A Quarterly insight to Cyber Law!

Cyber Niyam means rules of the Cyberspace. This quarterly newsletter aims to create awareness about the rules and regulations of cyberspace, cyber security and data protection. This is also an effort to create awareness about digital safety, trending cybercrimes and effective reporting mechanisms.

Disclaimer

This newsletter does not intend to advertise or solicit work and is for private circulation only. This newsletter is for the purpose of education and creating awareness on Cyber law and its latest developments. It does not intend to be comprehensive nor intends to provide any legal advice. Though every effort is made to share accurate, reliable and current information, Cyber Niyam is not responsible for any errors or omissions in information made available through this Newsletter. Sharing of this Newsletter does not intend to create attorney – client relationship between authors and reader.

By Adv. Vaishali Bhagwat *www.vaishalibhagwat.com*

Issue 4 of 2026 – October, 2026

In this Issue

- **A Deep Dive into Trust-Based Mobile Scams**
  1. *Ghost Pairing*
  2. *Finance Team Malware*
  3. *Call Forwarding Scams*
- **Key Case Studies**
- **Safety and Hygiene Guidelines**
- **Good to know**
  1. *SEBI warns against "Boss Scam"*
  2. *CERT-In warns against fake e-Challan*
  3. *India signs UN Convention Against Cybercrime*
- **News Corner**
  1. *Banks Warn of AI Shopping Risks*
  2. *Indian Engineers Hack OpenAI Using Claude*
- **Glossary of terms –**
  - *Ghost Pairing*
  - *APK*
  - *USSD*
  - *WhatsApp Web*
  - *Call Forwarding*
  - *1930*
  - *NCRP*
  - *Shopping Bot*

A DEEP DIVE INTO TRUST-BASED MOBILE SCAMS HIGHJACKING INDIAN MOBILE PHONES

Introduction

Recently attackers have advanced beyond phone hacking, with hijacked WhatsApp accounts, self-spreading malware, and rerouted OTPs. They are now encouraging customers to open the door themselves. You could receive a message from a colleague, a friend, or someone you already have stored on your phone, such as "Hi, check out this photo" or a link to "XYZ on Instagram". There is no suspect sender, no misspelled name, and no threat. The absence of any such warning flags is precisely why frauds have become so difficult to spot.

Over the past year, Indian authorities and security researchers have issued multiple warnings about cyber-attacks that all lean into the same weakness: our willingness to trust a familiar name. Each attacker abuses some features that is supposed to be helpful, WhatsApps's device-linking feature, the ability to forward files or a phone network's call- forwarding function. This newsletter looks into three of the most significant **cyber scams** in recent times, how they work and what connects them.

.....Continued on page 2

Three Scams To Watch Out For:

A. *GHOST PAIRING: HIJACK WITHOUT ANY PASSWORD*

- In December 2025, India's national cyber agency CERT-In published an advisory naming a campaign called "GhostPairing" with a high severity rating.
- **Ghost Pairing didn't start in India.** Security firm Gen Digital first spotted it in Czechia on December 18th, a day before India's advisory and warned it could spread globally via compromised accounts, using fake Facebook pages and legitimate WhatsApp features to pull off the attack.
- The advisory describes a chain of events that starts ordinary. The victim received a message such as "Hi, check out this Photo" from a contact they trust. It carries a Link with a Facebook-style preview. Tapping it leads to a fake Facebook page that asks the user to "verify" before the content can be viewed.
- That verification step is the trap. It exploits WhatsApp's feature of device linking using a phone number, and the victim is tricked into entering their phone number so that their account gets linked. Thus the victim unknowingly authorises the attacker's browser as an additional, hidden device on their own account, using a pairing code that looks authentic.

Why such Scam is hard to track

Unlike typical account takeovers, which trigger a logout, password reset alert, or dead SIM, GhostPairing leaves no trace. The phone works normally while the attacker's linked device silently accesses messages, photos, and OTPs in real time. Worse, the attacker can message the victim's contacts posing as them, turning each hijacked account into bait for the next.

