MINISTERSTVO OBRANY SLOVENSKEJ REPUBLIKY
VOJENSKÉ SPRAVODAJSTVO
CENTRUM PRE KYBERNETICKÚ OBRANU SLOVENSKEJ REPUBLIKY

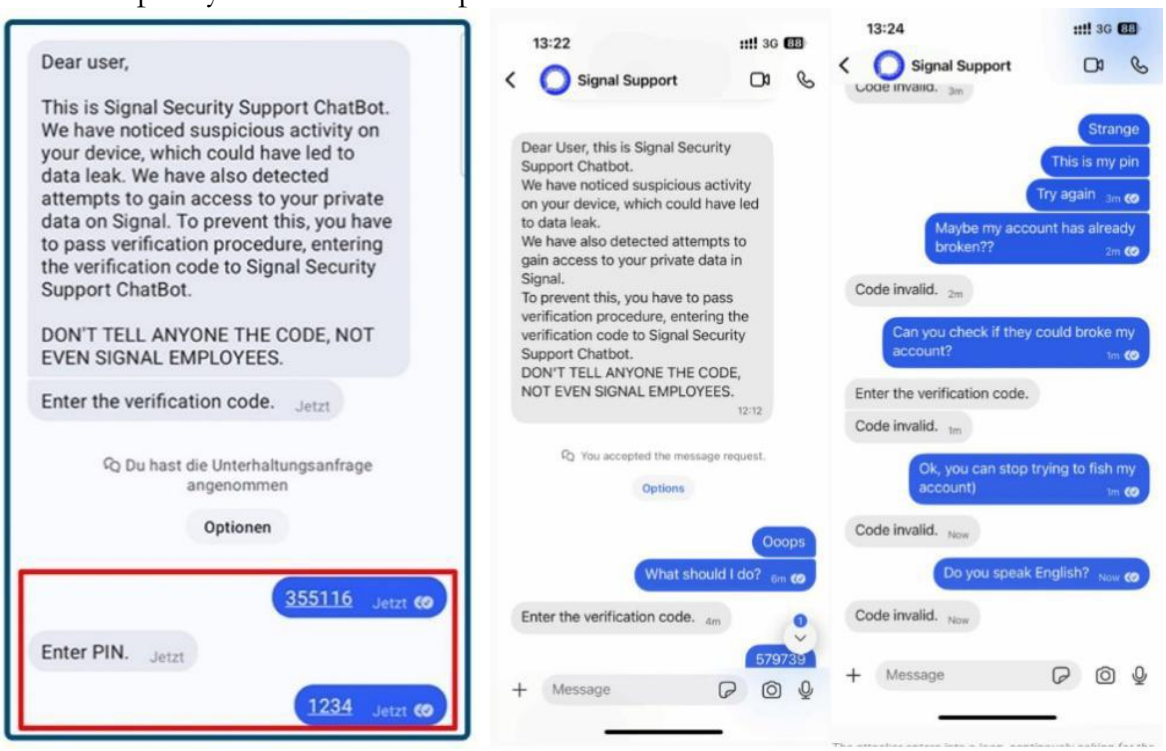
BEZPEČNOSTNÉ VAROVANIE

Odporúčané nastavenia používateľských účtov v komunikačných aplikáciách

Komunikačné aplikácie ako napr. Signal, WhatsApp, alebo Telegram poskytujú potenciálnemu útočníkovi možnosť získať prostredníctvom techník sociálneho inžinierstva prístup k zdieľaným informáciám nielen z individuálnych chatov, ale aj z chatovacích skupín. Nakoľko bezpečnostný dohľad nie je možné použiť na odhaľovanie, ani na zabránenie takýmto útokom, je dôležité udržiavať bezpečnostné povedomie používateľov týchto aplikácií.

