



Cybersecurity Advisory

Phishing via messaging apps Signal and WhatsApp

Netherlands Defence Intelligence and Security Service (MIVD)

General Intelligence and Security Service (AIVD)

March 2026



Cybersecurity Advisory

TLP:CLEAR

Phishing via messaging apps Signal and WhatsApp

March 2026

Key points

- Intelligence from the Netherlands Defence Intelligence and Security Service (MIVD) and the Netherlands General Intelligence and Security Service (AIVD) ('the Dutch services') reveals that Russian state actors are engaged in a large-scale global attempt to compromise Signal and WhatsApp accounts of dignitaries, civil servants and military personnel.
- Dutch government employees have also been targets and victims of this campaign. The services further deem it probable that targets include other persons of interest to the Russian government, such as journalists.
- The actors primarily make use of phishing and social engineering techniques to take over accounts or to link their devices.
- The advice of the Dutch services is that sensitive information should not be communicated using messaging apps which are neither intended nor suitable for this purpose.
- It is important to remain alert to messages that appear to be sent by Signal. The Signal customer service department never makes direct contact via a Signal message.
- Users are also advised to ignore requests via QR codes or links unless the legitimacy of the QR code or link has first been verified through contact with the purported sender.
- If a user discovers that their account has been compromised, they should inform all their contacts via another channel.
- Users can check for compromised contacts themselves; if a contact appears twice in Signal chat groups or has an unusual name, this may indicate a compromise.
- The Dutch services wish to stress that they are referring to the compromise of individual accounts and are not suggesting that Signal or WhatsApp themselves have been compromised.

TLP:CLEAR



Cybersecurity Advisory

TLP:CLEAR

Phishing via messaging apps Signal and WhatsApp

March 2026

Context

Intelligence from the Netherlands Defence Intelligence and Security Service (MIVD) and the Netherlands General Intelligence and Security Service (AIVD) ('the Dutch services') reveals that Russian state actors are engaged in a large-scale global attempt to compromise Signal and WhatsApp accounts of dignitaries, civil servants and military personnel.

Once an account has been successfully compromised, the actor may have access to the telephone numbers of the victim's contacts and may be able to read messages sent to the victim. In certain situations the actor may also be able to read messages in the chat groups of which the victim is a member.

It should be noted that attacks of this nature do not use malware, nor do they exploit any technical vulnerabilities of the messaging services. The attackers instead utilise legitimate security functions of the apps in combination with social engineering techniques.

The attacks target both Signal and WhatsApp. In the case of WhatsApp, the actor primarily appears to make use of the 'linked devices' function through malicious invitations to join chat groups.

The Dutch services emphasise that they are referring here to the compromise of individual accounts and are not suggesting that Signal or WhatsApp themselves have been compromised.



Cybersecurity Advisory

TLP:CLEAR

Phishing via messaging apps Signal and WhatsApp

March 2026

There are two modes of attack:

1. 'Account take-over'

In many cases the attackers pose as the official support team or the support chatbot of the messaging service. The victim receives a message purportedly from the Signal Security Support Chatbot, claiming for example that suspicious activities have been observed in the victim's account. The message also warns of a possible data leak and that attempts to gain access to the private data in Signal have been detected. The message then states that the victim can prevent this by going through the verification process and sharing the verification code with the chatbot.

After the conversation is accepted, the actor subsequently requests the verification code that the victim receives via sms from Signal (as a result of the actor's initiation) and the PIN that the victim has set within Signal. With this PIN the actor can also take control of accounts protected by Registration Lock (see the "Advice" section).

By using these codes, the actor fully takes control of the user account and changes the phone number linked to that account to a mobile number that they control. The actor then has full access to the contact lists and new messages in both one-to-one messages sent to the compromised account and group chats to which the compromised account belongs. The actor can also potentially send messages in the victim's name.

The victim is unable to access their account, although they are able to create a new Signal account using their existing telephone number, as the actor has already linked the compromised account to a new telephone number. Because Signal stores the chat history locally on the phone, a victim can regain access to that history after re-registering. As a result, the victim may assume that nothing is wrong. The Dutch services want to stress that this assumption could be incorrect.

