≡Q   ⦿ Watch Live

BBC

Home   **News**   **Sport**   **Business**   **Technology**   **Health**   **Culture**   **Arts**   **Travel**   **Earth**   **Audio**   **Video**   **Live**   **Documentaries**

Signal issues scam warning to users after hackers target officials

49 minutes ago   Share ⦉   Save ⦟

Liv McMahon
Technology reporter

Getty Images

Signal has warned users to look out for signs of scams, after Dutch intelligence said high-profile users of the secure messaging app were being targeted by hackers.

Dutch cybersecurity agencies said on Monday a Russia-backed campaign had targeted individual users of Signal, as well as WhatsApp.

They said this had seen hackers pose as support staff to try and obtain details that would give them access to accounts or hijack linked devices - with Dutch officials, military staff and civil servants among those targeted in the "global" campaign.

Signal says its systems remain secure but it is taking reports of such activity "very seriously".

The campaign was identified by Dutch intelligence agencies, the Military Intelligence and Security Service (MIVD) and General Intelligence and Security Service (AIVD).

They said **in a press notice** the "large-scale global cyber campaign" appeared to target people of interest to the Russian state, such as government officials and journalists.

"It is not the case that Signal or WhatsApp as a whole have been compromised. Individual user accounts are being targeted," said Simone Smit, AIVD director-general.

Signal reiterated this **in a series of posts on X**, stressing its systems "have not been compromised and remain robust".

"These attacks were executed via sophisticated phishing campaigns, designed to trick users into sharing information – SMS codes and/or Signal PIN – to gain access to users' accounts," it wrote.

So-called phishing attacks see criminals attempt to convince users to part with passcodes, money or details about their identity - often by impersonating customer support agents, friends, family and celebrities.

In the campaign identified by Dutch intelligence agencies, hackers pretended to be Signal Support to try and get people to share account details.

Allow X content?

This article contains content provided by X. We ask for your permission before anything is loaded, as they may be using cookies and other technologies. You may want to read X's cookie policy and privacy policy before accepting. To view this content choose **'accept and continue'**.

Users are asked when creating a Signal account to secure it with a PIN code - something it says should never be shared with anyone.

The company added users should also not share verification codes messaged to their phone number.

WhatsApp has given similar advice, saying users should not share six-digit codes used to secure their account.

It also says people can take extra steps **to secure their accounts**, including by blocking unknown messages or calls.

- What is the Signal messaging app and how secure is it?

'Human bugs'

Signal has stressed while they have protections in place, "user vigilance" is the best way to combat phishing attempts.

"Security features are being weaponised against the users," said Muhammad Yahya Patel, cybersecurity advisor at security firm Huntress.

"In the past, hackers looked for bugs in code. Now, they are looking for human bugs in how humans interact with apps," he told the BBC.

He said convenient features such as letting users access their account on other devices via QR codes, or regain access to it with text verification codes, have become "primary attack vectors being used by criminals".

Patel urged people to regularly check devices linked to their account in settings to make sure no one else can access their messages.

He said users should also be mindful that using an app with end-to-end encryption (E2EE) does not mean "total security".

WhatsApp users can limit who can see their profile picture, live location or add them to groups in the app's settings

E2EE, used to protect messages on Signal and WhatsApp, means only the sender and receiver of a message can read it.

"This type of encryption can't protect the account and device if it becomes compromised," Patel said.

Dutch intelligence services believe Russia targeted Signal because its reputation as a highly secure app has made it popular with officials seeking to communicate securely.

But they said this has also made the app "the ideal place for malicious actors" to try and capture sensitive information.

"Despite their end-to-end encryption option, messaging apps such as Signal and WhatsApp should not be used as channels for classified, confidential or sensitive information," said MIVD director Peter Reesink.

Dr Pia Hüsch, cyber research fellow at the Royal United Services Institute (Rusi), said "a lot of malicious actors in cyber-space are exploiting these apps".

But she added the use of "plain old phishing attempts" here may surprise some.

"Sometimes we think of state actors as these incredibly sophisticated threat actors that have all the capabilities and fancy tools... but this is a fairly basic way to try to gain access to something," Dr Hüsch said.

Additional reporting by Richard Morris

Five takeaways from leaked US top military chat group
TikTok won't protect DMs with controversial privacy tech, saying it would put users at risk
How does WhatsApp make money? It's free - with some tricks

Sign up for our Tech Decoded newsletter to follow the world's top tech stories and trends. **Outside the UK? Sign up here**.

End-to-end encryption   Cyber-security   Privacy

RELATED

TikTok won't protect DMs with controversial privacy tech, saying it would put users at risk

Apple's encryption row with UK should not be secret, court rules

Secret hearing on Friday in Apple and UK government data row

MORE FROM THE BBC

5 days ago

TfL hack in 2024 affected around 10 million people, BBC can reveal

TfL insists it has "kept customers informed throughout this incident and will continue to take all necessary action".

5 days ago

6 days ago

We have more privacy controls yet less privacy than ever

Has online privacy become "a luxury not a right" for us all in 2026?

6 days ago

6 days ago

The most important Google setting you aren't using

There's a free automated tool that removes information about you from Google search results. For some reason, most people don't use it.

6 days ago

26 Feb 2026

Four convicted over spyware scandal that shook Greece

In what became known as "Greece's Watergate", surveillance software called Predator was used to target 87 people.

26 Feb 2026

24 Feb 2026

Reddit fined £14m for 'concerning' child age check failings

The UK's data watchdog said the failings meant children could be exposed to harmful material online.

24 Feb 2026

BBC

Home **News** **Sport** **Business** **Technology** **Health** **Culture** **Arts** **Travel** **Earth** **Audio** **Video** **Live** **Documentaries**

Weather **BBC Shop** **BritBox**

BBC in other languages ▼