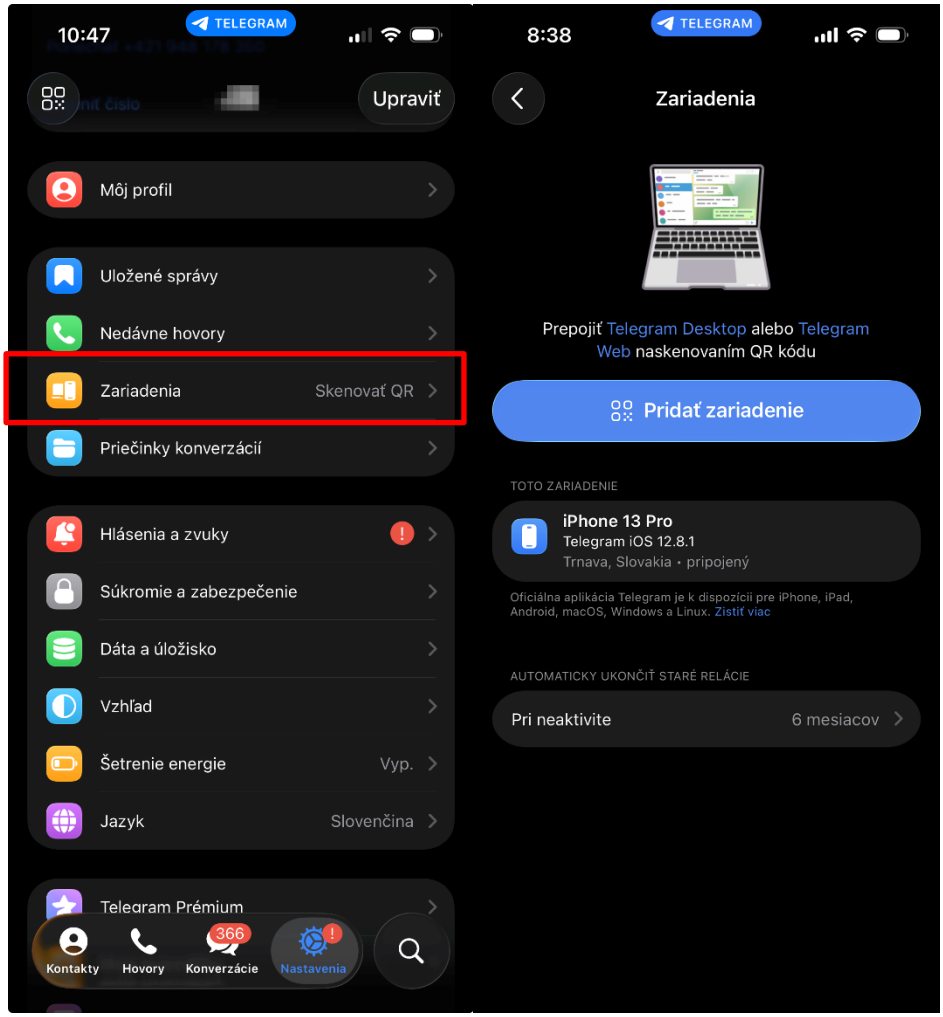
Čo sa môže stať

1. **Ste požiadaný o napísanie PIN kódu.** Tak ako pri platobných kartách, PIN kód je len váš a s nikým ho nezdieľajte. Nereagujte preto na výzvy na poskytnutie vášho bezpečnostného PIN kódu.

