

CENTRAL RESERVE POLICE FORCE

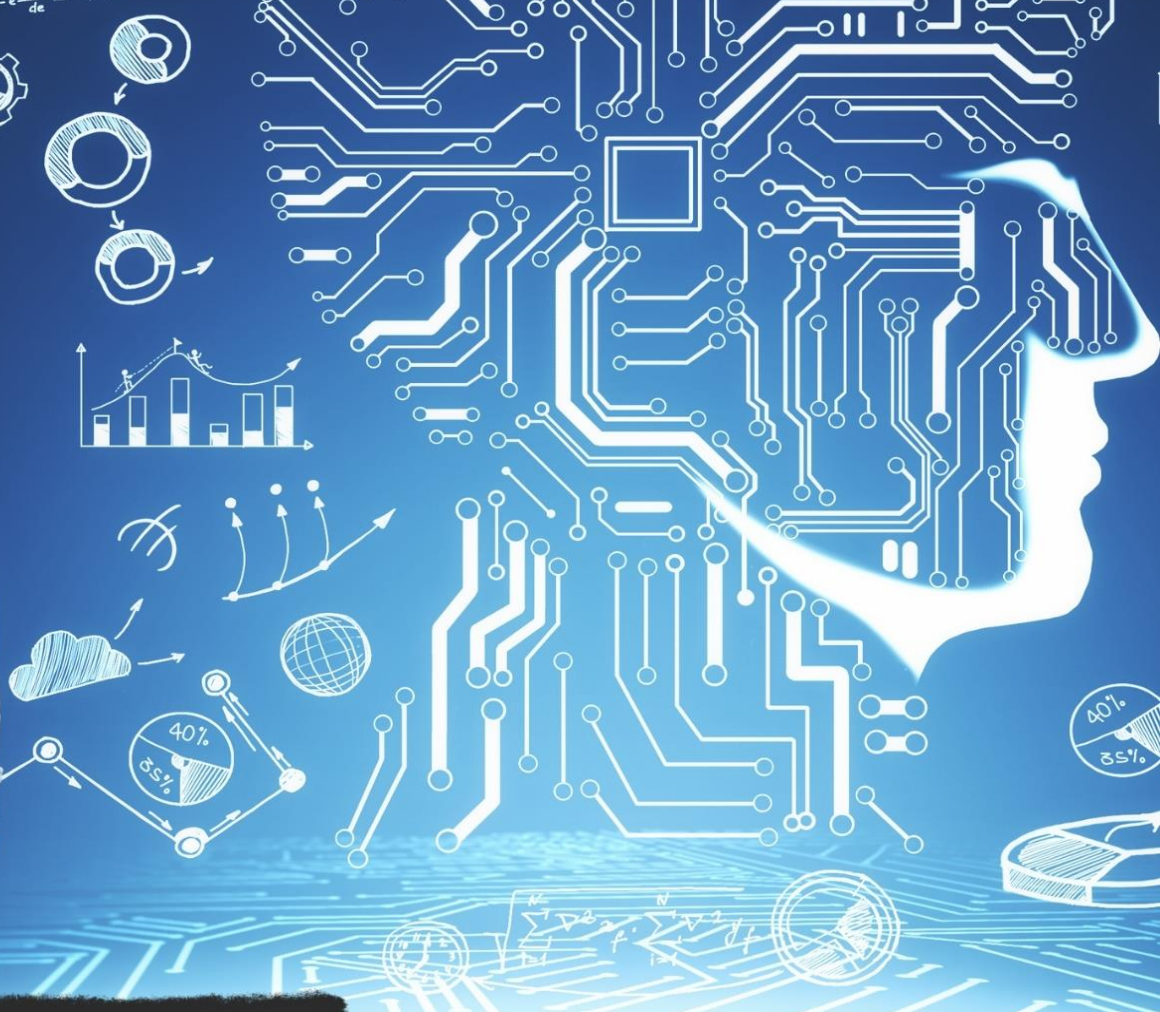
NOVEMBER-2025

CYBER BYTE

$$\tilde{G}^2(\varepsilon) = \tilde{G}^2(\varepsilon) = \frac{\sum_{i=1}^n e_i^2}{n - 2s}, (1)$$

$$\varepsilon_{ex} = \frac{dR_{ex}}{de} \frac{e}{R_{ex}}; \varepsilon_{im} = \frac{dR_{im}}{de} \frac{e}{R_{im}}$$
$$NE(e) = R_{ex}(e) - eR_{im}(e)$$

$$\Delta NE = \frac{dR_{ex}}{de} \Delta e - e \frac{dR_{im}}{de} \Delta e - eR_{im}$$



