Pravidla bezpečného užívání mobilního telefonu

Elektronické podpisy vytvářené s využitím služby I.CA RemoteSign mají v ČR stejnou právní váhu, jako vlastnoruční podpisy fyzických osob na papírových dokumentech. Aby bylo zabráněno jejímu neoprávněnému užití jinou osobou, je funkčnost aplikace vázána na více-faktorovou autentizaci uživatele, což znamená, že:

a) uživatel musí mít konkrétní aktivované zařízení pod svojí kontrolou (aktivní obrazovka) a
b) musí znát heslo ke klíči, aby jím mohl potvrdit svoji identitu.

Nesdělujte proto PIN k telefonu ani heslo ke klíči žádné další osobě.

Pro zajištění maximální bezpečnosti služby I.CA RemoteSign (v případě ztráty či krádeže telefonu nebo proti zneužití služby), doporučujeme dodržovat i následující obecná bezpečnostní pravidla:

Zámek zařízení – nastavte si zámek zařízení (PIN kód, gesto, otisk prstu apod.). Chráníte vaše zařízení v případě ztráty nebo krádeže před neoprávněným vstupem do zařízení.

Instalace z neznámých zdrojů – aplikace i aktualizace instalujte vždy jen z oficiálních zdrojů výrobců operačních systémů U neoficiálních zdrojů riskujete instalaci virů či malware. To může způsobit prozrazení přihlašovacích údajů, důvěrných informací nebo i ovládnutí vašeho zařízení na dálku.

Root zařízení – root zařízení odemyká administrátorská práva, které však běžný uživatel nepotřebuje. To může způsobit ztrátu bezpečnosti vašeho zařízení. Neprovádějte jej.

Práva aplikací – při instalaci jakékoliv aplikace kontrolujte, jaká oprávnění vyžadují. Pokud si nejste jisti, že aplikace požadovaná práva k zařízení nepotřebuje, odmítněte je povolit.

Neotevírejte odkazy v SMS, i když tato SMS vypadá, že přišla z důvěryhodného zdroje - odkazy v SMS mohou být využívány jako reklamní prostředek (obdoba spamu v e-mailech), v horších případech pak jako forma phishingu (obdoba e-mailového phishingu), kdy se z klientů snaží po kliknutí na odkaz vylákat na podvodné stránce důvěrné informace, v horším případě pak například údaje o Platební kartě a tyto informace následně zneužít.

Buďte obezřetní při využívání veřejných Wi-Fi připojení - jsou nesmírně pohodlná a užitečná věc, ale při jejich používání se nevyplatí zapomínat, že se do nich může přihlásit kde kdo – třeba i hacker snažící se získat vaše data. Nevíte nic o jejich zabezpečení a těžko tak posoudíte riziko. Pokud opravdu musíte využívat veřejných Wi-Fi sítí, instalujte do svého zařízení software, který vám poskytne zabezpečení připojení k veřejné Wi-Fi síti.

Pokud používáte mobilní zařízení na veřejnosti, dávejte pozor, jestli se vám někdo nedívá přes rameno.