The Dutch services emphasise that the example message in Fig. 1 is currently only the most common illustration of such a message and the method of account takeover. It is possible that attackers, in the future, devise other similar messages or employ other methods.

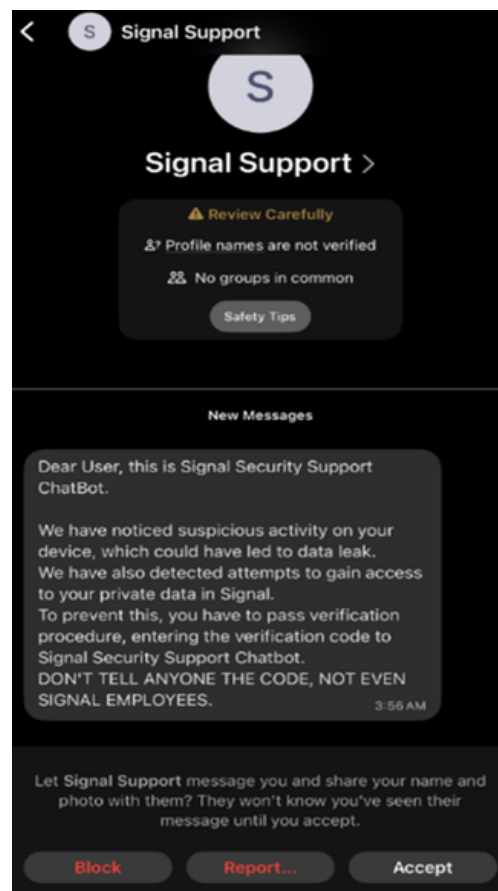


Figure 1. Example of Signal message



Cybersecurity Advisory

TLP:CLEAR

Phishing via messaging apps Signal and WhatsApp

March 2026

2. 'Linked devices and QR codes'

Actors use social engineering to persuade the victim to scan a QR code or click on a link. This method is used for Signal as well as WhatsApp accounts.

In these messaging apps, QR codes can be used to add contacts, share contact information and add individuals to chat groups. QR codes can also be used to make contact with companies and to use the messaging app on other devices (linked devices). The widespread use of QR codes and links makes this an attractive method for actors to induce victims to scan codes or click on links. For example, an actor may send a QR code or link to a victim to add them to a chat group, but this QR code or link actually links the actor's device to the victim's account.

This linked device, or the desktop version of the messaging app, gives the actor full access to all the victim's chats, often including the chat history. The actor is also able to read messages sent by the victim, and even to send messages in the victim's name. The victim retains access to their account, but does not usually immediately notice that someone else is accessing their communication.





Cybersecurity Advisory

TLP:CLEAR

Phishing via messaging apps Signal and WhatsApp

March 2026

Advice

Messaging apps are an important means of communication, for both business and personal contacts. However many measures are taken, there is always a risk of losing data through messaging apps. Use messaging apps wisely, consider whom you keep in contact with and what you communicate.

- It is important to never use a messaging app to send classified or sensitive information. Such information may only be sent using devices or apps that have been approved for this purpose by your organisation. Limit your use of messaging apps to the policy or level of classification established by your organisation.
- Regularly check the list of devices that have access to your Signal and/or WhatsApp account. You can find these under: Profile-icon (Signal) and the three dots (WhatsApp) -> Linked devices. Delete unknown devices immediately.
- Signal's customer services will never contact you directly via a Signal message, neither will they ask you for your verification codes via a Signal message. Do not respond to Signal messages from purported support accounts. Block or report accounts purporting to be Signal support accounts.
- Never give your Signal PIN in an sms or Signal message. Legitimate requests for PIN verification can be recognised by the fact that your PIN never appears in plain text but only as asterisks or dots.
- Scan QR codes only with the Signal or WhatsApp app when you are personally linking a device to Signal or WhatsApp.
- Ignore unsolicited invitations to join group chats or invitations from unknown contacts. If in doubt, contact the person in question through a different trusted channel to verify the invitation. Consider automatic blocking of unknown contacts or contacts who are not in your contact list.
- Where possible use a user name rather than a telephone number, or utilize the option to hide your telephone number. Hiding your telephone number from an actor reduces the attack surface of your device and hinders a phishing attack or account takeover.
- Activate Registration Lock in Signal via: Settings -> Account -> registration lock -> toggle the switch.
- Consider activating the automatic Disappearing Messages feature. Should your device or messaging app account be compromised, this will prevent the actor from gaining access to the entire chat history.

