MINISTRY OF DEFENCE OF THE SLOVAK REPUBLIC
MILITARY INTELLIGENCE
CYBER DEFENCE CENTRE OF THE SLOVAK REPUBLIC

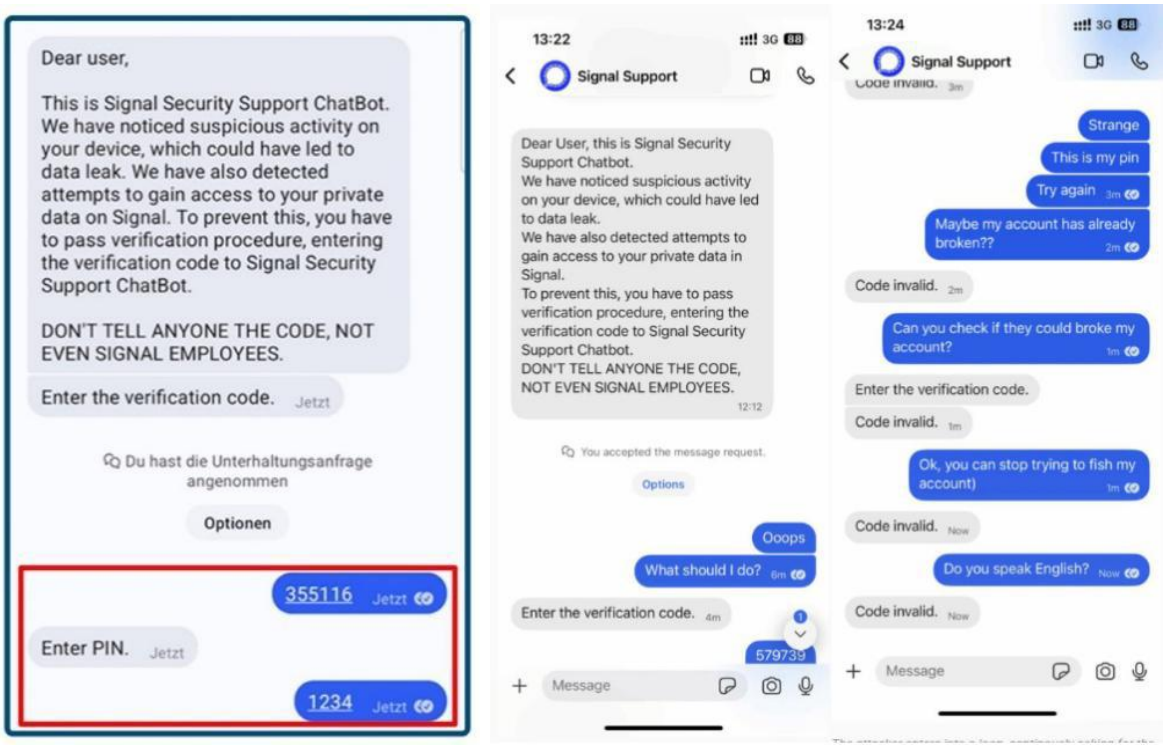
SECURITY WARNING

Recommended Settings for User Accounts in Messaging Applications

Messaging applications such as Signal, WhatsApp and Telegram may allow attackers to gain access to shared information through social engineering techniques, not only from individual chats, but also from group conversations. Since security monitoring cannot be used to detect or prevent such attacks, it is important for users of these applications to maintain good security awareness.