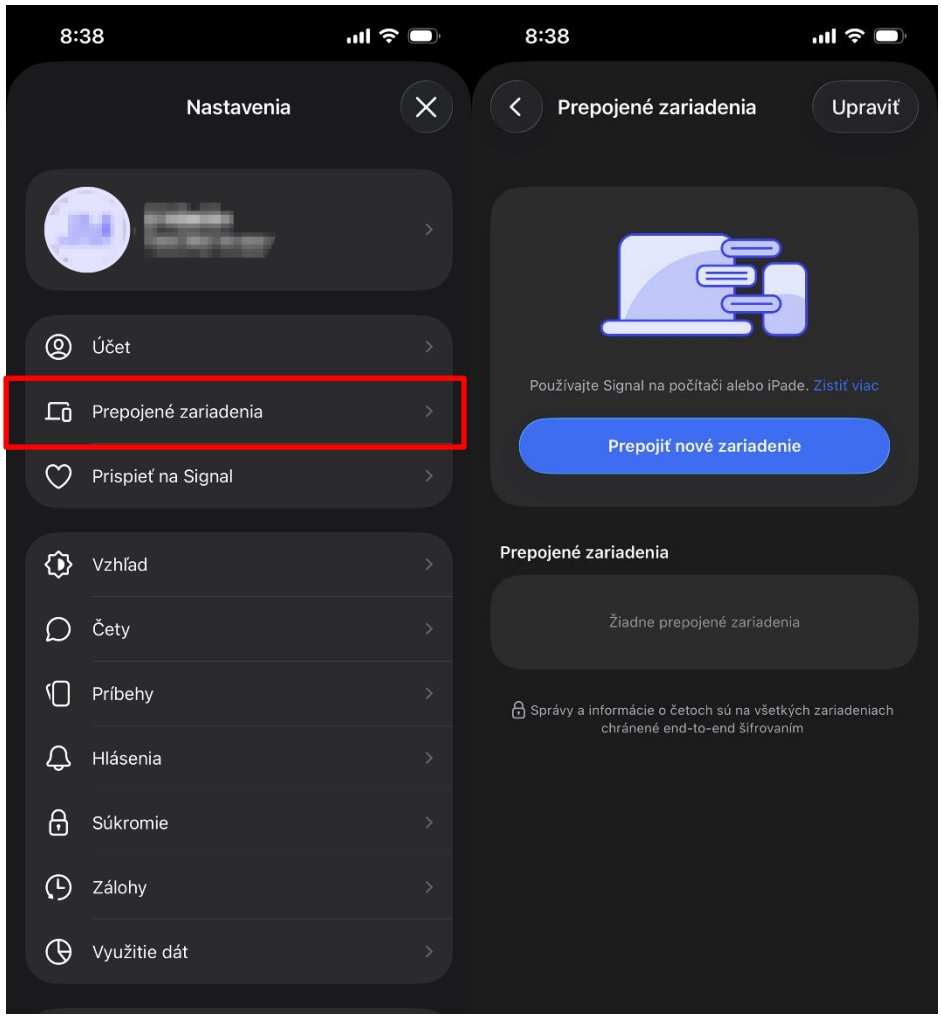


2. **Dostali ste informáciu, že ste odhlásený z aplikácie a musíte sa opätovne registrovať bez nejakého zrejmého dôvodu.** Na takúto výzvu nereagujte.

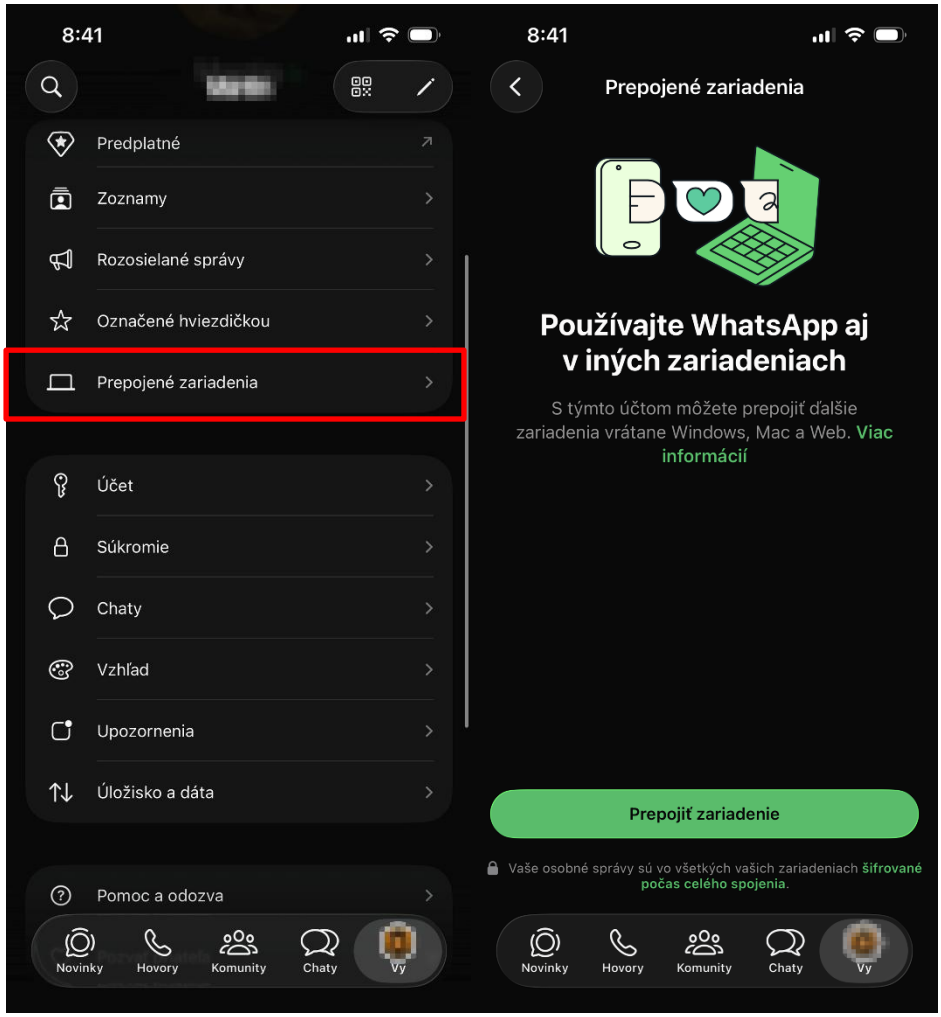
3. **Pri kontrole svojho účtu v komunikačnej aplikácii zistíte, že máte k svojmu účtu prepojené iné zariadenia.** Pokiaľ o nich nemáte vedomosť, zrušte im prístup. Prepojené zariadenia je možné skontrolovať v nastaveniach aplikácie. Obdobný prípad môže nastať aj u služieb napr. GMAIL alebo OUTLOOK, kde je možné k používateľským účtom pripájať iné aplikácie.