Recent Global Developments

Variations of this scam have surfaced globally through 2026:

- **March 2026:** Singapore Police reported scammers claiming a code was sent "by mistake" and asking victims to share it, logging them out of WhatsApp and repeating the scam with their contacts.
- **May 2026:** Switzerland's National Cyber Security Centre warned about a similar "Vote for your Child" scam that tricked victims into sharing their WhatsApp six-digit registration code, and urged users to enable two-factor authentication.
- **August 2026:** Malwarebytes reported a "vote for my friend/child" scam where victims are asked to scan a QR code or enter a code to "vote", which actually links the attacker's device to the victim's WhatsApp.

Case Study: Hong Kong, June 2026

Hong Kong Police reported more than 100 WhatsApp account- hijacking scams in a single week in early June 2026, with losses totalling above HK$ 18 million. In one case a 62-year old women received a WhatsApp message from someone posing as her daughter, who urgently needed money to buy stocks with friends. She transferred the money to the account provided and lost HK $ 400,000.

The reports show that once a scammer controls a trusted identity, the money transfer is easy. Police advised people to stop replying in the chat and Phone the person on a number they already know.

The takeaway: Ghost Pairing shows how a simple request to verify or enter a code can give an attacker access to a WhatsApp account without the victim realising it.

GOOD TO KNOW!

1. **SEBI has warned about "Boss Scams", where fraudsters impersonate CEOs or senior officials through WhatsApp, email or AI-generated calls/videos and instruct employees to transfer money. In some cases, malicious files are used to hijack WhatsApp Web and send payment instructions to other employees.**
   SEBI advises employees to verify such requests by directly calling the senior concerned and never transfer money solely on social media instructions.

2. **Received an e-Challan APK on WhatsApp or SMS? Don't install it.**
   CERT-In has warned about fake e-Challan messages that use malicious APK files to infect user's devices. Always verify challans through the officials e-Challan portal or your state traffic police websites/app

3. **India has signed the UN Convention against Cybercrime, strengthening international cooperation to tackle cybercrime and share electronic evidence across borders. The Convention is the first comprehensive global treaty on cybercrime.**

B. *MALWARE CAMPAIGN TARGETING FINANCE TEAMS*

In September 2026, Quick Heal Technologies warned of an ongoing WhatsApp-based malware campaign targeting finance teams, executives, and Chartered Accountants. Attackers compromise a WhatsApp account, then send malicious files, disguised as "Financial Report," "Account Statement," or "Debt Confirmation," sometimes imitating RBI or MCA communications, to the victim's contacts, who trust the source and open them.

The campaign has evolved from VBS files to ZIP archives and disk-image (.IMG/.VHD) files, making it harder to catch with one security rule. Using an active WhatsApp Web session, the malware can self-forward to contacts, turning one infection into a chain reaction across Windows-based offices.

Case study — The ₹1.5 Crore "Boss Scam" (Ahmedabad, June 2026):

After scammers posed as RBI officials to a businessman, his accountant received WhatsApp messages using the boss's name and photo, instructing an urgent ₹1.5 crore transfer to a Kolkata company. Believing it genuine, he paid. Police found the scammers had compromised the executive's WhatsApp Web session using malware, and uncovered a wider network supplying SIMs and OTPs to fraud call centres.

The pattern is national: I4C's June 2026 advisory on "Boss Scams" cited a Delhi garment company that lost ₹7.8 crore across four transfers to a fake owner, and a Lucknow businessman who lost ₹18 lakh after his accountant received a malware-laced message impersonating his son.

Police advised companies to avoid unknown ZIP, EXE and DLL files, regularly check WhatsApp linked devices, and verify payment requests directly with senior officials.

The takeaway: A familiar name or profile picture does not prove that a message is genuine. Always verify urgent payment requests through another channel.

C. *THE CALL FORWARDING SCAM*

In December 2025, India's Cybercrime Threat Analytics Unit (I4C) flagged a rise in USSD-based call forwarding scams. Fraudsters pose as courier agents claiming a parcel needs confirmation, and ask victims to dial a code starting with **21** followed by the scammer's number. This silently activates unconditional call forwarding, diverting bank verification calls, OTPs, and WhatsApp/Telegram authentication calls straight to the scammer. Some also impersonate telecom customer service citing fake SIM issues.
This isn't new: DoT suspended USSD-based call forwarding in April 2024 after similar OTP theft reports, but the scam has resurfaced.