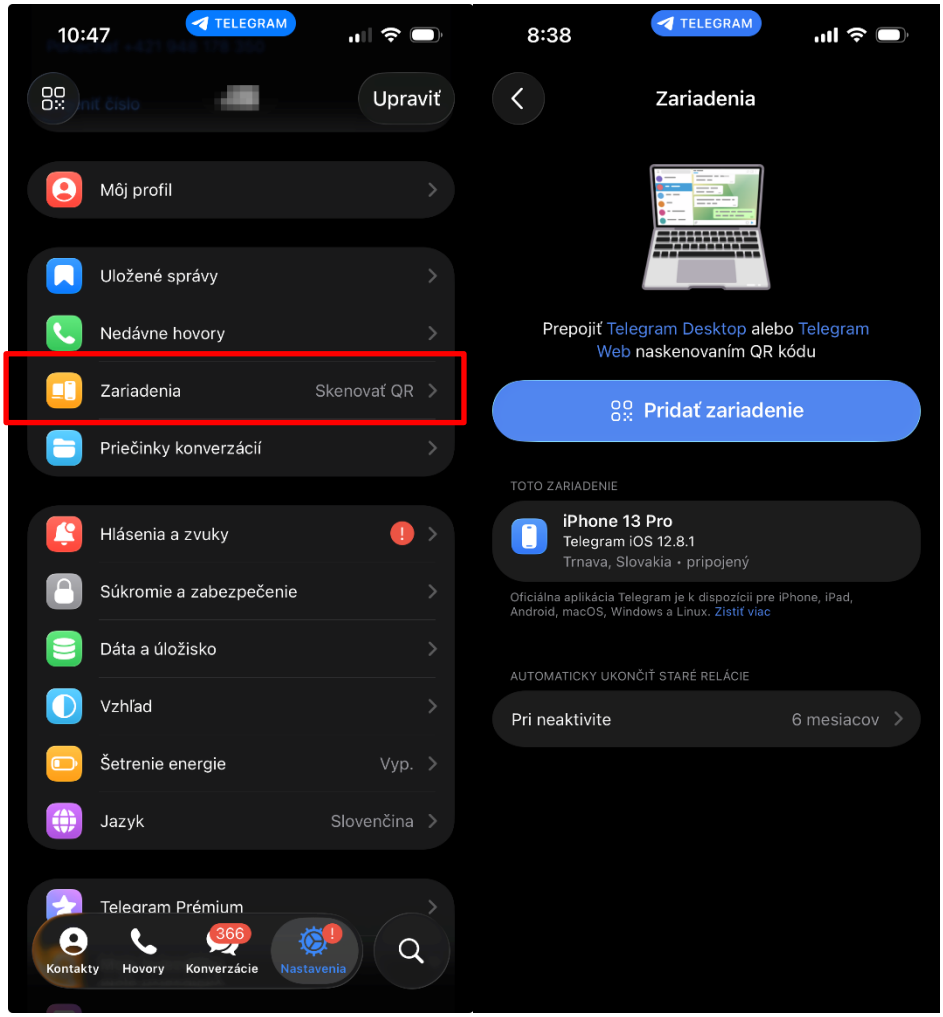
What Can Happen

1. **You are asked to enter your PIN code.** Just like with card payments, your PIN code is intended for your use only and must never be shared with anyone. Therefore, do not respond to requests asking you to provide your security PIN code.

