inSign – Bezpečnostní zásady pro používání vašeho mobilního zařízení

1) **Používejte programy pro ochranu svého mobilu. Jde hlavně o antivirový program.**

I když placené antiviry nabízí mnohem lepší ochranu, dají se najít i kvalitní bezplatné programy. Při jejich výběru se řiďte hodnocením a recenzemi uživatelů, kteří už program používají. Svůj antivirový program pravidelně aktualizujte.

2) **Pravidelně aktualizujte operační systém, prohlížeč a veškeré další programy. Používejte jen legálně pořízené programy a systémy.**

Používejte jen originální operační systém a neprovádějte v něm úpravy, které umožní plný administrátorský přístup typu root nebo jailbreak. Takto upravená zařízení nekupujte a rozhodně nepoužívejte.

3) **Zvolte si bezpečný PIN.**

Jako PIN si nastavte 4 číslice. Vyberte takové, které nejde jednoduše uhádnout. PIN nikomu neprozrazujte, nepište si ho na papírky nebo do mobilu a pravidelně PIN měňte. Pokud váš telefon neumožňuje přihlašování otiskem prstu, nastavte si pro odemčení telefonu jiný PIN, než je PIN pro vstup do dalších aplikací. Nezapomínejte, že zodpovědnost za ochranu vašich uživatelských účtů a vašich dat je jen na vás.

4) **Navštěvujte jen známé webové stránky a stahujte prověřené aplikace.**

Vždy, když se dostanete na nějakou stránku, ověřte si, že její doména odpovídá obsahu. Nestahujte a nespouštějte soubory s neznámým obsahem. Do chytrého telefonu stahujte pouze aplikace z oficiálních zdrojů (Google Play, App Store).

5) **Své citlivé údaje nikdy nikomu neprozrazujte ani nepředávejte přes e-mail. Neklikejte na odkazy v podezřelých e-mailech.**

Nedůvěryhodné a podezřelé e-maily ze své poštovní schránky vymažte. Banka, jiní dodavatelé služeb, policie ani nejbližší členové rodiny nemají právo požadovat vaše přihlašovací údaje. V žádném případě nereagujte na výzvy k zadání/ověření přihlašovacích údajů. Svá uživatelská jména a hesla k aplikacím chraňte a nikomu je neprozrazujte.

6) **Používejte jen důvěryhodné Wi-Fi sítě.**

Nepoužívejte nedůvěryhodné Wi-Fi sítě (např. bezplatné a otevřené Wi-Fi sítě v obchodních centrech, kavárnách apod.). Hrozí totiž, že by někdo cizí mohl získat vaše citlivá data (např. přihlašovací údaje) a zneužít je.

7) **Zkontrolujte si, pro co udělujete souhlas a co potvrzujete.**

Vždy kontrolujte, čí služby a aplikace používáte, a zda skutečně provádíte zamýšlený úkon na správné webové stránce nebo ve správné aplikaci. Kontrolujte také, co potvrzujete a k čemu se zavazujete, a zda kontext odpovídá tomu, co chcete skutečně provést.

8) **Buďte obezřetní při svých nákupech na internetu.**

Při nákupech na internetu buďte opatrní, prověřte si předem důvěryhodnost prodávajícího. Čtěte recenze a různá upozornění od ostatních uživatelů.

9) **Nastavte si možnost najít a smazat zařízení.**

Nastavte si ve svém zařízení možnost vyhledání zařízení. Pokud svůj telefon ztratíte nebo budete mít obavy, že se dostal do nepovolaných rukou, můžete ho najít a případně z něj i vzdáleně vymazat data. U Androidu tuto funkci nastavíte v sekci Najdi moje zařízení, u iOS zařízení ji najdete v sekci Nastavení pod položkou Najít iPhone.

10) **Můžete povolit ověření vašeho telefonu otiskem prstu nebo snímáním obličeje.**

Pokud váš telefon umožňuje odemknutí otiskem prstu nebo snímáním obličejem, můžete tuto možnost pro zabezpečení telefonu využít. Odemykání telefonu tímto způsobem nepovolujte žádné další osobě.