



Středočeský kraj Role a aktivity v oblasti kyberbezpečnosti a digitální závislosti

Konference kyberbezpečnosti a digitální gramotnosti Snooper 2026
26. 2. 2026

Digitální svět: regulace, realita, dopady

- Digitální technologie zásadně mění život dětí, rodin, škol i obcí.
- Dopady řešíme dnes – bez ohledu na tempo regulace.

Co dnes v kraji skutečně vidíme:

- přetížené školy a pedagogové
- nárůst úzkostí a závislostního chování
- tlak na sociální služby
- digitální vyloučení i digitální přetížení

Role kraje: koordinace, propojení, podpora

Koordinace

- Prevence kriminality
- Politika v oblasti závislostí

Propojení

- Komise, Expertní skupiny (např. Expertní skupina prevence kriminality, Expertní skupina pro oblast závislostí)
- Regionální platformy, Metodická setkání zástupců obcí, metodiků prevence, spolupráce se službami

Podpora – finanční a metodická

- Fond prevence
- Příspěvek na plnění preventivního programu (školy zřizované krajem)

Fond prevence

STŘEDOČESKÝ FOND PREVENCE

Program

Pravidla SEL

Pravidla AED

Primární prevence

Selektivní a indikovaná
primární prevence

Pořízení AED

Prevence kriminality

Adiktologické služby

Středočeský kraj

Podpora všeobecné primární prevence

- Program 2026 pro poskytování dotací ze Středočeského Fondu prevence
- Celkem vyčleněno 29,3 milionu korun:
 - **Primární prevence – 14 milionů korun** na podporu programů všeobecné primární prevence, duševního zdraví dětí, zlepšení školního klimatu a vzdělávání pedagogů.^[L]_[SEP]
 - **Prevence kriminality – 6,3 milionu korun** na projekty zvyšující bezpečnost, prevenci kyberkriminality, domácího násilí či rozvoj kamerových systémů.
 - **Adiktologické služby – 9 milionů korun** na rozvoj a udržitelnost služeb pro osoby s adiktologickými problémy vč. digitálních závislostí

Rok 2026 - historicky
největší podpora
preventivních programů

Podpora selektivní a indikované primární prevence aneb rychlá pomoc školám

Od roku 2025 je vyhlášena **nová dotační výzva na podporu specifické selektivní a indikované primární prevence.**

Výzva je otevřená po většinu roku, aby školy mohly žádat hned, když řeší akutní problém (šikana a pod.)

