Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Č.j. 21670/2026-NÚKIB-E/630 • BRNO • 11. SRPNA 2026

[SITUAČNÍ REPORT]

RUSKÉ ZPRAVODAJSKÉ SLUŽBY CÍLÍ NA UŽIVATELE APLIKACE SIGNAL: CÍLEM JE SBĚR CITLIVÝCH INFORMACÍ SKRZE PHISHING

SHRNUTÍ

- **Uživatelé aplikace Signal jsou terčem cílených phishingových kampaní, které jsou spojovány zejména s aktéry napojenými na Ruskou federaci. Ti se primárně zaměřují na politiky, příslušníky bezpečnostních složek, úředníky a další osoby představující zájmové cíle z pohledu ruských národních zájmů.**
- **Útočníci neobcházejí end-to-end šifrování aplikace, ale zneužívají nepozornost uživatelů, stejně jako v případě „běžných" phishingových e-mailů. Nejčastěji se snaží přimět oběť k propojení útočníkova zařízení s jejím účtem Signal nebo k prozrazení PIN kódu či jiných přístupových údajů, což může vést ke kompromitaci komunikace. Součinnost oběti je v rámci tohoto typu útoků klíčová.**
- **Riziko lze významně snížit důsledným využíváním bezpečnostních funkcí aplikace a dodržováním několika zásad kybernetické hygieny, zejména ověřováním kontaktů, pravidelnou kontrolou propojených zařízení a obezřetností vůči níže popsaným variantám phishingu.**

UPOZORNĚNÍ: Informace a závěry obsažené v této analýze vycházejí z informací partnerů NÚKIB, z veřejně dostupných informací a z informací získaných v rámci činnosti NÚKIB v době publikace. Jedná se o analýzu kybernetické bezpečnosti z pohledu NÚKIB na základě jemu dostupných informací.

KONVERZACE V APLIKACI SIGNAL JSOU TERČEM KYBERNETICKÉ ŠPIONÁŽE NAVZDORY END-TO-END ŠIFROVÁNÍ

Aktéři hrozeb spojovaní s Ruskou federací v rostoucí míře cílí na uživatele komunikační platformy Signal s cílem získávat citlivé informace. **Zaměřují se zejména na politiky, zástupce bezpečnostních složek či obecně členy bezpečnostní komunity, kteří svou činností představují zájmové osoby v kontextu ruských národních zájmů.**[1]

Útočníci neobcházejí end-to-end šifrování aplikace, ale zneužívají nepozornost uživatelů, stejně jako v případě „běžných" phishingových e-mailů. Společným cílem těchto dosud odhalených variant útoku je **nepozorované přidání útočníkova zařízení mezi „připojená zařízení" oběti nebo získání přístupového kódu uživatele**, což umožňuje příjem nových zpráv a potenciálně také získání obsahu starších konverzací.

Jedná se o aktivitu, kterou ruské zpravodajské služby pravděpodobně (55–70 %) poprvé nasadily vůči členům ukrajinské armády, kteří aplikaci Signal používají jakožto jeden z alternativních komunikačních kanálů. [2] Obdobné taktiky byly následně nasazeny i proti dalším zájmovým cílům v členských státech NATO, kde je Signal bezpečnostní komunitou do určité míry vnímán jako standardní doplňková platforma pro neutajovanou, avšak velmi flexibilní a bezpečnou komunikaci.[3]

