

# Bezpečnostní checklist v době AI od Red Button EDU

## Hesla a přihlašování

- Zaměstnanci používají password manager  
1Password, Bitwarden nebo KeePass
- Hesla jsou náhodně generovaná (16–32 znaků)  
Žádné kombinace oblíbených slov a čísel
- Každá služba má unikátní heslo  
Jedno heslo = jedno místo úniku
- Dvoufaktorové ověřování je zapnuto všude, kde to jde  
Ideálně přes autentizační aplikaci, ne přes SMS

## Ověřování identity

- Lidé vědí, jak ověřit podezřelý telefonát nebo videohovor  
Jiný kanál, tajné heslo v rodině/týmu
- Je nastaven jasný postup pro citlivé požadavky  
Převody peněz, přístup k datům — vždy ověřit jinak
- Tým rozumí hrozbě vishingu a deepfake hovorů  
Naléhavost a tlak = nejčastější signál útoku

## Práce s AI nástroji

- Víte, jaké AI nástroje vaši lidé reálně používají  
Včetně neschválených — Shadow AI
- Firemní a zákaznická data nejdou do neschválených nástrojů  
Žádné citlivé informace mimo oficiální systémy
- AI nástroje mají přístup jen k nezbytným datům  
Citlivá data se anonymizují ještě před použitím
- Lidé nepoužívají slepý copy-paste z neznámých zdrojů  
Prevence Prompt Injection útoku
- Prompty jsou před odesláním vždy zkontrolovány  
Skrytá instrukce je v promptu čitelná, na webu ne

## Role lídra a firemní kultura

- Lidé mají prostor a čas pracovat s AI zodpovědně  
Tlak na rychlost zvyšuje bezpečnostní riziko
- Bezpečnost je součástí onboardingů a pravidelného vzdělávání  
Nejde o jednorázové školení
- Je jasné, kdo ve firmě za bezpečnost nástrojů zodpovídá  
Bezpečnost není jen úkol IT oddělení

**Naučte své lidi pracovat  
bezpečně s AI**

[www.redbuttonedu.cz/workshopy-a-prednasky](http://www.redbuttonedu.cz/workshopy-a-prednasky)