

Ref. No. 24019/2026-NÚKIB-E/630 • BRNO • 30 SEPTEMBER 2026
[SITUATION REPORT]

RUSSIAN INTELLIGENCE AGENCIES ARE TARGETING SIGNAL USERS: THE GOAL IS TO COLLECT SENSITIVE INFORMATION THROUGH PHISHING

SUMMARY

- Signal users are being targeted with tailored phishing campaigns linked mainly to Russian state-sponsored threat actors. These actors focus primarily on politicians, members of the security forces, officials and other personnel of interest from the perspective of the Russian state.
- The attackers do not bypass the app's end-to-end encryption, but instead exploit users' inattention, just as they do with "ordinary" phishing emails. Most often, they try to trick the victim into linking the attacker's device to their Signal account or into revealing their PIN or other login credentials, which can lead to the compromise of their communications. In these types of attacks, user interaction is crucial.
- The risk can be significantly reduced by using the app's security features and following general cybersecurity best practices, particularly by verifying contacts, regularly auditing connected devices, and exercising caution regarding the phishing schemes described below.

NOTE: The information and conclusions contained in this analysis are based on information from NÚKIB partners, information in the public domain, and information obtained through NÚKIB activities at the time of publication. This is an analysis of cybersecurity from the perspective of NÚKIB based on the available information.

SIGNAL CONVERSATIONS ARE A TARGET OF CYBER ESPIONAGE DESPITE END-TO-END ENCRYPTION

Threat actors linked to the Russian Federation are increasingly targeting users of the Signal messaging platform in order to obtain sensitive information. **They focus primarily on politicians, law enforcement officials, and members of the security community in general, whose activities make them valuable in the context of Russian national interests.**¹

Attackers do not bypass the app's end-to-end encryption, but instead exploit users' inattention, just as they do with "ordinary" phishing emails. The common goal of the attack variants discovered so far is to secretly add the attacker's device to the victim's "connected devices" or to obtain the user's access code, which allows the attacker to receive new messages and potentially also access the content of older conversations.

This is an operation that Russian intelligence services likely (55–70%) carried out for the first time against members of the Ukrainian military who use the Signal app as one of their alternative communication

channels.² Similar tactics were subsequently deployed against other targets of interest in NATO member states, where Signal is viewed by the security community, to a certain extent, as a standard supplementary platform for unclassified, yet highly flexible and secure communication.³

USER CAUTION IS KEY: A COMPROMISE CAN BEGIN SIMPLY BY OPENING A LINK OR SCANNING A QR CODE

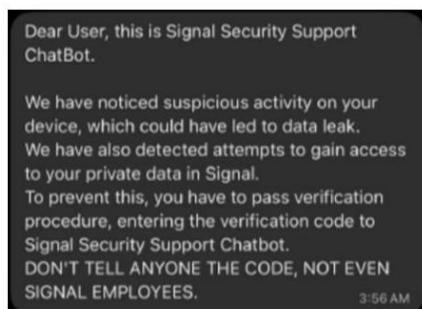
The primary threat relevant to Czech users is so-called "linked-device phishing." Based on knowledge of the victim's phone number and the assumption that the victim uses the Signal app, attackers send the victim a malicious message. This message most often appears to be a legitimate notification from the Signal platform, typically mimicking the visual identity of the app's IT or security support team. The second observed variant involves the use of a malicious QR code, which may appear to be an invitation to join a group. Both variants may also trick users into entering their app PIN or other login or recovery credentials under a false pretext. The common goal of both variants is to gain access to the victim's app, particularly by linking the device to a device controlled by the attacker. According to

available information and similar analyses published by NÚKIB partners, attacks of this type have targeted users in Ukraine, Germany, France, and the Netherlands; however, the geographic scope of this malicious campaign is highly likely (75–85%) broader.⁴

The main phishing variants targeting Signal users that have been discovered so far are:

Fake messages posing as technical or security support from Signal asking users to provide their PIN or other access credentials (Figure 1).