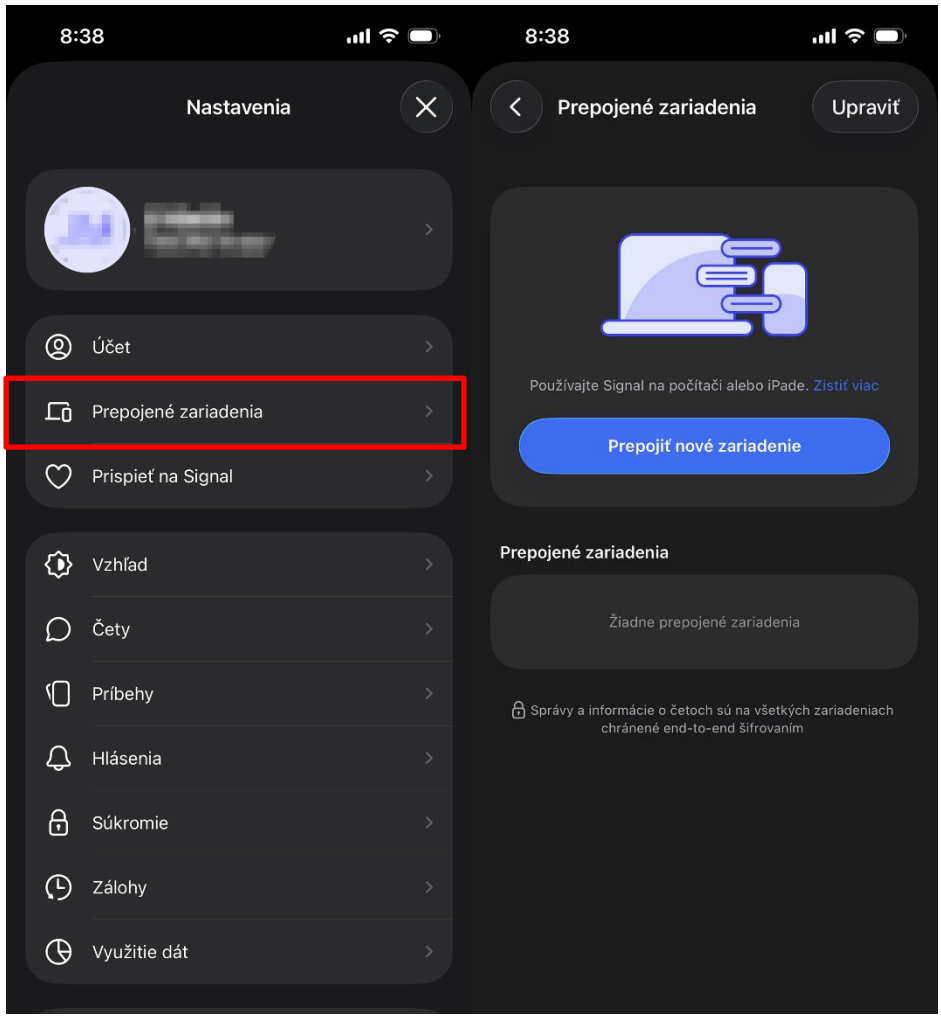


2. **You received a notification that you have been logged out of the application and need to register again without any apparent reason.** Do not respond to such a request.

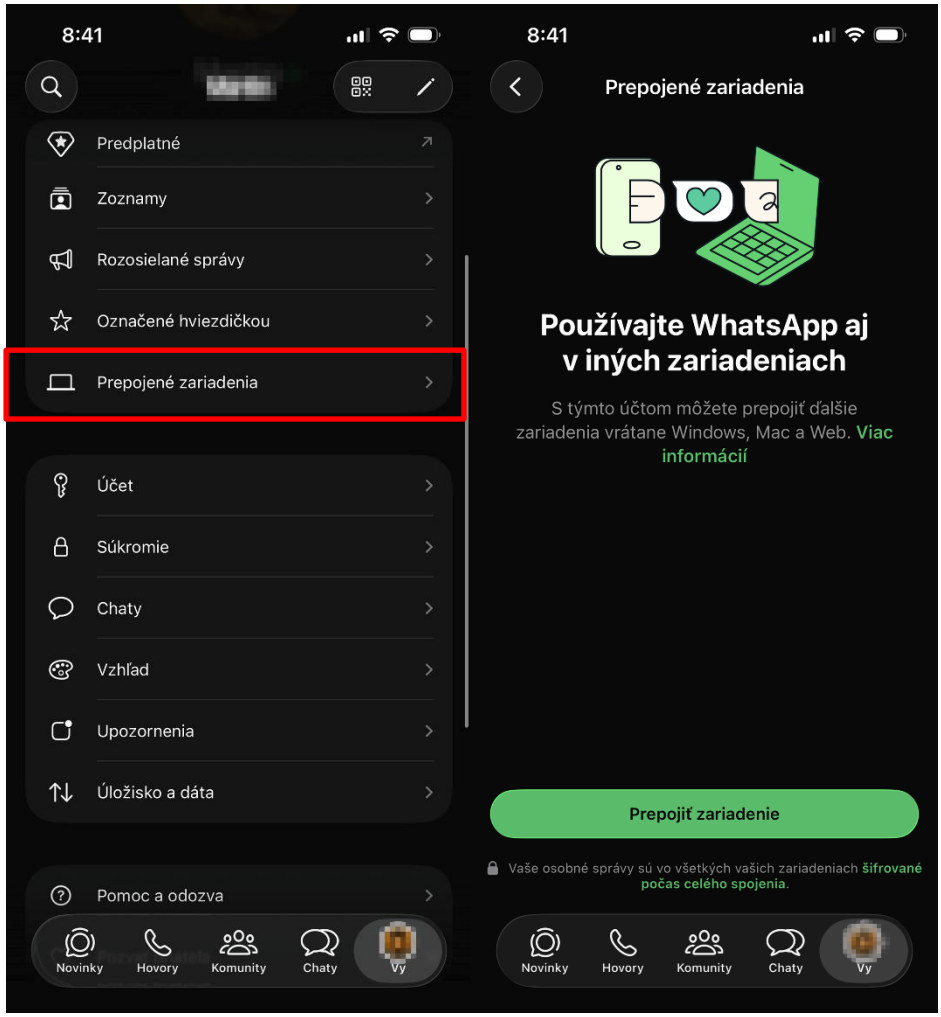
3. **While checking your account in a messaging application, you discover that other devices are linked to your account.** If you are not aware of these devices, immediately revoke their access. Linked devices can be checked in the application´s settings. A similar situation may also occur with services such as GMAIL or OUTLOOK, where other applications can be connected to user accounts.