Cyber Expert Warn of APK Malware Posing as Official RTO Challans on WhatsApp

New Cyber Fraud Alert! Dialing 21# Or Any Other Code Can Cost- Stop, Don't Dial

1. CYBER GEEKS NEWS

(A) RBI Mandates Banks to Adopt '.bank.in' Domain by October 2025 for Safer Online Banking: -

The Reserve Bank of India (RBI) has directed all banks in the country to migrate their official websites and internet banking portals to the new **“.bank.in”** domain by **October 31, 2025**, in a major step toward strengthening cybersecurity in digital banking. The move aims to protect customers from phishing attacks, fake websites, and online frauds by ensuring that only verified and authorized banks operate under this exclusive domain.



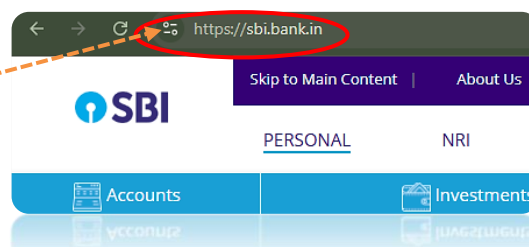
Previously, banks used more generic domains like **.com**, **.in**, or **.co.in**, which made it easier for fraudsters to create look-alike sites. The exclusive **.bank.in** domain provides a clearer signal of authenticity. The new **“.bank.in”** domain will be managed and monitored by the **Institute for Development and Research in Banking Technology (IDRBT)**. Several banks, including Punjab National Bank and State Bank of India, have already begun the transition. Customers are advised to check that their bank’s website ends with **“.bank.in”** before logging in, to ensure a safe and secure online banking experience.

For example, instead of visiting <https://www.onlinesbi.sbi.in/> you will now go to <https://onlinesbi.sbi.bank.in/>. This new domain will only be given to verified banks, so customers can easily know they are on the real website.



✚ Before entering login details, ensure the website ends with **.bank.in** (e.g., <https://sbi.bank.in>).

✚ Ensure the site starts with ~~https://~~ and displays a generic **“tune” icon** in the browser address bar.



✚ Bookmark your bank’s new official site once it’s live and use that instead of clicking links.

✚ Fraudsters often **send fake links that look like bank messages**. Type the URL manually or use the official app

(B) Delhi top cop issues norms on handling e-FIRs in cybercrime incidents : -

The Delhi Police has started a new system that allows **automatic registration of e-FIRs for cybercrime cases**, especially those involving financial fraud. Earlier, people had to visit a police station to file a complaint, which often caused delays. Now, if someone reports a cyber fraud (like an online scam or fake investment) through the national helpline **1930** or the **National Cybercrime Reporting Portal (NCRP)**, the system will **automatically create an electronic FIR (e-FIR)** without the victim needing to visit a police station immediately.



This new setup, called the “**e-Zero FIR system**”, has been launched as a pilot project in Delhi by the **Ministry of Home Affairs (MHA)** and the **Indian Cyber Crime Coordination Centre (I4C)**. Initially, it covered only large frauds (₹10 lakh and above), but now it applies to cases involving **₹1 lakh or more**. Once an e-FIR is created, it is automatically sent to the right police unit based on the amount of money involved smaller cases go to district cyber police stations, while bigger cases are handled by specialized units like the **Crime Branch** or **IFSO (Intelligence Fusion & Strategic Operations)**.



