



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

Co můžete udělat pro své zaměstnance?

Dejte ku 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 hlase na:
csirt@muni.cz

- ### Návky pro bezpečný pohyb v online prostředí
- Zpracovávejte e-maily i komunikaci v domě (STOPka vám pomůže)
 - Pravidelně kyberbezpečnostní školení
 - Incidenty i podezřelou komunikaci hlase
 - Obnovujte zastaralý HW (5+ let)

Povinnosti vedoucích

- Spolu zodpovědnost za dořešení incidentů na vašem pracovišti
- Řídit se pokyny kyberbezpečnostního týmu MU
- Reagovat a rozhodnutí neodkládejte, nechte si vysvětlit podstatu problému

Technická opatření

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

Vybudujte si návyk



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



P

Pokračuj: nahlaš podvod nebo pokračuj v práci.

O

Overňuj: při pochybnostech overň jiným kanálem.

T

Testuj: zkontroluj adresu, odkazy, přílohy.

S

Stůj: zastav se před akcí.