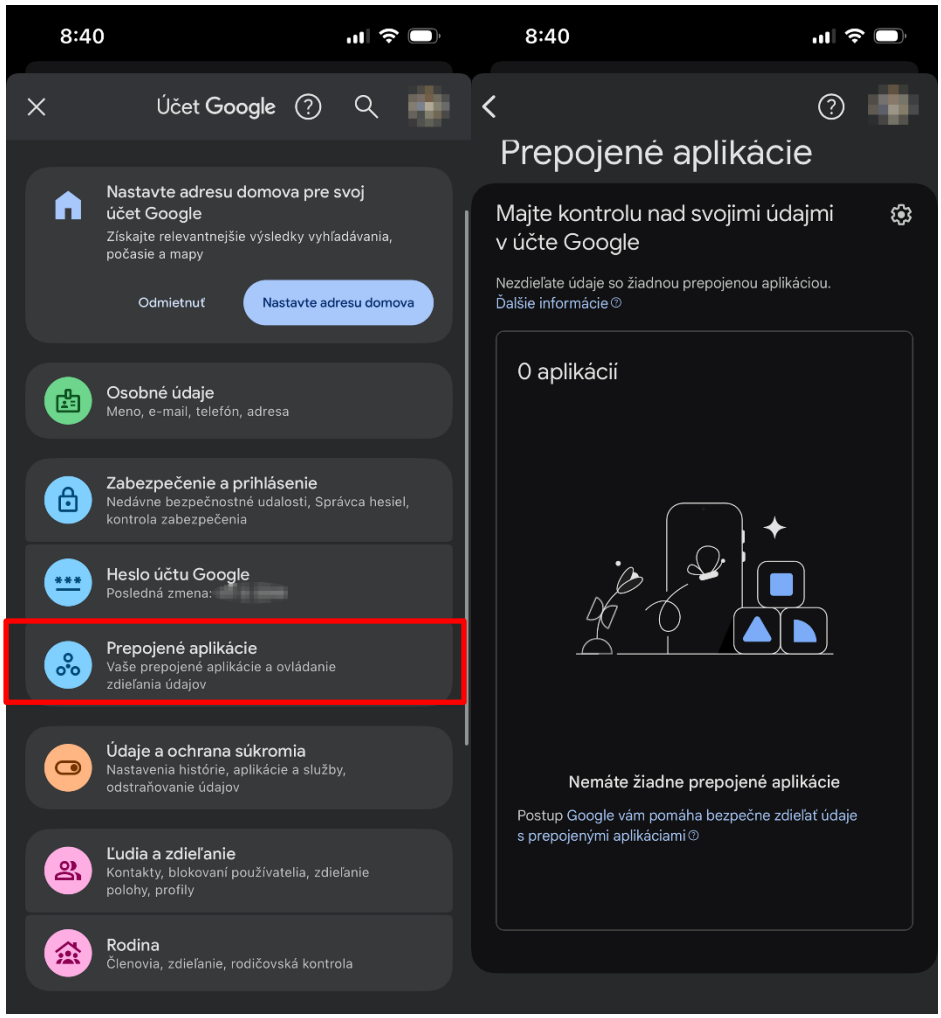
Prepojené zariadenia v komunikačnej aplikácii Telegram



