BLINDAJE EJECUTIVO

El WhatsApp de un Directivo Se Puede Tomar sin Tocar Su Teléfono

El 9 de marzo de 2026, los servicios de inteligencia neerlandeses AIVD y MIVD advirtieron de una campaña mundial de actores estatales rusos para tomar cuentas de Signal y WhatsApp de dignatarios, funcionarios y militares. Según el aviso, no usaban malware ni fallos de las aplicaciones. En WhatsApp aprovechaban sobre todo la función de dispositivos vinculados: un código QR o un enlace que parecía una invitación a un grupo vinculaba en realidad el equipo del atacante a la cuenta.

La víctima seguía usando su WhatsApp con normalidad, mientras el dispositivo vinculado podía leer los chats, a menudo con su historial, y escribir en su nombre. El aviso describe también, con un ejemplo de Signal, mensajes que se hacen pasar por el soporte oficial de la aplicación para pedir códigos y PIN. Esa campaña buscaba a personas de interés para el Estado ruso, no a empresarios venezolanos; lo que sirve aquí es la técnica, que no necesitó robar ningún teléfono.

El aviso fue publicado por el AIVD de los Países Bajos el 9 de marzo de 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

Los Nombres de Usuario Abren Otra Forma de Suplantar

El 29 de junio de 2026, Meta abrió la reserva de nombres de usuario de WhatsApp y dijo que la función se lanzaría más adelante este año. No habrá directorio: para escribirle a alguien por primera vez hará falta su nombre exacto. Creadores, pequeñas empresas y organizaciones pueden reclamar el nombre que ya usan en Instagram o Facebook. Según BleepingComputer, el despliegue es gradual, la aplicación avisa cuando llega a cada país y algunos nombres quedan apartados para gobiernos, figuras públicas y empresas.

El anuncio de la reserva está en la sala de prensa de Meta del 29 de junio de 2026.
https://about.fb.com/news/2026/06/its-time-to-reserve-your-whatsapp-username/

TechCrunch informó el 1 de julio de 2026 que, en sus pruebas, nombres parecidos a los de políticos, empresarios e instituciones de India seguían libres para reservar. Según el mismo medio, el Ministerio de Electrónica y Tecnologías de la Información de India envió a WhatsApp una notificación en la que advertía de más fraude y suplantación y le pedía no lanzar la función hasta terminar unas consultas. Meta respondió que reserva nombres de figuras públicas, entidades de gobierno y algunas variantes, sin explicar cómo elige cuáles. Para un ejecutivo, el riesgo práctico es

que alguien escriba a su equipo o a su familia con un nombre casi igual y sin un número de teléfono que comparar.

Lo publicó TechCrunch el 1 de julio de 2026.
https://techcrunch.com/2026/07/01/whatsapp-usernames-are-already-raising-impersonation-red-flags/

Las Defensas Existen, Pero Alguien Tiene que Usarlas

WhatsApp añadió protecciones este año. Meta anunció el 11 de marzo de 2026 que la aplicación avisa cuando ciertas señales sugieren que una solicitud de vinculación puede ser una estafa, y muestra desde dónde llega. En enero presentó Strict Account Settings, una configuración estricta que, según Security Affairs, bloquea adjuntos y archivos multimedia de remitentes desconocidos y silencia llamadas de quien no conoces; se activa en la sección avanzada de privacidad de los ajustes. Y en agosto, según BleepingComputer, empezó a probar con investigadores de su programa de recompensas por fallos una beta limitada de Scam Alert, un aviso opcional que analiza los mensajes dentro del propio teléfono. El aviso de vinculación solo sirve si quien lo ve se detiene, la configuración estricta hay que activarla y Scam Alert empezó como una prueba limitada.

Una Rutina para el Ejecutivo, Su Equipo y Su Familia

- Una vez al mes, abre Dispositivos vinculados en el teléfono principal (en los ajustes o en el menú de tres puntos, según el teléfono) y cierra la sesión de cualquier equipo que no reconozcas.
- Activa la verificación en dos pasos con un PIN que no uses en ningún otro lugar y un correo de recuperación que controles.
- Activa la configuración estricta si la exposición del ejecutivo lo justifica, sabiendo que limitará adjuntos y llamadas de desconocidos.
- Reserva ahora el nombre de usuario del ejecutivo y el de la empresa; si la empresa ya tiene un nombre en Instagram o Facebook, valora reclamar ese mismo.
- Escanea un código QR de vinculación solo cuando tú mismo estés conectando un equipo tuyo, e ignora invitaciones a grupos que no esperabas.

Deja por escrito, para el equipo y la familia, dos reglas cortas. Ningún soporte real pide códigos, PIN ni que escanees un QR por chat. Y cualquier mensaje desde un nombre de usuario o un número nuevo que diga ser el ejecutivo se confirma por un segundo canal ya conocido, como una llamada al número de siempre, antes de responder con datos, pagos o accesos.

Cómo lo Hace Blindaje Ejecutivo

Revisamos con el ejecutivo, y con su familia si lo acuerdan, la lista de dispositivos vinculados de cada WhatsApp, cerramos los que nadie reconoce y fijamos la revisión mensual. Activamos la verificación en dos pasos y, donde el riesgo lo justifica, la configuración estricta, explicando antes qué deja de funcionar. Reservamos los nombres de usuario del ejecutivo y de la empresa y redactamos el protocolo de suplantación con el canal de confirmación de cada persona. Si aparece una cuenta que se hace pasar por el ejecutivo, preparamos la solicitud de retirada por los canales de denuncia de WhatsApp.

> *Ninguna configuración impide que alguien engañe a una persona del entorno. La llegada de los nombres de usuario y de funciones como Scam Alert a cada país depende de WhatsApp, y la retirada de una cuenta suplantadora la decide la plataforma.*

Una Comprobación Concreta

Toma el teléfono principal del ejecutivo y abre Dispositivos vinculados en WhatsApp (en los ajustes o en el menú de tres puntos, según el teléfono). Anota cada computadora, tableta, navegador u otro equipo de la lista junto a la persona que lo usa. Si nadie puede explicar una entrada, cierra su sesión desde esa misma pantalla y deja la próxima revisión en el calendario del mes siguiente. Háganlo juntos y sin leer los chats de nadie. WhatsApp también desconecta los dispositivos vinculados tras 30 días sin actividad, así que una lista corta es normal.

Documentación de apoyo: Página de ayuda de WhatsApp sobre dispositivos vinculados.
https://faq.whatsapp.com/378279804439436/

Para seguir leyendo: Si Pierdes el Teléfono, ¿desde Dónde Vas a Pedir Ayuda?.
https://systems.kavaliero.com/blog/si-pierdes-el-telefono-que-haces-primero

Si necesitas ayuda con este trabajo, consulta el alcance de Blindaje Ejecutivo.
https://systems.kavaliero.com/soluciones/blindaje-digital