Alokovaná částka **700 tis. Kč.**

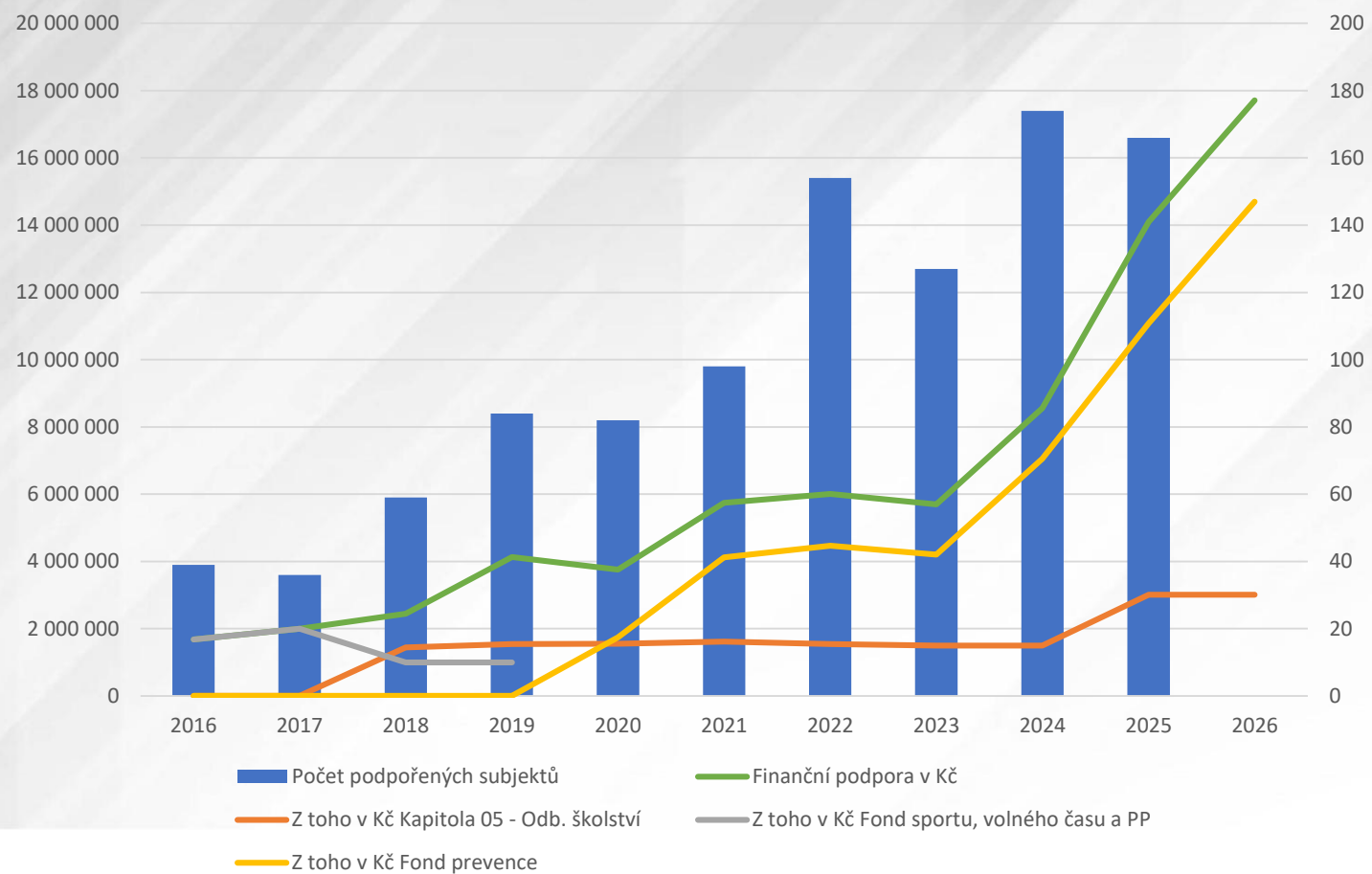
Žadatelem je pouze škola a dotaci lze použít pouze na realizaci intervenčních **programů specifické a indikované primární prevence.**



Středočeský kraj

Podpora primární prevence

Podpora primární prevence z prostředků SČK v letech 2016-2026 v Kč



Program prevence kriminality - projekty

- **Rozvoj kybernetické a informační bezpečnosti pro pracovníky v oblasti prevence kriminality a prevence závislostí obcí SČK (2025)** – série seminářů na téma „Aktuální trendy v rizikovém chování dětí na internetu“ a „Umělá inteligence – principy, využití a rizika“
- **Rozvoj kybernetické bezpečnosti a prevence kybernetické kriminality (2026)** – semináře na téma kyberbezpečnosti a prevence kyberkriminality
- **Osvěta v oblasti prevence závislostí a prevence patologických jevů**
 - **Kuchařka pro (nejen) školní metodiky prevence** – informační brožura pro pedagogy
 - **Kuchařka vol. 2 (nejen) pro rodiče** – informační brožura pro veřejnost

Kraje pro bezpečný internet

- **Projekt pod Asociací krajů ČR**
- Účelem projektu je zvýšit informovanost o rizicích internetu a možnostech prevence a pomoci.
- Soutěžní kvíz pro žáky ZŠ a SŠ, e-learningové kurzy, videospoty pro děti, dospělé a seniory.
- **Kyberguru** – podcastový seriál na téma bezpečnosti na internetu, rozhovory s vybranými odborníky



Nenech sebou manipulovat

Seriál videí na téma manipulace a šíření dezinformací vytvořen ve spolupráci s prof. MUDr. Jiřím Horáčkem, Ph.D., FCMA.

Témata dílů:

- Nebezpečí manipulace
- Jak funguje nenápadná manipulace
- Konkrétní typy technik manipulace s příklady
- Vysvětlení cílů manipulátorů
- Konkrétní rady, jak se manipulacím bránit
- Role dezinformací

Cílem je naučit diváky včas rozpoznat manipulativní jednání a zvýšit jejich odolnost vůči dezinformacím.