Figure 1: A fake message asking users to provide their security PIN



Source: Google Threat Intelligence Group

Malicious links or QR codes may also be delivered to the victim outside the Signal app and direct them to spoofed external domains. The content may again relate to the supposed security of the device, invitations to various groups, or requests to connect with an unknown user (Figure 2).⁵

Figure 2: Fake QR code and malicious link to join a group



Source: Google Threat Intelligence Group

Less common is what is known as “OAuth phishing.” These are messages in which an attacker poses as someone interested in a video conference call. The target is then directed to log in through an attacker controlled authentication portal or to send an

authentication code. Microsoft applications and services are often the targets.⁶

RECOMMENDATIONS: SAFE USE OF THE SIGNAL APP⁷

To download the app, use only its official website <https://signal.org/>.

Make the most of the app's security features. (See Appendix 1 for more)

Your Signal account is linked to your phone number. If someone gains access to it, they could impersonate you in the app. Therefore, enable the “Registration Lock” feature in your account. Additionally, reduce the risk of unauthorized access to the app by enabling the “Screen Lock” feature. Configure your notification settings so that only notifications of new messages appear on the lock screen. For more sensitive communications, use the “Disappearing Messages” feature and limit visibility and traceability by phone number by setting the option to “Nobody”.

To rule out any previous compromise and to prevent future compromises, regularly check linked devices and thoroughly verify who you are communicating with:

In the settings, under “Linked Devices”, check whether you recognize every device on the list. We also recommend linking additional devices only when necessary and only if you consider them secure and trustworthy. If one device is compromised, attackers may gain access to the content of your conversations; laptops and workstations are generally more exposed to cyber threats.

Communicate only with contacts verified via a security number, and do not accept contact requests from numbers that are not saved in your contacts without secondary verification. Also, check for duplicate accounts in group chats. In general, it’s a good idea to first contact the other person through another trusted communication channel to verify that it’s actually their profile.

For highly exposed users: Restart your mobile device at least once a day. Although this won't prevent your device from being compromised, restarting it can limit the impact of malware or spyware that lacks persistence.

Exercise caution when scanning QR codes, as well as in the context of attempts to elicit PIN codes and other possible variants of the same threat described in this analysis.

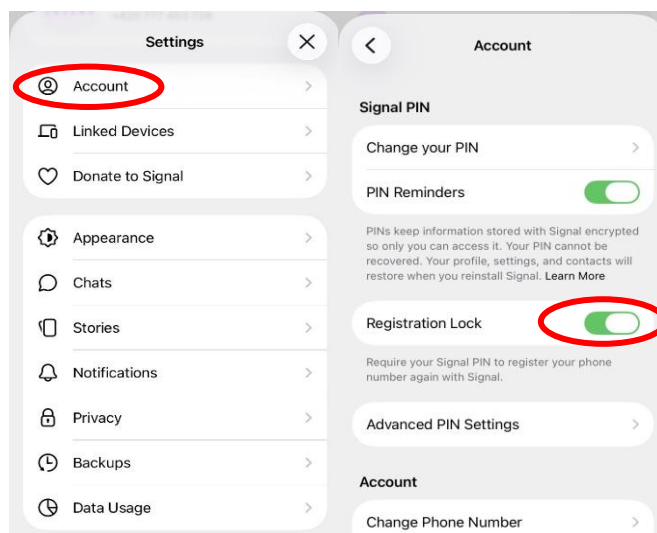
If you suspect any activity described in this analysis, contact the appropriate person in your organization—typically the cybersecurity manager.

ANNEX 1: SECURITY SETTINGS IN THE SIGNAL APPLICATION

1. Registration Lock

One of the most important security measures is enabling the Registration Lock feature. This setting requires a security PIN to be entered when the phone number is registered again and significantly reduces the possibility of an account takeover if an attacker obtains a verification code.