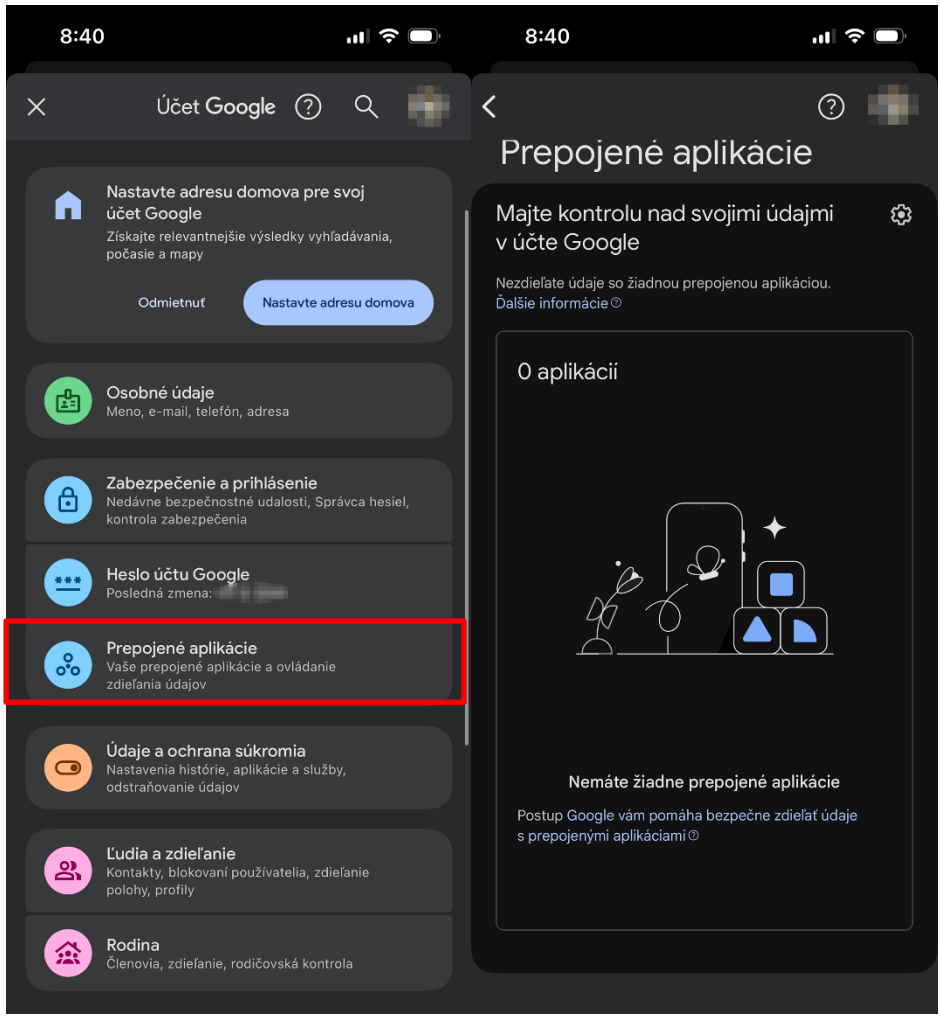
Linked devices in the Telegram messaging application



Linked devices in the Signal messaging application



Linked devices in the WhatsApp messaging application



Linked devices in the GMAIL messaging application

4. **You unexpectedly received an invitation to join a chat group using a link or QR code together with instruction on how to proceed.** This method is used by attackers to add their own device to your user account.

