NCA-01.011226– National CERT Advisory – Widespread WhatsApp Account Hijacking & Unauthorized Access Incidents

Introduction

The National Cyber Emergency Response Team (National CERT) of Pakistan issues this advisory highlighting the growing risk of WhatsApp account hijacking and urging users to remain vigilant against emerging cyber threats. Attackers are exploiting various social engineering techniques and technical vulnerabilities to gain unauthorized access to user accounts, enabling them to steal personal data, impersonate legitimate users to defraud their contacts, and distribute malicious content.

WhatsApp's architecture is designed such that account ownership is fundamentally tied to SIM card possession and phone number verification. This advisory outlines the attack vectors being exploited, official recovery procedures, and preventive measures to help users maintain control of their accounts.

The rising frequency of these incidents poses risks not only to individual users but also to organizations whose employees use WhatsApp for business communications, potentially exposing sensitive information and enabling business email compromise-style attacks through trusted communication channels.

Impact

Successful account hijacking may lead to:

1. **Identity Theft** – Attackers impersonate victims to their contacts, family, and colleagues.
2. **Financial Fraud** – Hijacked accounts are used to request money transfers from the victim's contact list.
3. **Data Exposure** – Access to chat history, media files, and personal/business communications.
4. **Malware Distribution** – Compromised accounts spread phishing links and malicious content to trusted contacts.
5. **Reputation Damage** – Victims suffer personal and professional credibility loss from attacker actions.
6. **Privacy Violation** – Unauthorized access to private conversations, contacts, and location data.

Threat Details

Vulnerability Overview

- **Incident ID**: WhatsApp Account Hijacking Campaign – 2026
- **Affected Platform**: WhatsApp Messenger (All versions, all platforms)
- **Attack Category**: Social Engineering, Authentication Bypass, Session Hijacking
- **Description**: Multiple attack vectors allowing unauthorized takeover of WhatsApp accounts through exploitation of user trust, call forwarding mechanisms, phishing techniques, and QR code manipulation.

Attack Complexity & Vector

- **Attack Vector**: Remote (Social Engineering)
- **Attack Complexity**: Low to Medium
- **Privileges Required**: None
- **User Interaction**: Required (victim must perform action)
- **Estimated Severity**: High
- **Likely CWE**: CWE-287 (Improper Authentication), CWE-346 (Origin Validation Error), CWE-601 (URL Redirection to Untrusted Site)

Attack Vectors

1. Social Engineering (OTP Scams)

Method: Attacker poses as a trusted contact, WhatsApp Support, or service provider and requests the victim share a 6-digit SMS verification code sent to their phone, claiming it was sent "by mistake" or is needed for "account verification."

How It Works: The attacker initiates WhatsApp registration on their device using the victim's phone number, triggering an SMS with the verification code. Once the victim shares this code, the attacker completes registration and takes over the account.

2. Call Forwarding Exploits

Method: Attackers trick users into dialing USSD codes (e.g., **21*) that enable call forwarding to the attacker's phone number.

How It Works: With call forwarding active, when WhatsApp attempts voice verification (if SMS fails), the call is redirected to the attacker, who receives the spoken verification code and completes account takeover.

3. Phishing Links

Method: Messages claiming prize winnings, account expiration warnings, or security alerts direct users to fraudulent websites mimicking WhatsApp login pages.

How It Works: Victims enter credentials or verification codes on fake pages, which are captured by attackers and used to access the legitimate WhatsApp account.

4. QR Code Scams ("Quishing")

Method: Attackers send QR codes claiming to offer "WhatsApp Web login," "desktop version access," or "account verification."

How It Works: Scanning the malicious QR code links the victim's WhatsApp account to the attacker's WhatsApp Web/Desktop session, granting real-time access to all conversations and contacts.