Středočeský kraj ve spolupráci s prof. MUDr. Jiřím Horáčkem a jeho kolegy z Národního ústavu duševního zdraví Klecany připravil projekt

NENECH SEBOU MANIPULOVAT

- Co je demagogie a jaké jsou základní techniky manipulace? Jak je odhalit?
- Jak poznat, že s vámi někdo manipuluje v dnešním složitém světě?
- Jak na internetu rozeznám pravdu od lži? Komu můžu věřit a komu ne?
- Jak konkrétně se bránit proti manipulaci, která se na mě valí ze všech stran?
- Dovolím manipulátorům, aby ovlivnili moje názory a chování?

Projekt je podpořen Středočeským krajem.

Středočeský kraj

Kybernetické útoky na krajské PO

- **V roce 2025 se staly obětí kyberpodvodu 2 PO SČK – škoda 15 mil Kč**
- Informační a vzdělávací kampaň – školení:
 - ✓ informační letáky na PO
 - ✓ vzdělávací akce v rámci Poradního sboru ŘÚ pro spolupráce s PO
 - ✓ vzdělávací akce v rámci porady ředitelů PO z oblasti školství, sociálních věcí, kultury
 - ✓ vzdělávací akce v rámci Pracovní skupiny Bezpečná nemocnice – oblastní nemocnice + ZZS
 - ✓ **v součinnosti s VISK vzdělávací akce pro PO** – zaměřené zejména pro statutární orgány, ekonomy, IT pracovníky, příkazce operací, rozpočtáře – **proškoleny cca 1 000 osob**
(zaměřeno na způsoby páchaní, včasné rozpoznání, efektivní obranu, odpovědnost a náhradu škody)



Kybernetické útoky na krajské PO

Středočeský kraj

KYBER PODVODY

V PŘÍSPĚVKOVÝCH ORGANIZACÍCH STŘEDOČESKÉHO KRAJE

Pozor na podvodníky! Ti se mohou vydávat za banku, policii nebo jinou důvěryhodnou instituci a snaží se vás vyděsit tím, že je váš bankovní účet ohrožen či napaden, a to za účelem získání citlivých přístupových údajů a následně i peněz.

Cílem těchto podvodů se staly v nedávné době **příspěvkové organizace Středočeského kraje** a byla způsobena velká škoda v řádech milionů korun. Nebezpečí je tedy bezprostřední a reálné.

Pracovníci na klíčových pozicích jsou přitom **odpovědní za své jednání a za způsobené škody**, proto je důležité dodržovat bezpečnostní opatření a být obezřetní.

VISHING
Je podvodný telefonát při kterém se sítňák vydává za důvěryhodnou instituci, aby vyžádal citlivé údaje nebo peníze.

SPOOFING
Je technika, při níž útočník falšuje identitu nebo adresu odesílatele, aby působil důvěryhodně a otkamal oběť.

Jak se chránit:

- Nesdělujte hesla, autorizační kódy ani osobní údaje.
- Nepovolujte vzdálený přístup k počítači.
- Neinstalujte žádné neověřené aplikace do svého počítače.
- Kontrolujte web banky – správná doména.
- Aktualizujte software, antivir a firewall.
- Ověřujte informace přímo u banky.

Co dělat při podezření:

- Zznamenejte údaje podvodníka (jméno, číslo účtu, e-mail).
- Kontaktujte banku a Policii ČR – linka 158.
- Kontaktujte svého zřizovatele.

Další informace a preventivní materiály jsou dostupné na těchto odkazech:

[POLICIE ČR - VISHING A SPOOFING](#) [OSVĚTOVÁ KAMPAŇ - VELKÉ ODHALENÍ](#) [VIDEO O SDÍLENÉM PŘÍSTUPU](#)

Pravidelně informujeme na našem webu "[BEZPEČNÝ STŘEDOČESKÝ KRAJ](#)"

Dávejte pozor - podvodníci neustále hledají nové způsoby, jak vás otkamat!

- **Organizační opatření – usnesení RK ze dne 13.11.2025:**
 - ✓ uložena povinnost pro PO SČK při provádění odchozích plateb:
 - ✓ – dvoufaktorová autentizace (2FA)
 - ✓ ověřování nejméně dvěma různými oprávněnými osobami
 - ✓ nastavení denních limitů dle individuálního posouzení dané PO
- **V roce 2025 a 2026 vzdělávací semináře pro pracovníky obcí SČK v rámci schváleného Programu pravence kriminality na rok 2026**



**Středočeský kraj
Role a aktivity v oblasti
kyberbezpečnosti a
digitální závislosti**

Konference kyberbezpečnosti a digitální gramotnosti Snooper 2026
26. 2. 2026