TLP:CLEAR



Cybersecurity Advisory

TLP:CLEAR

Phishing via messaging apps Signal and WhatsApp

March 2026

Advice

Analyze contacts for indications of compromise

All Signal users can personally check whether there are any potentially compromised contacts in their group chats. If you see any people who appear twice in the list of members (under the same or a slightly different name), this may be evidence of either a compromised account or a new account created by a victim.

If you suspect this to be the case, report this to the information security department of your organisation. Together you can try to verify (preferably using a channel other than Signal or WhatsApp, such as an email or a telephone call) whether it is correct that the account in question appears twice in the chat group contact list. Should this not be the case, ask the group administrator to remove both accounts from the group chat, after which the legitimate account holder can request to rejoin the group.

Please remain vigilant for group members who are not recognised by the rest of the group. The actor may occasionally change the display name of a compromised account to remain unnoticed in chat groups, for example to names such as 'Deleted account'. If a member's display name changes, the group will receive a notification. When the change is the legitimate transition to 'Deleted account', no notification is sent. Actor-controlled accounts can also gain entry to the group via an obtained Group Link, of which the group always receives a notification. In all such unauthorised scenarios, ask the group administrator to remove the offending accounts from the chat.

If there is any indication that the group administrator themselves may have been compromised, it is advisable to exit the group and create a new one.



TLP:CLEAR



Cybersecurity Advisory

TLP:CLEAR

Phishing via messaging apps Signal and WhatsApp

March 2026

Think you may be a victim?

If you have doubts about strange behaviour in your messaging app, if you have received verification codes via an sms that you do not recognise, or if you temporarily lost control of your messaging app or had to spontaneously reactivate it, you should report this to your security adviser or to the Security Authority Office as soon as possible.

Signal is not managed by a central party. There are no facilities for retrieving or deactivating an account that has been taken over, nor for recovering the associated data such as chats and contact lists. The loss of an account is irreversible and can lead to lasting damage unless all contacts are informed (in some cases repeatedly) about the compromised account.

Your contacts will not be able to tell whether your account has been compromised in one-to-one chats, and may therefore assume that they are still able to send messages to you when that is not the case. It is therefore very important that you inform your contacts about this. Failing to report or waiting longer increases the risk of further damage to you, your organisation and your contacts. If you do inform your contacts, do so preferably by a method other than Signal or WhatsApp (e.g. email or telephone).



Cybersecurity Advisory

TLP:CLEAR

Phishing via messaging apps Signal and WhatsApp

March 2026

Further reading

For further reading, please consult the resources below:

- CISA, Mobile Communications Best Practice Guidance, d.d. 18 december 2024,
<https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf>
- Politie, Wat gebeurt er als uw WhatsApp-account is gehackt (overgenomen)?,
<https://www.politie.nl/informatie/wat-gebeurt-er-als-uw-whatsapp-account-is-gehackt-overgenomen.html>
- NCSC, Phishing uitgelegd,
<https://www.ncsc.nl/phishing/phishing-uitgelegd>
- Surveillance Self-Defense, How to: Use WhatsApp, d.d. 3 april 2025,
<https://ssd.eff.org/module/how-to-use-whatsapp>
- Surveillance Self-Defense, How to: Use Signal, d.d. 26 maart 2025,
<https://ssd.eff.org/module/how-to-use-signal>
- Bundesamt für Sicherheit in der Informationstechnik, Phishing über Messengerdienste, d.d. 6 februari 2026,
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/202602_BfV_BSI_Sicherheitshinweis.html

About this Cybersecurity Advisory

A Cybersecurity Advisory (CSA) is intended to give users practical instructions in the form of security measures, in order to increase resilience against state actors. The Netherlands General Intelligence and Security Service (AIVD) and the Netherlands Defence Intelligence and Security Service (MIVD) have issued these instructions based on assessed intelligence, knowledge and expertise, with a focus on national security.

Distribution of this Cybersecurity Advisory

This document is marked **TLP:CLEAR**. This means that this Cyber Advisory may be released and distributed without restrictions.