- ❖ ₹1-25 lakh → District Cybercrime PS
- ❖ ₹25-50 lakh → Crime Branch Cyber Cell
- ❖ Above ₹50 lakh → Special Cell's IFSO (Intelligence Fusion & Strategic Ops) unit

The main aim of this system is to **save time and help victims faster**. Cybercrimes usually require quick action, like freezing bank accounts or tracing digital transactions. With automatic e-FIR registration, the police can start investigating immediately instead of waiting for paperwork. Victims still need to visit the police station within **72 hours** to sign the complaint and provide supporting documents.



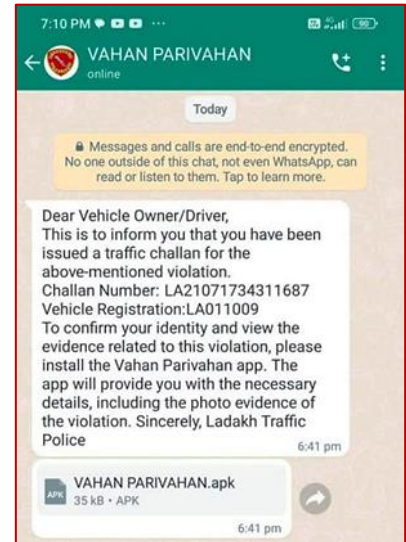
- ✚ Use official channels only, Call the cybercrime helpline 1930 or visit the official portal cybercrime.gov.in. Never share your case details on social media or unofficial websites.
- ✚ If you ever fall victim to a cybercrime, the first thing to remember is to act quickly. The quicker you complain, the higher the chance police can freeze the fraudster's account and recover your money.
- ✚ Make sure to save all evidence, such as screenshots of messages, payment details, and phone numbers used by the scammer, as these will help the police trace the fraud.
- ✚ Once your e-FIR is created, visit your nearest police station within 72 hours to sign and confirm your complaint.

2. CYBER FRAUDS

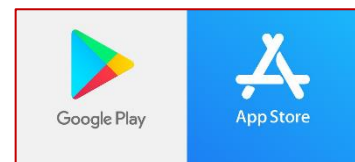
(A) Cyber Expert Warn of APK Malware Posing as Official RTO Challans on WhatsApp: -

A new scam is spreading through WhatsApp messages, tricking people into downloading a fake “RTO e-Challan” app. The message often comes from someone you know, which makes it seem safe. It includes a file named “RTO VAHAN PARIVAHAN.apk” claiming to show a traffic fine. **But once the app is installed, it secretly gives hackers access to your phone.** Several people have already lost access to their WhatsApp accounts, and some even had money stolen from their bank accounts.

Cyber Expert say this is a new kind of cyberattack, instead of sending suspicious links or emails, criminals are now using trusted contacts to spread malware. The fake app can read messages, steal personal data, and even spy on financial information. Authorities are warning people not to install any app shared on WhatsApp, especially if it comes as an **.apk file** instead of from the official Play Store.



- ✚ Never download or install any .apk file received on WhatsApp or SMS. Apps should only be installed from the **Google Play Store** or **Apple App Store**.



- ✚ The RTO or traffic police **never send challans through WhatsApp**. Verify any pending fines only on **echallan.parivahan.gov.in** or the official **mParivahan app**.



- ✚ Turn off the “Install unknown apps” option in your phone settings, keep your phone’s software and apps updated.
- ✚ **If you already installed it, disconnect your phone from the internet immediately, Uninstall the suspicious app and Change your online banking passwords and UPI PINs.**

(B) New Cyber Fraud Alert! Dialing 21# Or Any Other Code Can Cost- Stop, Don't Dial: -

Cyber police have warned people about a new and dangerous type of cyber fraud. In this scam, fraudsters trick people into dialing certain mobile codes like **21#** on their phones. The scammers usually pretend to be officials from banks, mobile companies, or government agencies. They call victims and give false reasons — such as verifying a SIM card, improving network service, or fixing an issue — and then convince them to dial the code.

***21*MobileNumber#
(For Call Forwarding)**

Once the victim does this, **all their incoming calls and text messages get forwarded to the fraudster's number.** This

***#21#
(To Check Call Forwarding on a Phone)**

means the scammer starts receiving all OTPs, bank alerts, and verification codes that are meant for the victim. With this access, they can easily hack into the victim's bank accounts, WhatsApp, or social media, and even use the victim's identity to cheat their friends and relatives.