5. **You notice in the messaging application that the messages you have not read yet are already marked as read.** In this case, check the list of linked devices to make sure there is no unknown device.

6. **You notice in the messaging application that there are messages among your sent messages that you did not write, but were sent under your**

name. In this case, check your linked devices to ensure that there is no unknown device.

7. **You notice that a chat group now contains an unknown phone number or a new account.** In such case, inform directly the administrator who created the group about it.

Recommendations for Users

If you use the Signal messaging application or similar communication applications, we recommend applying the following measures:

1. **Delete your user account and uninstall the messaging application if you do not use it for a long time.**

2. **Enable the „Registration lock“**
   - When re-registering your phone number, you will be required to enter your user security PIN code. This prevents the attacker with a valid verification code from finishing account take over because they will not know the user-defined security PIN code.
   - Setting: „Settings“ > „Account“ > „Registration lock“ > „Enable“.

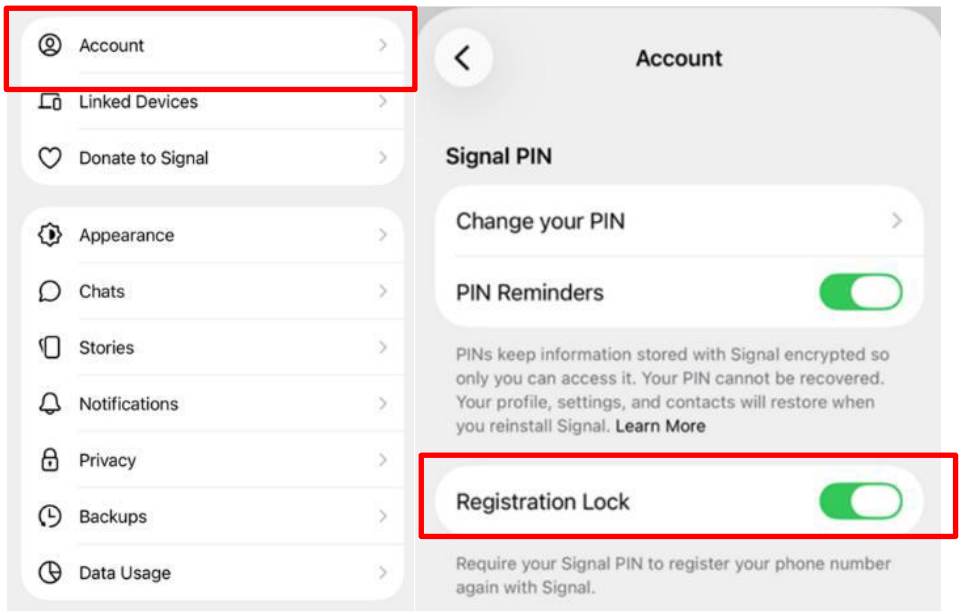
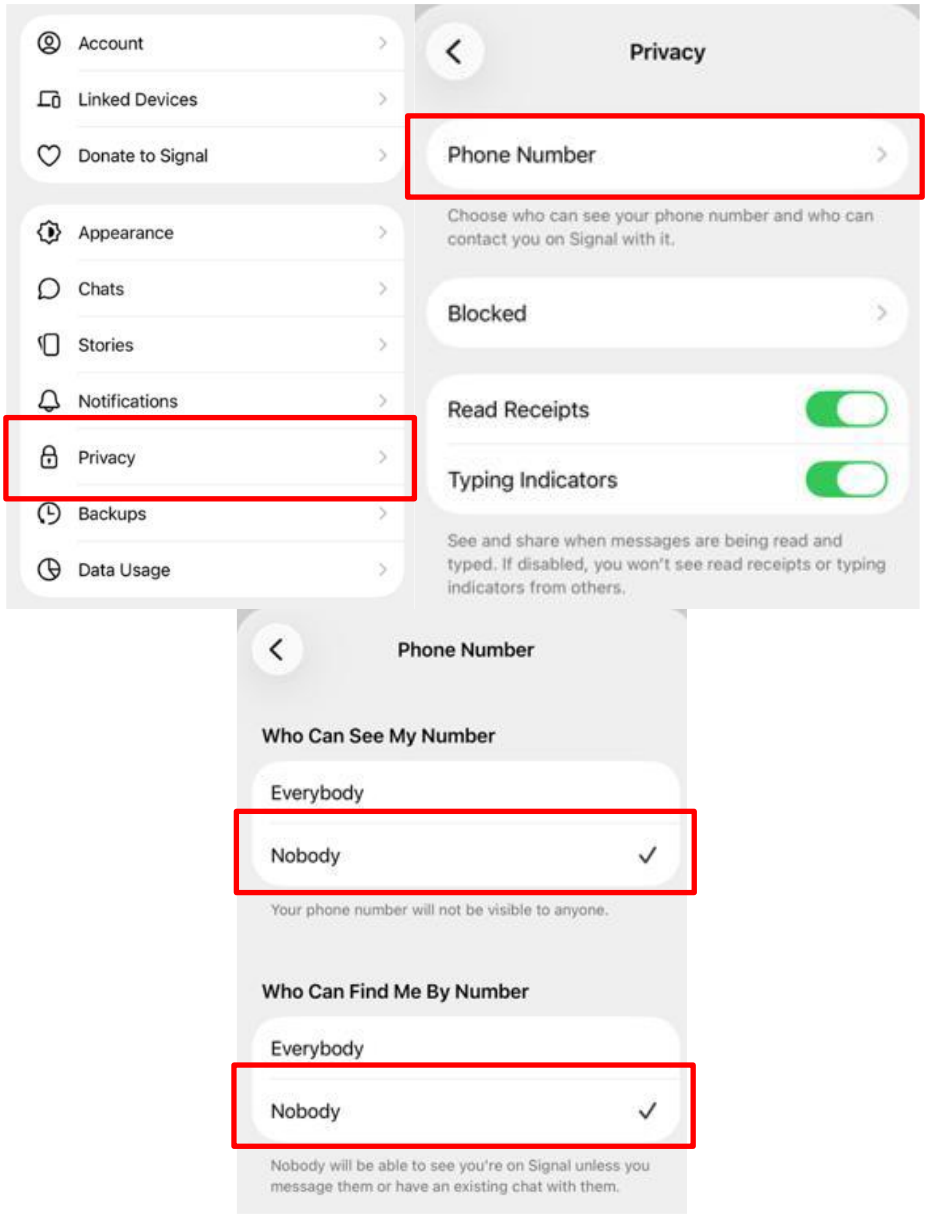