Prepojené zariadenia v komunikačnej aplikácii Signal



Prepojené zariadenia v komunikačnej aplikácii WhatsApp



Pripojené aplikácie v komunikačnej aplikácii GMAIL

4. **Neočakávane ste dostali pozvánku na pripojenie sa do chatovacej skupiny pomocou odkazu alebo QR kódu s inštrukciou ako postupovať.** Túto metódu využívajú útočníci na pridanie svojho zariadenia k vášmu používateľskému účtu.

5. **Spozorujete v komunikačnej aplikácii, že správy, ktoré ste ešte nečítali, sú už označené ako prečítané.** V tomto prípade skontrolujte prepojené zariadenia, či sa tam nenachádza vám neznáme zariadenie.

6. **Spozorujete v komunikačnej aplikácii, že medzi odoslanými správami, sú správy, ktoré ste síce vy nepísali, ale boli odoslané pod vaším**

menom. V tomto prípade skontrolujte prepojené zariadenia, či sa tam nenachádza vám neznáme zariadenie.

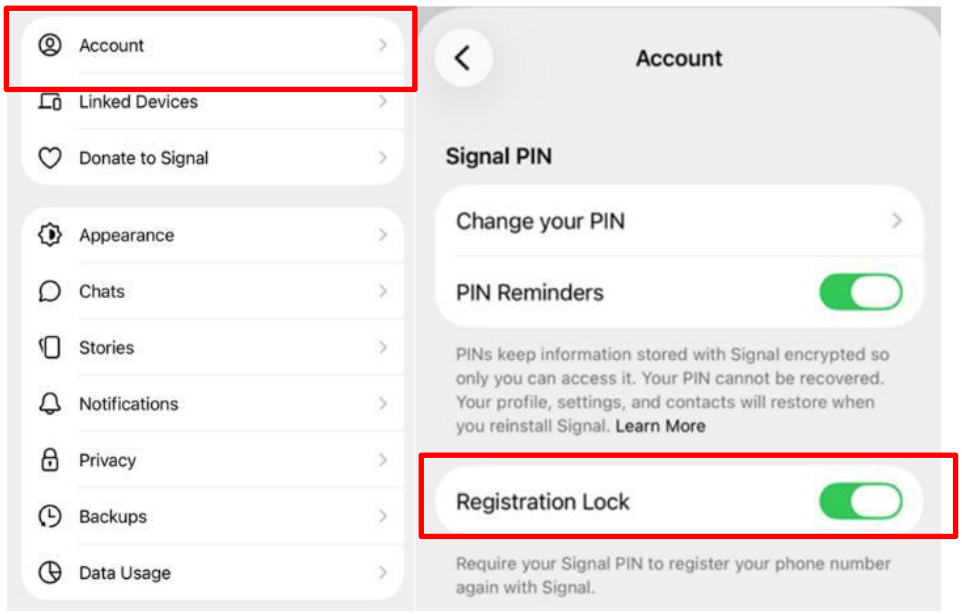
7. **Spozorujete v rámci chatovacej skupiny, že sa v nej objavilo vám neznáme tel. číslo, prípadne nový účet.** V takom prípade o tejto skutočnosti informujte priamo „administrátora“, ktorý danú skupinu založil.

Odporúčania pre používateľa

Ak využívate komunikačnú aplikáciu Signal alebo podobné komunikačné aplikácie snažte sa pri používaní daných aplikácií aplikovať nasledovné body:

1. **Zrušte používateľský účet a vymažte komunikačnú aplikáciu, ak ju dlhodobo nevyužívate.**

