. Choose the right preventive measure

Situation	Preventive measure
Email / SMS	Do not open attachments or links until you verify their source.
Payment requests	Verify changes through another known channel.
Accounts / credentials	Use unique passwords; enable MFA where available.
Possible incident	Keep the message; follow IT support instructions.

Good practice: Do not rely only on the display name or how a message looks. Multi-factor authentication (MFA) adds protection; never share its codes.

6. FORTNIGHTLY ACTION Before clicking on an unexpected message, verify its source. Identify the internal channel for reporting concerns.

READ • VERIFY • PROTECT • REPORT

CNCS: good practice CNCS: passwords