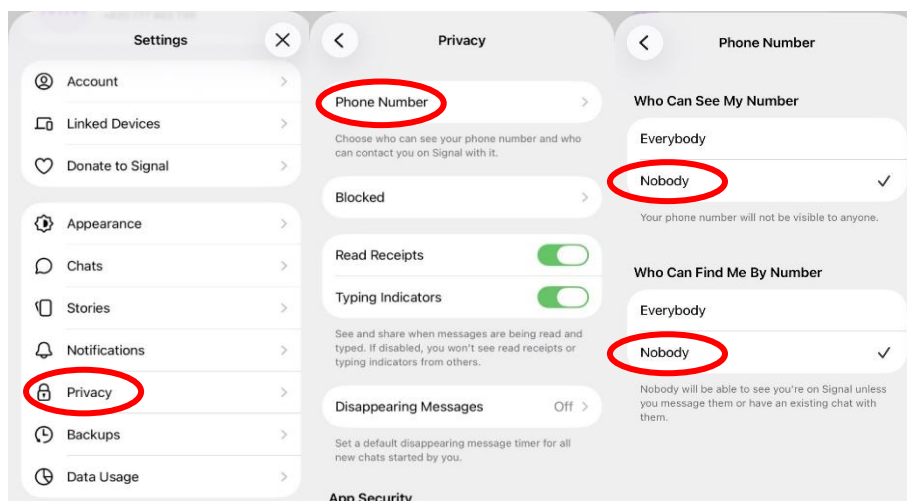
Open the Signal app, click on **Settings** → **Account** → **Registration Lock** and enable this option.



2. Find an account by phone number

It is equally important to set your privacy settings correctly and to limit the possibility of finding an account by phone number. It is recommended to set the options **“Who Can Find Me By Number”** and **“Who Can See My Number”** to **“Nobody”**.

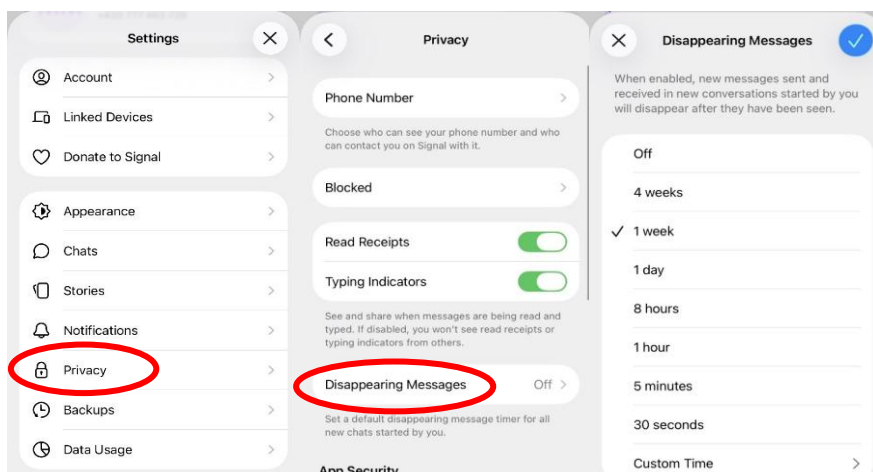
Settings → **Privacy** → **Phone Number** → **Who Can Find Me By Number** → **Nobody** and **Who Can See My Number** → **Nobody**



3. Disappearing messages

Another important security measure is the use of disappearing messages, which automatically delete the content of a conversation after a set period of time. Although this measure does not prevent an account from being compromised, it limits the amount of information that could be accessed by unauthorized individuals in the event of a security incident.

Settings → Privacy → Disappearing Messages → 1 week (the recommended period is one week, but for legitimate reasons this feature may also be turned off).



4. QR codes

Extra caution should be exercised with QR codes, links, and invitations to groups. QR codes should only be scanned when the user is consciously connecting their own device to the Signal app. Unexpected group invitations, links sent by unknown contacts, or requests to link devices may be attempts to gain unauthorized access to your account.