Illustration of the instructions for enabling Registration lock

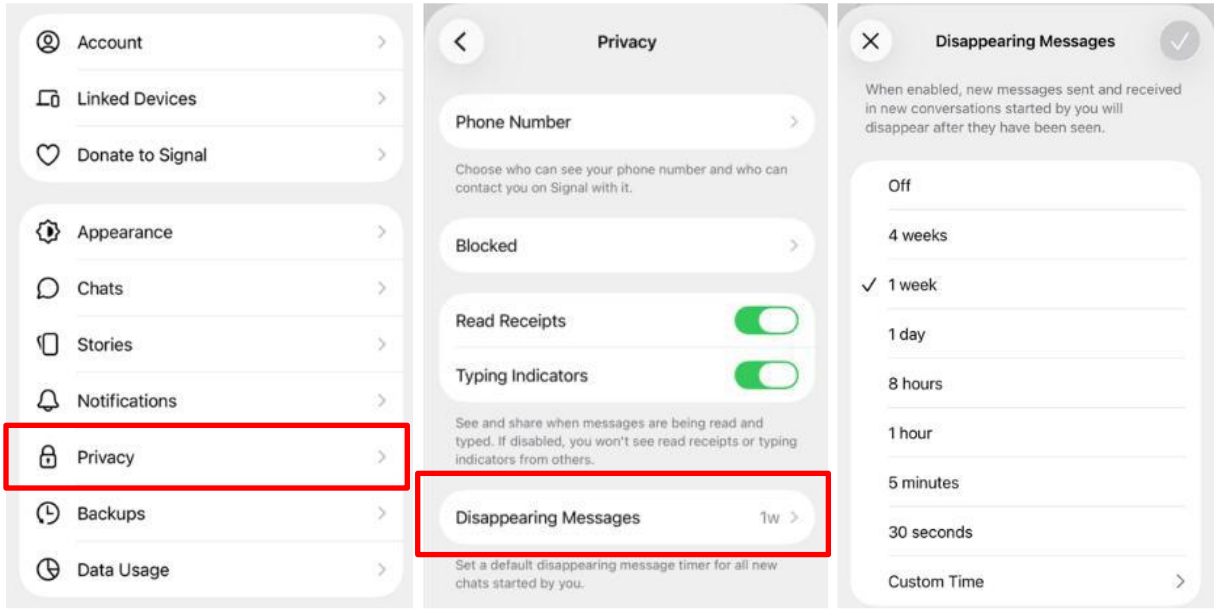
3. **Configure who can find you using your phone number and who can see your phone number.**
   - This makes it more difficult for a potential attacker to contact you using your phone number. In addition, if an attacker gains access to the chat group you are a member of, your phone number will not be visible to the attacker.
   - Setting: „Settings“ > „Privacy“ > „Phone number“ > „Who can find me by my phone number“ > select „Nobody“ .