OBEZŘETNOST UŽIVATELE JE KLÍČOVÁ: KOMPROMITACE MŮŽE ZAČÍT OTEVŘENÍM ODKAZU ČI NASKENOVÁNÍM QR KÓDU

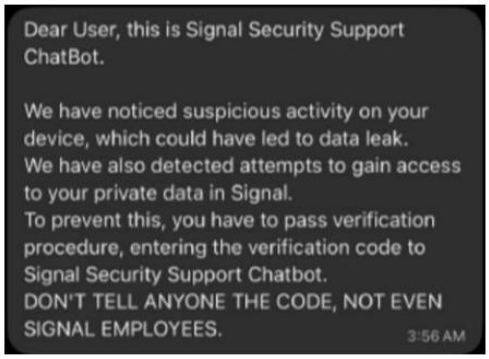
Primární variantou hrozby relevantní pro české uživatele je tzv. linked-device phishing. Útočníci na základě znalosti telefonního čísla oběti a předpokladu, že používá aplikaci Signal, mohou oběti zaslat škodlivou zprávu. Ta nejčastěji vypadá jako legitimní sdělení od platformy Signal, typicky zneužívající grafickou identitu IT či bezpečnostní podpory aplikace. Druhou pozorovanou variantou je zneužití škodlivého QR kódu, který se může tvářit jako pozvánka do skupiny. Obě varianty mohou taktéž navádět uživatele k zadání přístupového PIN kódu či jiných přístupových nebo obnovovacích údajů k aplikaci pod smyšlenou záminkou. Společným cílem obou variant je získat přístup do aplikace oběti, zejména skrze propojení zařízení pod kontrolou útočníka. Podle dostupných informací a obdobných analýz zveřejněných partnery NÚKIB útoky tímto způsobem cílily na uživatele na Ukrajině, v Německu, ve Francii a v Nizozemsku,

nicméně geografický rozsah této škodlivé kampaně je velmi pravděpodobně (75–85 %) širší.[4]

Hlavní dosud objevené varianty phishingu vůči uživatelům aplikace Signal jsou:

Falešné zprávy vydávající se za technickou či bezpečnostní podporu společnosti Signal, které vyzývají uživatele k předání PIN kódu či jiných přístupových údajů (Obrázek 1).

Obrázek 1: Falešná zpráva vyzývající uživatele k předání bezpečnostního PIN kódu



Zdroj: Google Threat Intelligence Group

Škodlivé odkazy či QR kódy mohou být oběti doručeny i mimo aplikaci Signal a navádět ji na podvržené externí domény. Tematicky se mohou týkat opět domnělé bezpečnosti zařízení, pozvánek do různých skupin nebo výzev k propojení cizího uživatele (Obrázek 2).[5]

Méně častý je tzv. „OAuth phishing“. Jde o zprávy, v nichž se útočník vydává za někoho, kdo má zájem o videokonferenční hovor s obětí, po níž požaduje přihlášení do „ověřovacího portálu“ nebo zaslání autentizačního kódu. Terčem jsou často aplikace a služby Microsoft.[6]

Obrázek 2: Falešný QR kód a škodlivý odkaz na připojení ke skupině

Zdroj: Google Threat Intelligence Group

DOPORUČENÍ: PRO BEZPEČNÉ POUŽÍVÁNÍ APLIKACE SIGNAL[7]

Ke stažení aplikace používejte pouze její oficiální webové stránky https://signal.org/.

Využívejte v maximální možné míře bezpečnostní funkce aplikace. (Více v příloze 1.)

Účet Signal je propojen s vaším telefonním číslem. Pokud k němu někdo získá přístup, může se za vás v této aplikaci vydávat. Aktivujte si proto v účtu funkci „Zámek registrace“. Dále omezte riziko neoprávněného přístupu k aplikaci aktivací funkce „Zámek displeje“. Nastavte si obsah notifikací tak, aby se na zamykací obrazovce zobrazovalo jen upozornění na novou zprávu. Pro citlivější komunikaci využívejte funkci „Mizející zprávy“ a omezte viditelnost a možnost dohledání podle telefonního čísla nastavením volby „Nikdo“.

Pro vyloučení předchozí kompromitace a její budoucí prevenci pravidelně kontrolujte připojená zařízení a důsledně ověřujte, s kým komunikujete:

V nastavení v sekci „Připojená zařízení“ zkontrolujte, zda rozpoznáváte všechna zařízení uvedená v seznamu. Zároveň doporučujeme, abyste další zařízení připojovali pouze tehdy, je-li to nutné a považujete-li je za zabezpečená a důvěryhodná. Kompromitace jednoho zařízení může útočníkům umožnit přístup k obsahu vašich konverzací, přičemž laptopy či pracovní stanice jsou obecně více vystaveny kybernetickým hrozbám.

Komunikujte pouze s kontakty ověřenými prostřednictvím bezpečnostního čísla a nepřijímejte žádosti o kontakt z čísel, která nejsou zaregistrována ve vašich kontaktech, bez sekundárního ověření. Kontrolujte taktéž duplicitní účty ve skupinových konverzacích. Obecně je vhodné nejprve kontaktovat druhého účastníka komunikace prostřednictvím jiného důvěryhodného komunikačního prostředku a ověřit si, zda jde skutečně o jeho profil.