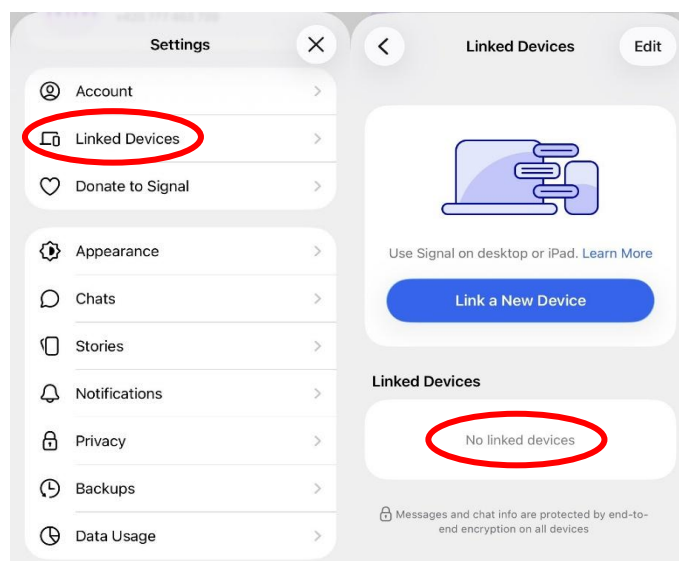
5. Never disclose your PIN

It is never acceptable to share your Signal PIN, verification codes, or other security information with anyone. Attackers often pose as technical support or administrators and try to obtain this information from users under the pretext of resolving a technical issue. It is important to remember that Signal's official support team does not contact users via in-app messages and never asks for your PIN or verification information. Any account claiming to be Signal support should be reported and blocked immediately.

6. Checking linked devices

It is equally important to regularly check connected devices. The application settings make it possible to display a list of all devices connected to the account. Any unknown or unused devices must be removed immediately. The connection of an unauthorized device can be one of the first signs that your account has been compromised. Users should perform this check regularly, especially if they notice unusual behavior in the app.

Settings → Linked Devices



SOURCES

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

² Ibid.

³ POLITICO. 2025. Inside the Hazy, Fractured Mess of Signal Use in the Government. Available at: <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. Available at: <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. Available at: 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. Available at: <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. Available at: 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. Available at: <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. Available at: <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. Available at: <https://nukib.gov.cz/cs/infoservis/doporuceni/1816-doporuceni-pro-pouzivani-aplikace-signal/>

TERMS OF USE OF INFORMATION

The use of the information provided is in accordance with the Traffic Light Protocol methodology. The information is marked with a flag that specifies the terms for the use of the information. The following flags are set out, indicating the nature of the information and the terms of their use:

Colour	Terms of use
Red TLP:RED	The information may not be provided to anyone other than the person to whom the information was addressed unless other persons to whom such information may be provided are specifically identified. If the recipient considers it important to disclose the information to other entities, this can only be done with the consent of the originator of the information.
Orange TLP:AMBER+STRICT	The information may only be shared within the recipient's organisation, and only to individuals who meet the need-to-know criteria and whose awareness is essential for resolving the issue or threat described in the information.
Orange TLP:AMBER	The information may be shared within the recipient organisation and its partners, and only to individuals who meet the need-to-know criteria and whose awareness is essential for resolving the issue or threat described in the information.
Green TLP:GREEN	The information may be shared within the beneficiary's organisation and, where appropriate, with other partners of the beneficiary, but not through publicly available channels; the beneficiary must ensure the confidentiality of the communication when forwarding it.
White TLP:CLEAR	The information may be further provided and disseminated without restriction. Any restrictions based on the intellectual property rights of the originator and/or the beneficiary or third parties are not affected by this provision.

NÚKIB EXPRESSIONS OF PROBABILITY

Expression	Probability
<i>Almost certainly</i>	90–100 %
<i>Highly likely</i>	75–85 %
<i>Likely</i>	55–70 %
<i>Cannot be ruled out/Realistic possibility</i>	40–50 %
<i>Unlikely</i>	20–35 %
<i>Highly unlikely</i>	0–15 %