ZEROFOX INTELLIGENCE

Flash

Introduction of WhatsApp Usernames

F-2026-07-29a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Social Engineering, Threat Actor, Fraud

July 29, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EDT) on July 29, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Introduction of WhatsApp Usernames

| Key Findings

- On June 29, 2026, Meta began allowing WhatsApp's three-billion-plus users to reserve a username that new contacts can use instead of a phone number, ahead of a phased, country-by-country rollout later in 2026.
- ZeroFox assesses the feature will likely act as a threat multiplier by increasing the credibility of impersonation and social engineering campaigns rather than introduce a fundamentally new attack method.
- Meta has reportedly reserved usernames tied to public figures, government entities, celebrities, and verified accounts and added limits on new-contact messaging volume and username key guessing; ZeroFox assesses these controls will likely reduce, but not eliminate, abuse.
- Within 48 hours of the announcement, India's Ministry of Electronics and Information Technology (MEITy) issued a formal notice warning the feature could materially increase online fraud, phishing, digital arrest scams, and impersonation attacks and temporarily paused rollout in that market; Finland's national cyber authority (Traficom) issued a similar public warning in early July.

- ZeroFox assesses that impersonation risk is very likely to be highest during the initial rollout window, as threat actors test platform controls and attempt to register deceptive usernames before enforcement matures.

Overview

Feature Status	Key Safeguards	Primary Risk	Regulatory Responses
Reservations open; messaging-by-username rolling out gradually by country later in 2026	No public directory; optional username key; high-profile names reserved; rate limits	More convincing impersonation of brands, executives, and support functions	India (MEITy notice, rollout paused); Finland (Traficom warning)

Overview of the WhatsApp username rollout
Source: ZeroFox Intelligence

On June 29, 2026, Meta announced usernames for WhatsApp to allow people to connect with new contacts without sharing their phone number.[1] There is no public directory; a sender must know the exact handle. An optional username key can gate first contact further. Existing contacts who already have the receiver's number are unaffected; the change applies to first contact with new people.

- Meta's reservation of high-profile names and look-alike variants very likely lends meaningful protection to global brands and public figures compared to unprotected namespaces on other platforms.
- ZeroFox has observed that impersonation of customer support, fraud investigators, recruiters, sales representatives, and executives is already a common tactic, technique and procedure (TTP) across social media and messaging platforms to facilitate credential theft, financial fraud, business email compromise, and investment scams.
- The concealment of phone numbers during first contact removes a weak but real historical screening signal (unfamiliar international numbers occasionally flagged potential fraud), shifting the trust decision onto the username.

[1] hXXps://about.fb[.]com/news/2026/06/its-time-to-reserve-your-whatsapp-username/

Analysis

Threat Multiplier, Not Threat Creator

ZeroFox assesses that the introduction of usernames on WhatsApp will likely change how threat actors represent themselves rather than how they conduct impersonation. Existing impersonation campaigns already rely on recognizable display names, copied corporate branding, profile images, and persuasive social engineering to establish trust. Usernames very likely provide threat actors with another identity attribute that can reinforce these fraudulent personas but do not materially alter the underlying techniques used to conduct impersonation. Accordingly, ZeroFox recommends that organizations treat WhatsApp usernames as an additional identity element requiring the same monitoring and validation as display names, profile pictures, and other established impersonation indicators.

Novel Opportunities for Threat Actors

ZeroFox assesses that the username feature introduces several incremental advantages for threat actors without fundamentally changing their tradecraft:

- **Namespace squatting**: Registering usernames resembling targeted organizations, subsidiaries, or senior executives before the legitimate party claims their own handle or adopting typo-variant usernames where the exact match is unavailable.
- **Cross-platform identity cloning**: Maintaining matching usernames and cloned profile pictures across WhatsApp, Telegram, Instagram, Facebook, and X to strengthen victim confidence in a coordinated fraudulent persona.
- **Region-specific scam scripts**: Digital arrest, fake bank/regulator alerts, and Know Your Customer (KYC) update lures adapted to a WhatsApp-native identity.
- **Username key social engineering**: Pretexts (such as support, verification, or “unlock messaging”) designed to get a target to hand over their own username key to a stranger.
- **Enumeration at scale**: Distributed, low-and-slow probing of Meta’s rate limits on new-contact messaging and username key guessing attempts.

Regulatory and Rollout Dynamics

India's MEITy issued a formal notice to Meta within 48 hours of the announcement, warning the feature "may materially increase the incidence of online fraud, phishing, digital arrest scams and impersonation attacks" and directed a temporary pause of the rollout in that market pending consultation.[2] Finland's Traficom issued a similar public warning in early July 2026.[3] ZeroFox assesses this regulatory pressure is likely to continue shaping rollout pace and safeguards by market and represents an independent, government-level signal that the abuse potential is likely being taken seriously rather than treated as hypothetical.

Implications for Targeted Organizations

ZeroFox assesses that the greatest risk to organizations is an increase in the effectiveness of existing impersonation campaigns rather than their frequency. Organizations with strong brands, large customer bases, or high executive visibility are already frequent targets of impersonation across social media and messaging platforms. Where official username reservation is available, organizations can reduce opportunities for impersonation while providing customers and employees with a consistent, verifiable identifier for legitimate accounts and a stable identifier to support monitoring, reporting, and takedown of impersonating accounts over time.

Assessment

Considering the independent regulatory scrutiny from India and Finland, ZeroFox assesses that the WhatsApp username feature will likely have a moderate enabling effect on the impersonation threat landscape despite Meta's stated safeguards (reserved high-profile names, absence of a public directory, an optional username key, and rate limiting). This assessment should be treated as preliminary, and ZeroFox will revisit it as messaging-by-username rolls out across additional markets and enforcement data becomes available.

Further, ZeroFox assesses that the greatest volume of abuse attempts (including namespace squatting, look-alike registrations, and enumeration probing) will very likely

[2] hXXps://techcrunch[.]com/2026/07/01/whatsapp-usernames-are-already-raising-impersonation-red-flags/
[3] hXXps://www.telecompaper[.]com/news/traficom-warns-that-new-whatsapp-username-system-could-be-abused-for-fraud--1576619

occur during the initial rollout window in each market before Meta's detection systems mature against real-world abuse patterns.

There is a roughly even chance that regulatory intervention (as seen in India) will meaningfully delay or reshape rollout in additional markets with high rates of messaging-based fraud, which would likely compress the timeline in which organizations need to secure official usernames.

Recommendations

- Reserve official WhatsApp usernames for the organization, key brands and subsidiaries, customer support functions, and senior executives ahead of namespace squatting.
- Expand brand monitoring to include WhatsApp usernames referencing the organization, its brands, subsidiaries, customer support functions, and senior executives following the complete rollout of messaging-by-username.
- Maintain an inventory of official WhatsApp usernames to allow fraud, customer support, and security teams to quickly validate reported WhatsApp contacts.
- Assess Meta's enforcement effectiveness during rollout by tracking the prevalence, persistence, and removal of impersonating usernames.
- Review customer, employee, and partner awareness messaging to reinforce that a username is a routing label, not proof of identity, and that a username key should never be shared with an unsolicited contact.
- Continue intelligence collection and reassess to monitor threat actor adoption, evolving tradecraft, and the effectiveness of Meta's controls as the feature matures.

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** **TLP:RED** with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** **TLP:AMBER** information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** **TLP:AMBER+STRICT** restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:GREEN** when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** **TLP:CLEAR** when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** **TLP:GREEN** information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** **TLP:CLEAR** information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%