Co můžete udělat pro sebe?

Technická opatření

- Vícefaktorové ověření + správce hesel
- Antivirový program + Automatické aktualizace
- Šifrování disku + zálohování
- Na veřejné WiFi jen s eduVPN
- Využívejte možnosti univerzitních M365 a Google Workspace

Návyky pro bezpečný pohyb v online prostředí

- Zpracovávejte e-maily i komunikaci vědomě (STOPka vám pomůže)
- Pravidelně kyberbezpečnostní školení
- Incidenty i podezřelou komunikaci hlaste
- Obnovujte zastaralý HW (5+ let)

Povinnosti vedoucích

- Spoluodpovědnost za dořešení incidentů na vašem pracovišti
- Řiďte se pokyny Kyberbezpečnostního týmu MU
- Reakci a rozhodnutí neodkládejte, nechte si vysvětlit podstatu problému

Co můžete udělat pro své zaměstnance?

- **Jděte příkladem**
- Dbejte na dodržování Pravidel IT MU
- Požadujte zavedení technických opatření, jež uplatňujete vy.
- Zajistěte pravidelné kyberbezpečnostní školení
- Motivujte zaměstnance k efektivnímu využívání IT služeb a nástrojů

SCAN ME

Dejte STOPku spearphishingu!

S	Stůj: zastav se před akcí
T	Testuj: zkontroluj adresu, odkazy, přílohy
O	Ověřuj: při pochybnostech ověř jiným kanálem
P	Pokračuj: nahlas podvod nebo pokračuj v práci

Jak vybudovat návyk?

1. Aplikujte STOPku alespoň 21x
2. Při každém použití STOPky zaškrtněte jedno políčko na spodním okraji
3. Je-li 21 aplikací málo, stáhněte si šablonu z webové stránky (QR kód na zadní straně) a postup opakujte

Podezření na podvodné zprávy hlaste na:
csirt@muni.cz

Vybudujte si návyk

S	Stůj: zastav se před akcí.
T	Testuj: zkontroluj adresu, odkazy, přílohy.
O	Ověřuj: při pochybnostech ověř jiným kanálem.
P	Pokračuj: nahlaš podvod nebo pokračuj v práci.

Podezření na podvod nahlaš na: csirt@muni.cz

Použijte STOPku alespoň 10x během tohoto týdne, ať se vám dostane do krve.