What to do: Dial **##002#** to cancel all call forwarding. Never dial codes shared by unsolicited callers, and verify deliveries only through official courier apps or numbers. Report fraud on **1930** or cybercrime.gov.in.

Case study (Bengaluru, 2025): Actor Priyanka Upendra received a fake delivery call asking her to dial a code "to receive an OTP." She lost access to her WhatsApp account, and scammers used it to solicit ₹55,000 each from her son and two friends, totalling ₹1.65 lakh. Police later traced the racket to a 100+ person operation based in Nalanda.

Takeaway: Never dial a code asked by an unknown caller. It could forward your calls and OTPs to a scammer.

While these scams use different methods, they all have one thing in common: **your phone is at the centre of the attack.** Whether it is linking a WhatsApp account, opening a malicious file or forwarding calls, scammers can exploit your phone to gain access to your accounts, information and money.

CYBER SAFETY

IS YOUR PHONE COMPROMISED?

Not every unusual phone behaviour means that your phone has been hacked. However, some warning signs should not be ignored, especially after clicking an unknown link or installing an unfamiliar app.

Warning signs to look out for:

- **Unknown apps:** An app appears that you do not remember installing.
- **Unusual permissions:** An unfamiliar app has access to SMS, calls, contacts or notifications.
- **Unusual battery or data usage:** Your phone suddenly uses much more battery or mobile data.
- **Strange account activity:** Messages are sent from your WhatsApp account without your knowledge.
- **Unfamiliar transactions:** You notice payments or banking activity that you do not recognise.

A compromised phone may not always show obvious signs, as some malware can operate quietly in the background

WHAT TO DO IF YOUR PHONE IS COMPROMISED?

If you think you have installed a suspicious app, act quickly.

1. **Disconnect from the internet**: Turn off mobile data and wi-fi if you suspect malicious activity.
2. **Remove the suspicious app:** Check recently installed apps and uninstall anything unfamiliar.
3. **Check app permissions**: Look for unusual access to SMS, calls, contacts, notifications or accessibility features.
4. **Secure your accounts**: From a trusted device, change important passwords and check active sessions.
5. **Check your bank and UPI accounts:** Report any unfamiliar transaction to your bank immediately.
6. **Warn your contacts:** If your messaging account has been compromised, tell your contacts not to trust unusual messages or payment requests.
7. **Report the incident:** For cyber financial fraud, call **1930** and report it on the National Cyber Crime Reporting Portal.

PHONE HYGIENE: SMALL HABITS THAT CAN PREVENT BIG PROBLEMS

Cyber-security does not always require technical knowledge. A few simple habits can help prevent scams.

1. KEEP WHATSAPP SAFE

- **Check Linked Devices regularly.** Remove any device you do not recognise.
- **Do not share pairing codes or QR codes.**
- **Verify unusual messages.** If a friend suddenly asks for money, an OTP or asks you to click a link, call them directly.

2. BE CAREFUL WITH APPS AND PERMISSIONS

- Download apps from trusted app stores and avoid APK files received through WhatsApp, SMS, Telegram or unknown websites.
- Keep your phone updated and enable security features such as **Google Play Protect** where available.
- Most importantly, do not give an app permissions that it does not need.

3. PROTECT YOUR MONEY AND ACCOUNTS

- Use strong passwords and two factor authentication where available.
- Keep banking and payment apps updated.

Never share OTPs, UPI PINs or passwords.

FROM PERSONAL PHONE TO ORGANISATIONAL RISK

A compromised phone can quickly become an organisational problem. Employees often use WhatsApp and personal devices for work, allowing malicious files, links or payment scams to spread through trusted contacts.

Employees should:
- Verify unexpected documents, payment requests and messages from senior employees.
- Avoid unknown APKs and links.
- Never share OTPs or login details.
- Report suspicious activity immediately.

Organisations should:
- Train employees to identify phishing and impersonation scams.
- Keep devices and software updated.
- Limit access to sensitive information.
- Independently verify unusual payment requests.
- Have a clear process for reporting compromised accounts or devices.