- Setting: „Settings“ > „Privacy“ > „Phone number“ > „Who can see my phone number“ > select „Nobody“
- To find your profile (you), a person will need to know your username.



Instructions for limiting the visibility of your profile in the Signal application

4. Consider using the so called „Disappearing Messages“



Instructions for enabling „Disappearing messages“

5. **Do not respond to messages claiming to be from „technical support“.**
   - Technical support will never contact you directly through a messaging application.

6. **Block and report accounts impersonating the support team of the messaging application.**

7. **Never provide your security PIN code to anyone who requests it via SMS, a message in a messaging application, or during a phone call.**

8. **Scan QR codes using the messaging application only when you have personally decided to link another device to that messaging application.**

9. **Ignore invitations to chat groups if you were not expecting them or if they come from unknown contacts.**

10. **Regularly check the list of devices linked to your account.**
    - Immediately remove any unknown devices linked to your accounts.

11. **If you are unsure of the identity of the person you are communicating with, verify their identity through another communication channel if possible.**

Measures for Chat Group Administrators

If a compromised user account is identified in a chat group, proceed as follows:

1. Stop communicating with the affected user through the messaging application.
2. Restrict the affected user's access to chat groups that you manage.
3. Contact the affected user outside the messaging application and ask them to register a new user account with a new phone number.
4. Ask the affected user to apply the measures described in the „Recommendations for Users" section.
5. Add the new user account to the chat group.

If you suspect that user accounts in your chat group may have been compromised, proceed as follows:

1. Stop communicating with suspicious users through the messaging application.
2. Suspend the use of any chat groups you administer that contain suspicious user accounts.
3. Ask all users to remove all linked devices from their user accounts.
4. Create a new chat group.
5. Invite only those users whose accounts have not been confirmed as compromised to the new chat group.
6. Treat the remaining users as compromised and follow the procedure for identifying a compromised user account in a chat group.

If the availability of the chat group is high/critical for its intended purposes and the procedure described above cannot be applied directly, take the following steps:

1. Contact the members of the group through a communication channel other than the compromised chat group and inform them that communication in the chat group may have been monitored (compromised) by an attacker.
2. Assess whether it is absolutely necessary to continue using the current chat group.
3. Continue monitoring the chat groups under your administration.
4. If possible, treat all users as though they have been compromised and continue according to the procedure described above.
5. Create a new chat group.
6. Require all users to apply the recommended security measures for users.
7. Add the newly created user accounts to the new chat group.
8. After all users have been transferred to the new chat group, delete the original (compromised) chat group.

The purpose of this document is to:

1. increase security awareness among users of messaging applications,
2. improve user´s resilience against social engineering attacks,
3. minimize the risk of compromised accounts being used to spread phishing messages, fraud or malicious content,
4. prevent unauthorized takeover of user accounts,
5. ensure the timely detection of potential account compromise and enable a rapid response to security incidents,
6. protect the confidentiality, integrity and security of user accounts and shared information.

This document is recommended for distribution to:

1. professional soldiers and employees of the Ministry of Defence,
2. organizations operating under the Ministry of Defence of the Slovak Republic,
3. organizations and entities that communicate with the Ministry of Defence under contractual arrangements (e.g. suppliers).

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