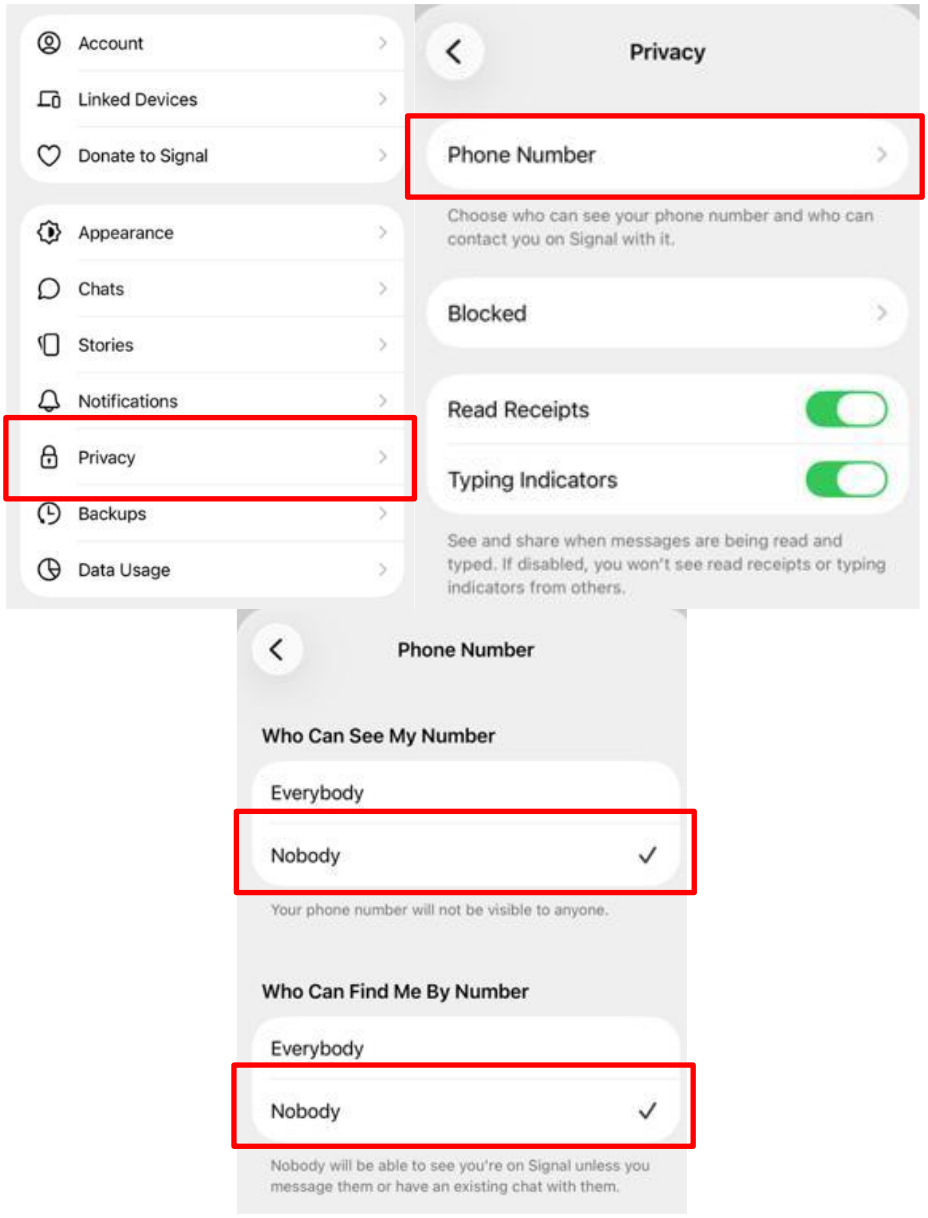
2. **Zapnite si tzv. „Registračný zámok“ (Registration lock)**
   - Pri opätovnej registrácii telefónneho čísla sa bude vyžadovať zadanie bezpečnostného PIN kódu používateľa. To zabráni útočníkovi s platným verifikačným kódom dokončiť prevzatie používateľského účtu, nakoľko nebude poznať používateľom zvolený bezpečnostný PIN kód.
   - Nastavenie: „Nastavenia“ > „Účet“ > „Registračný zámok“ > „Zapnúť“.



