Ostrava 10. února 2025

**Den bezpečnějšího internetu**

Žijeme v době, kdy je užívání internetu dětmi a mladým lidmi praktický nevyhnutelné a k tomu je potřeba mít znalosti v oblastí informačních a komunikačních technologií. Internet je okénko do světa, které nabízí spoustu příležitostí, objevování, komunikace. Najdeme zde obsah, který není vhodný pro děti a s tím je potřeba počítat. Naivita, důvěřivost a nedostatek životních zkušeností, může být důvodem, že se dítě stane obětí například virtuálních predátorů nebo kyberšikany. Ideální způsob, jak minimalizovat nebezpečí online prostředí, je dodržovat pravidla a zároveň se vzdělávat o rizicích páchaných prostřednictvím internetu.

Sociální sítě jsou nejvíce využívané mladou generaci a zde je potřeba být obezřetný. Z pohledu dětí se sdílené informace mohou tvářit neškodně, ale takové rozposílání fotografií je rizikové, jelikož okamžitě ztrácí nad fotkou kontrolu. Zvláště rodiče by měli věnovat pozornost bezpečnosti svých dětí v online prostoru. Policie České republiky spolupracuje s mobilními operátory a správcem domény CZ.NIC na publikaci PRVNÍ MOBIL – příručka pro rodiče, která poskytuje užitečné informace a rady pro bezpečné používání mobilních telefonů dětmi. Častým jevem na sociálních sítích u dětí bývá kybešikana. Jedná se o úmyslné chování, kdy je oběť dlouhodobě a opakovaně napadána jedním nebo více útočníky a závažnost útoků se stupňuje, případně se zkracuje jejich frekvence. Kyber znamená v překladu prostředí, ve kterém se šikana odehrává (kybersvět mobilních telefonů, počítačů, tabletů…). Může se jednat například o zakládání falešných účtů s cílem oběť ponížit, zesměšnit jednoduše jí ublížit. Šikana v jakékoliv formě je pro společnost nepřijatelné chování a nemělo by být tolerováno.

Také je potřeba upozornit na **finanční podvody** páchané internetovými podvodníky. Tito primárně cílí na starší lidí, a to velmi sofistikovaným způsobem. Od poškozených lidí dokáží získat nemalé finanční částky. Nejčastějšími způsoby je využití strachu, že přijdou o své úspory, pokud okamžitě neučiní kroky k jejich zamezení.

* **NIKDY** nereagujte na podvodné hovory!
* **NIKDY** nikomu po telefonu, e-mailu apod. **nesdělujte** své **osobní údaje** a už vůbec ne konkrétní informace o svém bankovním účtu nebo platební kartě!
* **NIKDY** nikomu **nepřeposílejte** potvrzovací SMS zprávu s unikátním kódem nebo neprovádějte autorizaci transakcí ve svém internetovém bankovnictví, když transakci sami neprovádíte!
* **NIKDY** nikomu neumožňujte vzdálený přístup do Vašeho počítače!
* **SLEDUJTE**  a čtěte si varování a informace od Vaší banky v internetovém bankovnictví!
* **POZOR** na podvodné inzerce v oblastí kryptoměn!

Mnoho z Vás v běžném životě využívá **umělou inteligenci (AI)**. Existuje plno aplikací, které AI nabízí, ale důležité je věnovat zvláštní pozornost metodickému průvodci do světa AI. Tento se věnuje jejímu využití, ale také etickým a právním aspektům. Zkoumá, jaké dopady může mít AI na autorská práva, soukromí a bezpečnost, a upozorňuje na rizika spojená s jejím nekontrolovatelným využíváním popřípadě zneužíváním. Detailnější informace naleznete na stránkách **ai.e-bezpeci.cz.**

Krajské ředitelství policie Moravskoslezského kraje

oddělení prevence

por. Bc. Martina Jablońská