Pro výrazně exponované osoby: Restartujte své mobilní zařízení alespoň jednou denně. Ačkoli tím nezabráníte jeho kompromitaci, restart může omezit působení malwaru či spywaru bez schopnosti perzistence.

Postupujte s obezřetností v kontextu skenování QR kódů, snah vylákat PIN kódy a dalších případných variant stejné hrozby popsané v této analýze.

V případě podezření na aktivitu popsanou v této analýze kontaktujte odpovědnou osobu ve své organizaci, zpravidla manažera kybernetické bezpečnosti.

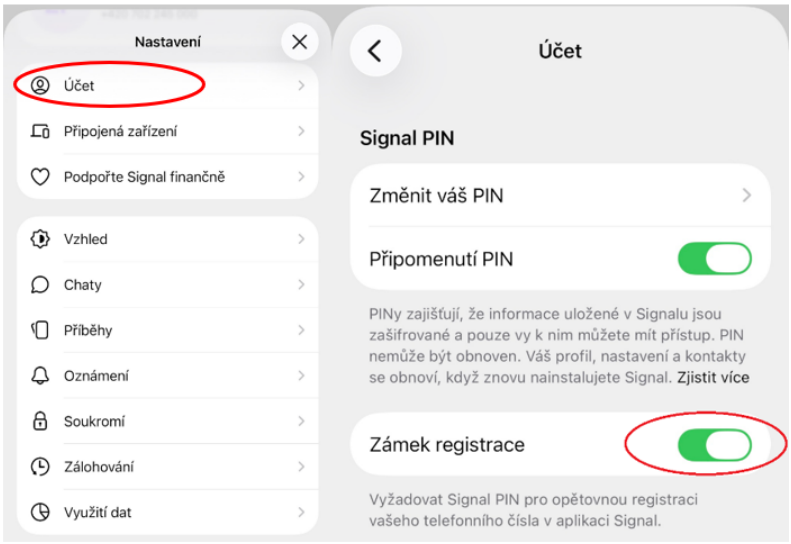
Jste-li odpovědnou osobou zastupující regulovaný subjekt, k hlášení využijte Portál NÚKIB. V případě, že vaše instituce pod regulované subjekty nespadá, využijte adresu cert@nukib.gov.cz.

PŘÍLOHA 1: NASTAVENÍ BEZPEČNOSTNÍCH OPATŘENÍ V APLIKACI SIGNAL

1. Zámek registrace / Registration Lock

Jedním z nejdůležitějších bezpečnostních opatření je aktivace funkce Zámek registrace (Registration Lock). Toto nastavení vyžaduje zadání bezpečnostního PINu při opětovné registraci telefonního čísla a významně snižuje možnost převzetí účtu v případě, že útočník získá ověřovací kód.

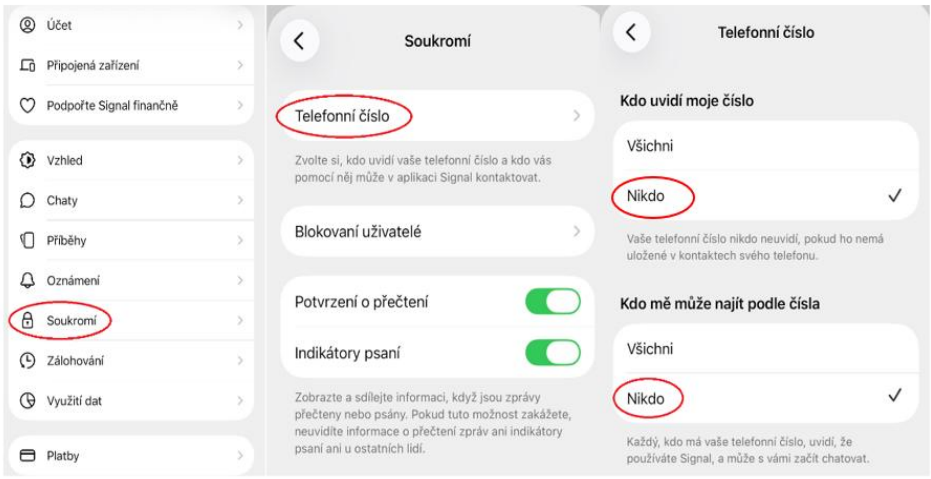
Otevřete si aplikaci Signal, v levém horním rohu klikněte na ***Nastavení → Účet → Zámek registrace*** *a tuto možnost povolte*.