Indicators of Compromise (IoCs)

Category	Indicator / Value	Description / Notes	Action Required
Unexpected Logouts	User is suddenly logged out of WhatsApp	Account may have been registered on another device	Immediately attempt re-registration
Unrecognized Messages	Contacts report receiving suspicious messages from your account	Account is compromised and being used for fraud	Alert contacts and begin recovery
Linked Device Notifications	Unknown devices appear in Linked Devices list	Unauthorized WhatsApp Web/Desktop sessions	Log out all devices immediately
Two-Step Verification Changes	Unsolicited 2FA PIN prompt or email notifications	Attacker may be attempting to lock you out	Verify you control recovery email
Call Forwarding Active	Calls not reaching your phone	May indicate call forwarding exploit	Dial ##21# to disable call forwarding
Verification Code Requests	Receiving SMS/voice codes without initiating login	Someone attempting to register your number	Do not share codes; report to contacts

Exploit Conditions

Successful hijacking requires:

- **Victim's phone number** – Known to or guessed by attacker
- **User interaction** – Victim must share OTP, scan QR code, click phishing link, or dial forwarding code
- **Lack of Two-Step Verification** – Accounts without 2FA PIN are more vulnerable
- **Social engineering success** – Victim must trust the attacker's pretext

The attacks are confirmed active and widespread, with ordinary users across all demographics being targeted.

Affected Platforms

- **WhatsApp for Android** – All versions
- **WhatsApp for iOS** – All versions
- **WhatsApp Business** – All versions
- **WhatsApp Web** – All versions
- **WhatsApp Desktop** – All versions

***Note**: The vulnerability lies not in software flaws but in social engineering exploitation of legitimate authentication mechanisms and user behavior.*

Official Recovery Procedure

If your WhatsApp account has been hijacked, follow this linear recovery flow:

Step	Action	Why It Works	Expected Outcome
1. Reinstall	Delete and reinstall WhatsApp on your phone	Clears corrupted cache and session data	Clean application state
2. Verify	Enter your phone number and request SMS code	Proves ownership via SIM card possession	6-digit code sent to your phone
3. Displace	Enter the SMS verification code	**Critical**: Immediately logs attacker out of all devices	You regain primary account control
4. Handle 2FA	If prompted for unknown PIN, select "Forgot PIN?"	Initiates PIN reset process	Proceed to step 5
5. Wait Period	Wait 7 days if hacker enabled 2FA without recovery email	Account is locked; neither party can access messages	Data remains secure during lockout
6. Complete Recovery	After 7 days (or email reset), set new 2FA PIN	Full account access restored	Account secured under your control

Critical Note on the 7-Day Wait Period

If the attacker enabled Two-Step Verification and you don't have a recovery email linked:

- **Lockout Duration**: 7 days mandatory wait
- **Security Benefit**: Neither you nor the attacker can read messages during this period
- **Data Protection**: Your chat history remains secure; the attacker cannot access it after Step 3
- **After 7 Days**: You can set a new PIN and regain full access

If you have a recovery email: The 7-day wait is bypassed, and you can reset the PIN immediately via email link.

Recommendations & Mitigation Actions

1. Enable Two-Step Verification with Recovery Email (Critical)

Two-Step Verification adds a 6-digit PIN that must be entered periodically and when re-registering your account on a new device.

Setup Instructions:

For Android:

1. Tap the three dots (⋮) in the top right → **Settings**
2. Tap **Account** → **Two-step verification**
3. Tap **Turn on**
4. Create a memorable 6-digit PIN
5. **Add your email address** (do not skip)
6. Confirm your email address

For iOS (iPhone):

1. Tap **Settings** in the bottom right corner
2. Tap **Account** → **Two-step verification**
3. Tap **Enable**
4. Create a memorable 6-digit PIN
5. **Add your email address** (do not skip)
6. Confirm your email address

Why the Recovery Email is Essential:

- Allows immediate PIN reset if you forget it or if an attacker changes it
- Bypasses the 7-day lockout period
- Acts as your "master key" to account recovery
- Provides notifications of suspicious 2FA changes