Vizualizácia inštrukcií zapnutia Registračného zámku

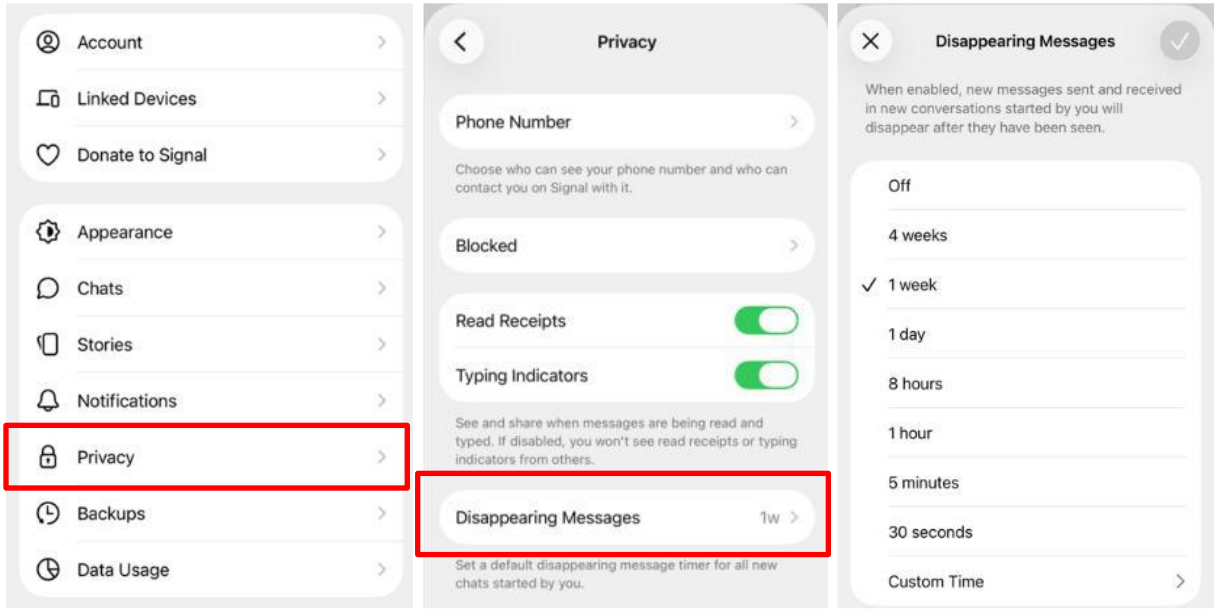
3. **Nastavte si, kto vás môže vyhľadať prostredníctvom vášho telefónneho čísla a kto môže vidieť vaše telefónne číslo**
   - Potenciálnemu útočníkovi tým sťažíte možnosť kontaktovať vás prostredníctvom vášho telefónneho čísla a zároveň, ak útočník získa prístup do chatovacej skupiny, ktorej ste súčasťou, nebude mu zobrazené vaše telefónne číslo.
   - Nastavenie: „Nastavenia“ > „Súkromie“ > „Telefónne číslo“ > „Kto ma môže vyhľadať prostredníctvom telefónneho čísla“ > vybrať „Nikto“

- Nastavenie: „Nastavenia“ > „Súkromie“ > „Telefónne číslo“ > „Kto môže vidieť moje telefónne číslo“ > vybrať „Nikto“
- Pre vyhľadanie vášho profilu (vás) bude nutné poznať vašu prezývku.



Inštrukcie na obmedzenie viditeľnosti vášho profilu v aplikácii Signal

4. Zvážte využívanie tzv. „Miznúcich správ“



Inštrukcie k zapnutiu „Miznúcich správ“

5. **Neodpovedajte na správy, ktoré prichádzajú od „údajnej“ technickej podpory.**
   - Technická podpora vás nikdy nebude kontaktovať priamo prostredníctvom komunikačnej aplikácie.

6. **Zablokujte a nahláste účty, ktoré sa vydávajú za tím podpory komunikačnej aplikácie.**

7. **Nikdy neposkytujte váš bezpečnostný PIN kód nikomu, kto oň požiada prostredníctvom SMS, správy v komunikačnej aplikácii, prípadne počas telefonického rozhovoru.**

8. **QR kódy skenujte pomocou komunikačnej aplikácie iba vtedy, ak sa sami rozhodnete prepojiť ďalšie zariadenie s danou komunikačnou aplikáciou.**

9. **Ignorujte pozvánky do chatovacích skupín, ak ste ich neočakávali alebo ak pochádzajú od neznámych kontaktov.**

10. **Pravidelne kontrolujte zoznam zariadení prepojených s vaším účtom.**
    - Okamžite vymažte neznáme zariadenia, ktoré sú prepojené s vaším účtom.

