Put a STOP to spear phishing!

S Stop: pause before taking action

T Test: check the address, links, and attachments

O Observe: when in doubt, use another channel

P Proceed: report the scam or continue working

How to build a habit?

1. Apply the STOP technique at least 21 times
2. For each use of STOP, tick a box at the bottom
3. If 21 applications are not enough, download the template from the website (QR code on the back) and repeat the process

Report suspected fraudulent messages to: **csirt@muni.cz**

☒ □ □ □ □ □ □ □ □ □

What can you do for yourself?

Technical measures:

- Multi-factor authentication + password manager
- Antivirus program + automatic updates
- Disk encryption + backup
- Use eduVPN on public Wi-Fi
- Utilize the university's M365 and Google Workspace services

Habits for safe online activity:

- Process emails and communication consciously (STOP technique helps)
- Regular cybersecurity training
- Report incidents and suspicious communication
- Replace outdated hardware (5+ years)

Manager responsibilities:

- Shared responsibility for resolving incidents at your workplace
- Follow the instructions of the MU Cybersecurity Team
- Don't delay reactions and decisions, ask for an explanation of the problem's essence

What can you do for your employees?

- **Lead by example**
- Ensure adherence to MU IT Rules
- Require the implementation of the same technical measures you follow
- Ensure regular cybersecurity training
- Motivate employees to use IT services and tools effectively

SCAN ME

Build the habit

S	Stop: pause before taking action
T	Test: check the address, links, and attachments
O	Observe: when in doubt, use another channel
P	Proceed: report the scam or continue working

✉ Report suspected fraud to: csirt@muni.cz.

Use the STOP technique at least 10 times this week to make it a habit.

○ ○ ○ ○ ○ ○ ○ ○ ○ ○