EXECUTIVE PROTECTION

An Executive’s WhatsApp Can Be Taken Over Without Touching Their Phone

On 9 March 2026, the Dutch intelligence services AIVD and MIVD warned of a global campaign by Russian state actors to take over the Signal and WhatsApp accounts of dignitaries, civil servants and military personnel. According to the advisory, the attackers used neither malware nor flaws in the apps. On WhatsApp they mainly abused the linked devices feature: a QR code or link that looked like an invitation to a group actually linked the attacker’s device to the account.

The victim kept using WhatsApp as normal while the linked device could read chats, often including their history, and send messages in the victim’s name. The advisory also describes, with a Signal example, messages posing as the app’s official support to ask for codes and PINs. That campaign targeted people of interest to the Russian state, not Venezuelan business owners; what matters here is the technique, which needed no stolen phone.

The advisory was published by the Netherlands’ AIVD on 9 March 2026.
https://english.aivd.nl/site/binaries/site-content/collections/documents/2026/03/09/cybersecurity-advisory.-phishing-via-messaging-apps-signal-and-whatsapp/cybersecurity-advisory-phishing-via-messaging-apps-signal-and-whatsapp.pdf

Usernames Open Another Route to Impersonation

On 29 June 2026, Meta opened WhatsApp username reservations and said the feature would launch later this year. There will be no directory: to message someone for the first time you will need their exact username. Creators, small businesses and organisations can claim the name they already use on Instagram or Facebook. According to BleepingComputer, the rollout is gradual, the app tells people when it reaches their country, and some names are held for governments, public figures and businesses.

The reservation announcement is on Meta’s newsroom, 29 June 2026.
https://about.fb.com/news/2026/06/its-time-to-reserve-your-whatsapp-username/

TechCrunch reported on 1 July 2026 that, in its testing, usernames resembling Indian politicians, business figures and institutions were still free to reserve. According to TechCrunch, India’s Ministry of Electronics and Information Technology sent WhatsApp a notice warning of more fraud and impersonation and asking it not to launch the feature until consultations were complete. Meta said it reserves names for public figures, government entities and some variations, without explaining how it chooses which. For an executive, the practical risk is someone writing to their staff or family under an almost identical name, with no phone number to compare.

This was reported by TechCrunch on 1 July 2026.
https://techcrunch.com/2026/07/01/whatsapp-usernames-are-already-raising-impersonation-red-flags/

The Defences Exist, but Someone Has to Use Them

WhatsApp added protections this year. Meta announced on 11 March 2026 that the app warns when behavioural signals suggest a device-linking request may be a scam, and shows where the request comes from. In January it introduced Strict Account Settings, which, according to Security Affairs, blocks attachments and media from unknown senders and silences calls from people you do not know; it is switched on in the advanced privacy section of the settings. And in August, according to BleepingComputer, it began testing Scam Alert, an optional warning that analyses messages on the phone itself, in a limited beta with researchers from its bug bounty programme. The linking warning only helps if the person who sees it stops, strict settings have to be switched on, and Scam Alert started as a limited test.

A Routine for the Executive, Their Staff and Their Family

- Once a month, open Linked devices on the main phone (in the settings or the three-dot menu, depending on the phone) and log out of any device you do not recognise.
- Turn on two-step verification with a PIN you use nowhere else and a recovery email you control.
- Switch on Strict Account Settings if the executive’s exposure justifies it, knowing it will limit attachments and calls from unknown people.
- Reserve the executive’s and the company’s usernames now; if the company already has an Instagram or Facebook name, consider claiming that same one.
- Scan a device-linking QR code only when you are connecting one of your own devices yourself, and ignore group invitations you did not expect.

Write down two short rules for staff and family. No real support team asks for codes, PINs or a QR scan over chat. And any message from a new username or number claiming to be the executive is confirmed through a known second channel, such as a call to the usual number, before anyone replies with information, payments or access.

How Executive Digital Protection Does It

We go through the linked devices list on each WhatsApp account with the executive, and with their family if they agree, log out the devices nobody recognises and set the monthly review. We turn on two-step verification and, where the risk justifies it, Strict Account Settings, explaining first what stops working. We reserve the executive’s and the company’s usernames and write the

impersonation protocol with each person’s confirmation channel. If an account impersonating the executive appears, we prepare the takedown request through WhatsApp’s reporting channels.

> *No setting prevents someone from deceiving a person close to the executive. When usernames and features such as Scam Alert reach each country depends on WhatsApp, and the removal of an impersonating account is the platform’s decision.*

A Check You Can Run

Take the executive’s main phone and open Linked devices in WhatsApp (in the settings or the three-dot menu, depending on the phone). Write down every computer, tablet, browser or other device on the list next to the person who uses it. Any entry nobody can account for gets logged out from that same screen, and the review goes in the calendar for next month. Do it together, without reading anyone’s chats. WhatsApp also disconnects linked devices after 30 days of inactivity, so a short list is normal.

Supporting guidance: WhatsApp’s help page on linked devices.
https://faq.whatsapp.com/378279804439436/

Continue with: If You Lose Your Phone, Where Will You Get Help?.
https://systems.kavaliero.com/en/blog/if-you-lose-your-phone-where-will-you-get-help

For help with this work, see the scope of Executive Digital Protection.
https://systems.kavaliero.com/en/services/executive-security