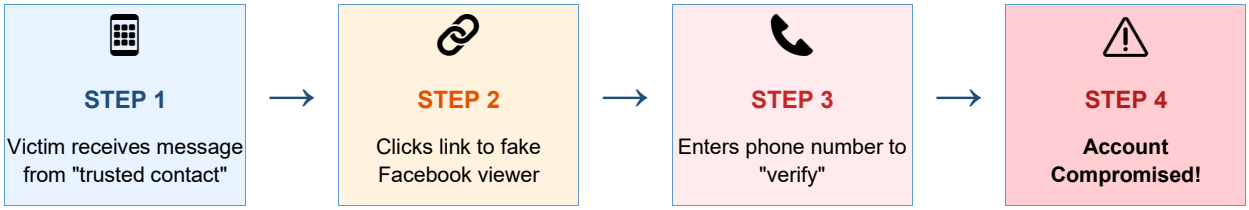
CERT-IN SECURITY ADVISORY: WHATSAPP ACCOUNT TAKEOVER GHOSTPAIRING ATTACK CAMPAIGN

Advisory No.:	CIAD-2025-0055
Issue Date:	December 19, 2025
Severity Rating:	**HIGH**
Affected Platform:	WhatsApp (All versions with device linking feature)

1. Overview

CERT-In (Indian Computer Emergency Response Team) has issued a high-severity advisory regarding a newly identified cyber campaign called "GhostPairing" that enables cybercriminals to take complete control of WhatsApp accounts without requiring passwords or SIM swaps. This advisory is critical for all individuals and organizations using WhatsApp for personal and business communication.

2. Attack Flow Diagram



3. Description (As per CERT-In Advisory)

It has been reported that malicious actors are exploiting WhatsApp's device-linking feature to hijack accounts using pairing codes without authentication requirement. This newly identified cyber campaign, called GhostPairing, enables cybercriminals to take complete control of WhatsApp accounts without needing passwords or SIM swaps.

The campaign usually begins with victims receiving a message, such as "Hi, check this photo", from a trusted contact. The message contains a link with a Facebook-style preview. The link leads to a fake Facebook viewer that prompts users to "verify" to see the content. Here the attackers exploit WhatsApp's "link device via phone number" feature by tricking unsuspecting users to enter their phone number.

By following a short, seemingly harmless sequence of steps, victims unknowingly grant attackers full access to their WhatsApp accounts, without any password theft or SIM swapping. In a nutshell, the GhostPairing attack tricks users into granting an attacker's browser access, as an additional trusted and hidden device, by using a pairing code that looks authentic.

4. Impact of Compromise (As per CERT-In)

Once the attacker links their device, they get almost the same access you would on WhatsApp Web:

1	They can read messages that sync to their device
2	They receive new messages in real time
3	They can view photos, videos, and voice notes
4	They can send messages as you
5	They can message your contacts and group chats

After taking over one account, attackers use it to send messages to the contacts of the victim, thereby spreading the attack further.

5. Recommendations for Individuals (As per CERT-In)

It is recommended to take following actions to mitigate risks associated with account compromise or takeovers:

- **Do not click suspicious links** even if they come from known contacts.
- **Never enter your phone number** on external sites claiming to be WhatsApp/Facebook.
- **Check Linked Devices regularly** in WhatsApp:
  - Open WhatsApp and go to: Settings → Linked Devices
  - If you see any device you don't recognize, log it out immediately

How to Check Linked Devices:

1	2	3	4
Open WhatsApp	**Go to Settings**	**Linked Devices**	**Review & Remove**
Launch the app on your phone	Tap ⋮ menu → Settings	Tap "Linked Devices"	Log out unknown devices

6. Recommendations for Organizations (As per CERT-In)

- **Provide security awareness training** focused on messaging-app attacks.
- **Implement policies** for official WhatsApp Business accounts requiring regular linked device audits.
- **Establish incident response procedures** for employees who suspect their accounts have been compromised.
- **Use dedicated secured devices** for official organizational WhatsApp accounts.

RELATED ADVISORY: SECURING SOCIAL MEDIA ACCOUNTS

CERT-In Advisory CIAD-2024-0006 | Issue Date: January 22, 2024

In today's interconnected world, social media plays a pivotal role in shaping public opinion and disseminating information. These platforms have become essential for individuals, governments, and enterprises alike. However, the widespread influence of social media also carries significant security risks. The security of social media accounts is paramount to prevent misuse, protect reputations, and ensure the dissemination of authentic information.

Best Practices as per CERT-In Guidelines:

1. Strong Password Policies **Implement strong passwords with regular changes and avoid reuse across platforms.**	**2. Multi-Factor Authentication** **Enable MFA for all social media accounts wherever possible.**
3. Access Control **Limit access to official accounts to designated officials and systems only.**	**4. Dedicated Secure Devices** Use dedicated devices with enhanced security for managing official accounts.
5. Dedicated Email Accounts **Use separate email accounts for official social media with distinct credentials.**	**6. Avoid Personal Email** Never use personal email accounts for managing official social media accounts.
7. Single Active Session **Ensure only one session is active; terminate other sessions regularly.**	**8. Content Approval** Ensure content is pre-approved by appropriate authority before posting.
9. Controlled Tool Access **Ensure controlled and secured access to social media management tools.**	**10. Avoid Public Devices** Do not use public or unauthorized devices to access official accounts.
11. Disable Geolocation **Turn off GPS access for social media platforms to prevent location tracking.**	**12. Software Updates** Regularly update social media apps and devices with latest security patches.
13. Access Revocation **Promptly revoke access when employee roles change or they leave.**	**14. Monitor Email Accounts** Regularly check linked email accounts for unusual activity alerts.
15. Login Alerts **Activate alerts for unrecognized login attempts in security settings.**	**16. Third-Party App Caution** Exercise caution with third-party applications for social media management.
17. Stay Informed **Keep abreast of security updates from social media companies.**	**18. Beware of Phishing** Don't click phishing links; scan systems regularly with antivirus.

References

Advisory	Details
CIAD-2025-0055	WhatsApp Account Takeover Campaign (GhostPairing) Issue Date: December 19, 2025 | Severity: High
CIAD-2024-0006	Securing Social Media Accounts Issue Date: January 22, 2024
CIAD-2024-0050	Preventing Online Scams Issue Date: October 24, 2024
CERT-In Website	https://www.cert-in.org.in/

KNOWLEDGE DESK

CISA Altamash Shaikh

CISA Shraddha Godbole

CISA Taher Pepermintwala

Disclaimer: This knowledge alert is prepared based on CERT-In advisories for informational purposes only. Organizations should assess applicability to their specific environment and consult with cybersecurity professionals for implementation guidance. For the latest advisories, please visit www.cert-in.org.in