2. Dohledání účtu podle čísla

Stejně důležité je správně nastavit ochranu soukromí a omezit možnost dohledání účtu podle telefonního čísla. Doporučuje se nastavit volby ***„Kdo mě může najít podle čísla“*** a ***„Kdo uvidí moje číslo“*** na možnost ***„Nikdo“***.

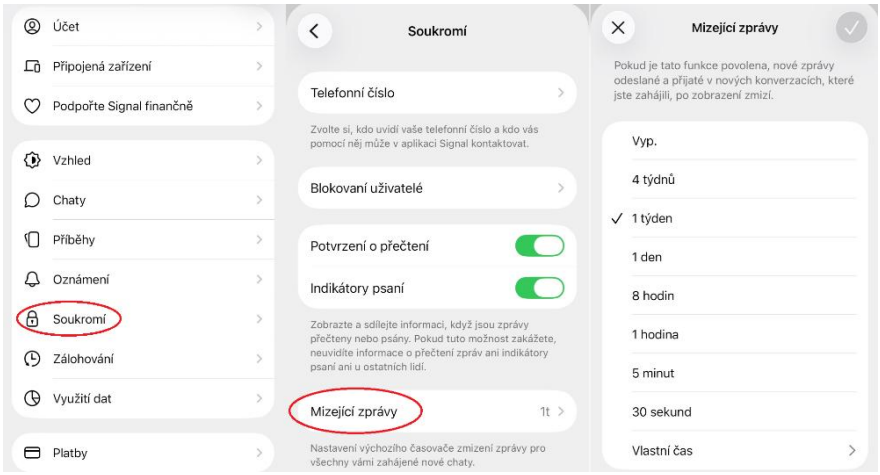
Nastavení → Soukromí → Telefonní číslo → Kdo mě může najít podle telefonního čísla → Nikdo *a* ***Kdo uvidí moje číslo → Nikdo***



3. Mizející zprávy

Významným bezpečnostním opatřením je také používání mizejících zpráv, které automaticky odstraňují obsah komunikace po uplynutí nastavené doby. Přestože toto opatření nezabrání kompromitaci účtu, omezuje množství informací, které mohou být v případě bezpečnostního incidentu zpřístupněny neoprávněným osobám.

Nastavení → Soukromí → Mizející zprávy → Týden (doporučená doba je jeden týden, ale z oprávněných důvodů může být tato funkce i vypnuta)



4. QR kódy

Zvýšenou pozornost je třeba věnovat QR kódům, odkazům a pozvánkám do skupin. QR kódy by měly být skenovány pouze v případě, kdy uživatel vědomě propojuje své vlastní zařízení s aplikací Signal. Neočekávané pozvánky do skupin, odkazy zaslané neznámými kontakty nebo požadavky na propojení zařízení mohou představovat pokus o získání neoprávněného přístupu k účtu.