One compromised account can become an organisational problem when trust allows the message to spread

A compromised personal device does not always remain a personal issue. When employees use their phones and messaging accounts for work, a single compromised account can expose business communications, sensitive information and other employees to further attacks. Individual awareness and organisational safeguards therefore need to work together. Prompt reporting, verification of unusual requests and basic security practices can help contain an incident before it spreads across the organisation.

GLOSSARY OF TERMS

GhostPairing: A WhatsApp account hijacking technique where an attacker links their device to the victim's account.

APK: The installation file format used for Android applications.

USSD: A mobile network service accessed through codes dialled on a phone.

WhatsApp Web: A service that allows WhatsApp to be used through a computer browser.

Call Forwarding: A phone feature that redirects incoming calls to another number.

1930: India's National Cyber Crime Helpline for reporting cyber financial fraud.

NCRP: National Cyber Crime Reporting Portal, the Government of India's online platform for reporting cybercrime.

Shopping Bot (AI Shopping Agent): An AI tool that acts as a personal shopping assistant to search for products, compare prices, and complete online purchases automatically.

NEWS CORNER

1. Banks Warn of AI Shopping Risks

AI shopping bots can now search, compare and even buy products for users, but banks are warning about new risks. Banks including NatWest, Bank of America and ING say these tools could increase the risk of scams, frauds and data privacy breaches, especially when bots handle credit card details or use payment methods with fewer consumer protections. Banks are calling for stronger safeguards and regulations as AI becomes more involved in online shopping.

NEWS CORNER

2. Indian Engineers Hack OpenAI Using Claude

Three Indian cybersecurity researchers, Harsh Jaiswal, Mohan Pedhapati, and Rahul Maini, recently shook up the tech world by discovering a major security vulnerability in OpenAI's systems. Operating as ethical "white-hat" hackers under an official security bug-bounty program, the trio found a flaw in OpenAI's public forum and used rival AI model Anthropic's Claude to help write and speed up code exploits. Within just 72 hours, their AI-assisted code allowed them to safely gain access to employee accounts and an internal code repository. OpenAI quickly patched the flaw and awarded the team a $6,500 bug bounty for responsibly reporting the issue.

Industry Warning: This event serves as a stark wake-up call for global tech safety. It proves that AI tools have become a double-edged sword, a small group spending under $3,000 on basic AI subscriptions can now automate and execute complex cyberattacks that used to take large teams months to pull off.

ABOUT THE AUTHORS



Adv Vaishali Bhagwat

Vaishali Bhagwat is a practicing lawyer with 25 years of experience in civil and cyber litigation and advisory practice in Pune and Mumbai.
Vaishali has a prior degree and work experience in the field of Computer Science, a Post graduation certification in Cyber Security and Information Assurance and is a certified Privacy Lead Assessor.

She is an advisor to several companies on Cyber law and privacy compliance and advisor to various educational institutions on Protection of children from sexual offences.

She has successfully conducted several prominent cases for corporate espionage and Data theft, Data Privacy, Digital Financial Frauds, Cyber-crimes against women and children, take down orders and IP infringement in cyberspace.

Vaishali is a *TCS Chevening Scholar on "Cyber Policy and Cyber Defense" and has earned the Post Graduate certification from Cranfield University UK. She is also a Disha Alumni which is a prestigious program of the British high Commission on Innovative Leadership chaired by UK PM David Cameron and PM Manmohan Singh.*

www.vaishalibhagwat.com



Adv Kunal Gokhale
BSC. LLB (Hons.) (Business Law) Degree

Advocate Kunal Gokhale is a legal professional with nearly fourteen years of post-qualification experience. He is a graduate from the National Law University, Jodhpur and holds a BSc LLB (Hons.) (Business Laws) degree. Advocate Kunal Gokhale has significant professional experience in handling civil litigation matters with focus on commercial matters. He also provides advisory services in relation to drafting of various types of agreements and has been associated with firms such as Vaish Associates, Advocates (Delhi), Ernst & Young, India (Mumbai) and Luthra & Luthra Law Offices (Mumbai) in the past.



Mrudula Arjunwadkar
BSc., LLB, MPM

POSH Consultant
Helping organizations in end to end POSH Compliance, External member to IC, POSH trainings



Amruta Nerlikar
Associate



Mahek Momin
Legal Intern