11. **Ak si nie ste istí totožnosťou používateľa, s ktorým komunikujete, overte si ju prostredníctvom iného komunikačného kanála, ak je to možné.**

Opatrenia pre administrátorov chatovacích skupín

V prípade identifikovania kompromitovaného používateľského účtu v chatovacej skupine postupujte nasledovne:

1. Prerušte komunikáciu s dotknutým používateľom v danej komunikačnej aplikácii.
2. Zamedzte prístup dotknutému používateľovi do chatovacích skupín vo vašej správe.
3. Kontaktujte dotknutého používateľa mimo danú komunikačnú aplikáciu a požiadajte ho o novú registráciu používateľského účtu s novým telefónnym číslom.
4. Vyžiadajte od dotknutého používateľa aplikovanie opatrení uvedených v časti „Odporúčania pre používateľa".
5. Pridajte nový používateľský účet do chatovacej skupiny.

V prípade podozrenia na možné kompromitovanie používateľských účtov v chatovacej skupine postupujte nasledovne:

1. Prerušte komunikáciu s podozrivými používateľmi v danej komunikačnej aplikácii.
2. Zastavte používanie podozrivých chatovacích skupín vo vašej správe, v ktorých sa nachádzajú podozrivé používateľské účty.
3. Požiadajte všetkých používateľov o vymazanie všetkých prepojených zariadení k ich používateľským účtom.
4. Vytvorte novú chatovaciu skupinu.
5. Do novej chatovacej skupiny pozývajte iba používateľov, u ktorých nebola potvrdená kompromitácia.
6. Zvyšných používateľov považuje za kompromitovaných a uplatnite postup pre identifikovanie kompromitovaného používateľského účtu v chatovacej skupine.

V prípade, ak je dostupnosť skupiny vysoká/kritické pre účely, pre ktoré existuje a nie je možné priamo uplatniť vyššie uvedený postup, tak aplikujte nasledovné kroky:

1. Nadviažte komunikáciu s členmi skupiny mimo kompromitovanú chatovaciu skupinu a informujte ich, že komunikácia v chatovacej skupine mohla byť monitorovaná (kompromitovaná) útočníkom.
2. Zvážte nevyhnutnosť pokračovania používania tejto chatovacej skupiny.
3. Pokračujte v monitorovaní chatovacích skupín vo vašej správe.
4. Ak je to možné, postupujte voči všetkým používateľom tak, ako by boli kompromitovaní a pokračujte podľa postupu uvedeného vyššie.
5. Vytvorte novú chatovaciu skupinu.
6. Vyžiadajte aplikovanie opatrení pre používateľa u všetkých používateľov.
7. Pridajte novovytvorené používateľské účty do novovytvorenej chatovacej skupiny.
8. Po presunutí všetkých používateľov do novej chatovacej skupiny zmažte pôvodnú (kompromitovanú) chatovaciu skupinu.

Cieľom tohto dokumentu je:

1. zvýšiť bezpečnostné povedomie medzi používateľmi komunikačných aplikácií,
2. zvýšiť odolnosť používateľov voči útokom sociálneho inžinierstva,
3. minimalizovať riziko zneužitia kompromitovaných účtov na šírenie phishingových správ, podvodov alebo škodlivého obsahu,
4. predchádzať neoprávnenému prevzatiu používateľských účtov,
5. zabezpečiť včasné odhalenie prípadnej kompromitácie a umožniť rýchlu reakciu na bezpečnostný incident,
6. ochrániť dôvernosť, integritu a bezpečnosť používateľských účtov a zdieľaných informácií.

Dokument odporúčame distribuovať:

1. profesionálnym vojakom a zamestnancom rezortu obrany,
2. organizáciám v pôsobnosti Ministerstva obrany Slovenskej republiky,
3. subjektom, ktoré zmluvne komunikujú s rezortom obrany (napr. dodávatelia).

Zdroj: CDT(2026)0104 - Cyber and Digital Transformation Division: NATO Enterprise Cybersecurity Advisory on Social Engineering Attempts Targeting Signal User Accounts (19.06.2026)