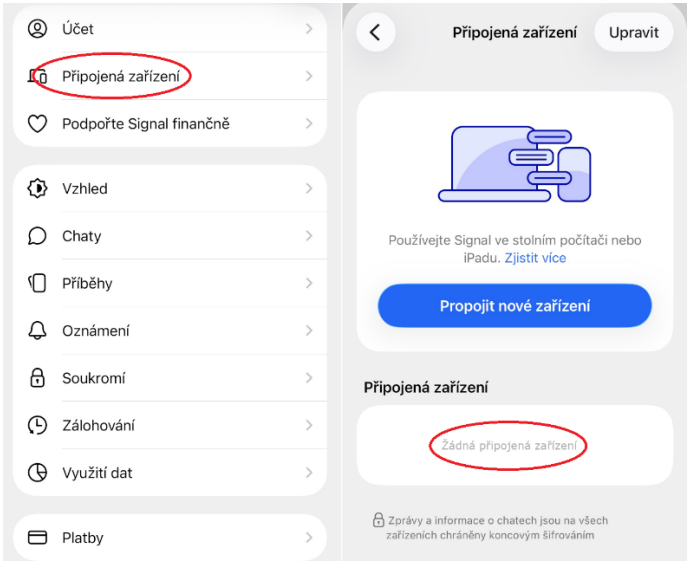
5. Nesdělovat PIN kód

Nikdy není přípustné sdělovat PIN kód platformy Signal, ověřovací kódy nebo jiné bezpečnostní údaje jakékoli osobě. Útočníci se často vydávají za technickou podporu nebo administrátory a snaží se od uživatelů získat potřebné údaje pod záminkou řešení technického problému. Je nutné si uvědomit, že oficiální podpora platformy Signal nekontaktuje uživatele prostřednictvím zpráv v aplikaci a nikdy nepožaduje zaslání PIN kódu nebo ověřovacích údajů. Jakýkoli účet, který se za podporu Signal vydává, by měl být okamžitě nahlášen a zablokován.

6. Kontrola propojených zařízení

Stejně důležitá je pravidelná kontrola propojených zařízení. V nastavení aplikace je možné zobrazit seznam všech zařízení připojených k účtu. Jakékoli neznámé nebo nepoužívané zařízení musí být neprodleně odebráno. Právě připojení cizího zařízení může být jedním z prvních příznaků, že byl účet kompromitován. Uživatelé by měli tuto kontrolu provádět pravidelně, a zejména pokud zaznamenají neobvyklé chování aplikace.

Nastavení → Připojená zařízení



ZDROJE

[1] Google Threat Intelligence Group. 2025. Signals of Trouble: Multiple Russia-Aligned Threat Actors Actively Targeting Signal Messenger. Dostupné z: https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger/

[2] Ibidem.

[3] POLITICO. 2025. Inside the Hazy, Fractured Mess of Signal Use in the Government. Dostupné z: https://www.politico.com/news/2025/04/02/inside-the-hazy-fractured-mess-of-signal-chats-in-the-government-00264466

The Record Media. 2026. Kremlin Hackers Attempting to Compromise Signal, WhatsApp Accounts Globally. Dostupné z: https://therecord.media/russian-hackers-target-signal-whatsapp-warn-dutch-intelligence-agencies

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI). 2026. Handlungsleitfaden bei Phishing über den Signal Support. Dostupné z: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Signal-Support/signal-support_node.html

National Cyber Security Centre (NCSC). 2025. NCSC Warns of Messaging App Targeting. Dostupné z: https://www.ncsc.gov.uk/news/ncsc-warns-of-messaging-app-targeting

Agence nationale de la sécurité des systèmes d'information (ANSSI) – Centre de Coordination des Crises Cyber (C4). 2026. Note d'alerte: Ciblage des messageries instantanées. Dostupné z: https://www.cert.ssi.gouv.fr/uploads/20260320_NP_C4_Alerte_Ciblage_messagerie_instantanee.pdf

[5] Google Threat Intelligence Group. 2025. Signals of Trouble: Multiple Russia-Aligned Threat Actors Actively Targeting Signal Messenger. Dostupné z: https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger/

[6] Volexity. 2025. Dangerous Invitations: Russian Threat Actor Spoofs European Security Events in Targeted Phishing Attacks. Dostupné z: https://www.volexity.com/blog/2025/12/04/dangerous-invitations-russian-threat-actor-spoofs-european-security-events-in-targeted-phishing-attacks/

[7] Aktualizovaná verze původního Doporučení NÚKIB:

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). 2022. Doporučení pro používání aplikace Signal. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1816-doporuceni-pro-pouzivani-aplikace-signal/

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol. Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
Červená **TLP:RED**	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
Oranžová **TLP:AMBER+STRICT**	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Oranžová **TLP:AMBER**	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
Zelená **TLP:GREEN**	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
Bílá **TLP:CLEAR**	Informace může být dále poskytována a šířena bez omezení. Případná omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

PRAVDĚPODOBNOSTNÍ VÝRAZY NÚKIB

Výraz	Pravděpodobnost
Téměř jistě	*90–100 %*
Velmi pravděpodobně	*75–85 %*
Pravděpodobně	*55–70 %*
Nelze vyloučit/Reálná možnost	*40–50 %*
Nepravděpodobně	*20–35 %*
Velmi nepravděpodobně	*0–15 %*