2. Regularly Check Linked Devices

Monitor and control which devices have access to your WhatsApp:

1. Open **Settings** → **Linked Devices**
2. Review all active sessions
3. Log out any unrecognized devices
4. Check this list weekly

3. Security Best Practices

Never share:

- 6-digit SMS verification codes
- Two-Step Verification PIN
- Any codes received via SMS or voice call

Legitimate entities will never:

- Ask for verification codes via chat or call
- Request your 2FA PIN for "account verification"
- Send unsolicited QR codes for scanning

Additional protections:

- Verify call forwarding status by dialing *#21#
- Disable call forwarding with ##21#
- Be suspicious of urgent requests for codes or money
- Verify unusual requests through alternative contact methods
- Do not click links in unsolicited messages
- Only scan QR codes from your own WhatsApp Web settings

4. Organizational Measures

For businesses and organizations:

- Educate employees about WhatsApp hijacking tactics
- Implement verification procedures for financial requests
- Establish out-of-band confirmation for sensitive communications
- Consider deploying WhatsApp Business API for authenticated business accounts
- Monitor for suspicious activity patterns
- Maintain incident response procedures for compromised accounts

Monitoring & Detection

User-Level Monitoring

- Regularly review **Linked Devices** for unauthorized sessions
- Monitor for unexpected logouts or verification code requests
- Check that your profile photo and status haven't been changed
- Verify Two-Step Verification status remains enabled
- Confirm recovery email is current and accessible

Organizational Monitoring

- Establish employee reporting channels for suspected compromise
- Monitor for unusual message patterns from employee accounts
- Track reports from external contacts about suspicious messages
- Maintain awareness of current phishing campaigns
- Educate staff on emerging attack techniques

Response Actions

If You Suspect Your Account is Compromised:

1. **Immediate**: Follow the Official Recovery Procedure above
2. **Alert Contacts**: Warn family, friends, and colleagues not to respond to messages or send money
3. **Document**: Take screenshots of any suspicious activity
4. **Report**: Contact WhatsApp Support through the app
5. **Monitor**: Watch for unauthorized financial transactions or data breaches
6. **Secure**: Enable 2FA with recovery email after regaining access

If Someone You Know is Compromised:

1. **Do not** send money or share sensitive information
2. **Verify** through alternative communication channels (phone call, in person)
3. **Alert** the account owner through other means
4. **Report** the compromised account to WhatsApp
5. **Warn** other mutual contacts

Prevention Summary

Security Measure	Implementation	Status Priority
Two-Step Verification + Email	Enable in Settings → Account	**Critical - Implement Immediately**
Linked Device Audit	Review weekly in Settings	**High - Ongoing Monitoring**
Never Share Codes	User education and awareness	**Critical - Continuous Practice**
Call Forwarding Check	Dial *#21# periodically	**Medium - Monthly Verification**
Phishing Awareness	Training and vigilance	**High - Continuous Education**

Call to Action

The National CERT urges all WhatsApp users to:

- **Immediately enable Two-Step Verification with a recovery email** on all WhatsApp accounts
- **Educate family members and colleagues** about these attack vectors, especially vulnerable populations

- **Review Linked Devices** and log out unrecognized sessions
- **Never share verification codes** regardless of who requests them
- **Report suspicious activity** to WhatsApp and warn contacts if compromised
- **Implement organizational security policies** for employees using WhatsApp for business communications

Remember: **Your SIM card is your ultimate key to account ownership.** With physical possession of your phone and SIM, you can always recover your WhatsApp account by following the official recovery procedure. Prompt action and preventive measures are essential to maintain control of your WhatsApp account and protect your personal communications, contacts, and identity from exploitation by malicious actors.

References

1. **WhatsApp Security Information:** https://www.whatsapp.com/security
2. **WhatsApp Help Center – Two-Step Verification**: https://faq.whatsapp.com/1102765226893199
3. **WhatsApp Help Center – Account Theft**: https://faq.whatsapp.com/791574618752508