The experts said that this is a **very risky fraud pattern and even one small mistake can expose a person's entire digital life.** They have advised everyone not to dial any unknown codes or follow instructions from callers claiming to be from banks or government offices. If anyone has already dialed such a

**#21#
(To Deactivate Call Forwarding)**

code, they should **contact their mobile operator immediately** to stop call forwarding, **change their passwords**, and **report the incident** to the nearest cybercrime police station or through the official website <https://cybercrime.gov.in>. The police have also stressed that as scammers keep changing their methods, **public awareness is the best protection** against such frauds.



Use full codes

***#06#** To check IMEI number

***#67#** To check all forwarding services

#002# To de activate all forwarding services



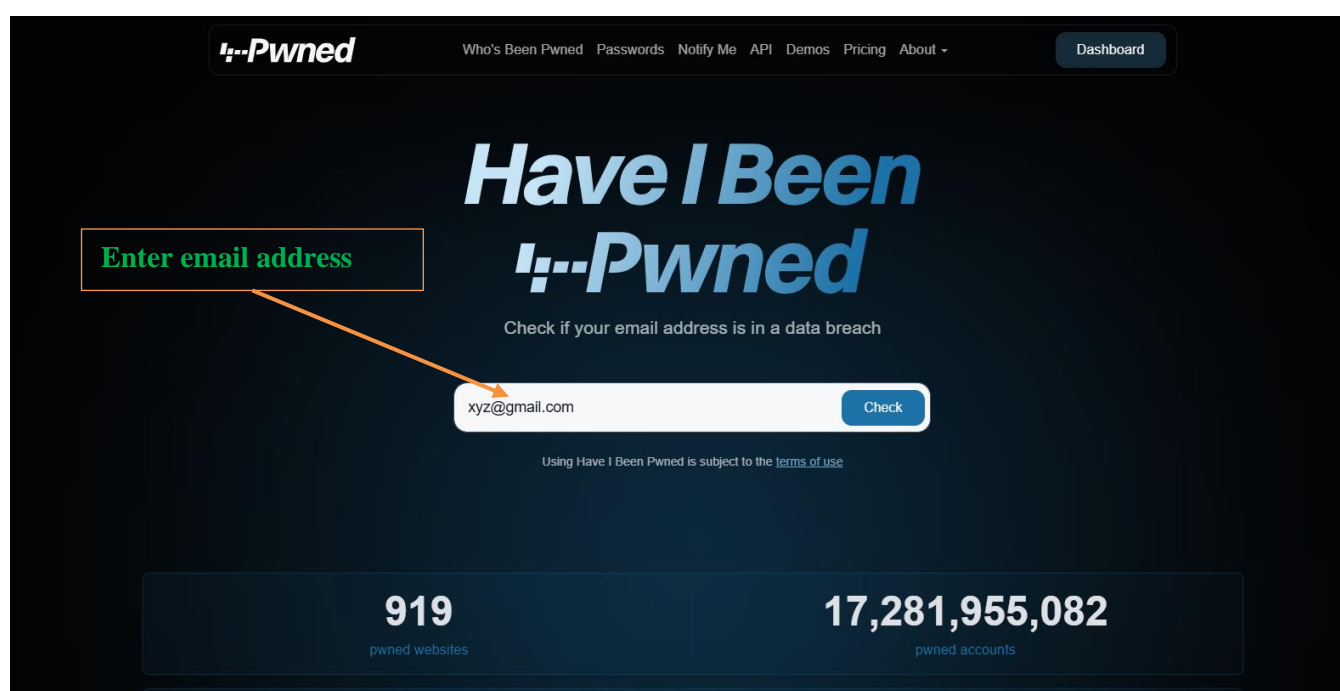
- +** **Never dial** unknown codes like *21*, *401* or any code given by a stranger.
- +** Do not share OTPs, PINs, or passwords with anyone, not even someone claiming to be from your bank or a government agency.
- +** Check your phone's call-forwarding settings regularly and turn off any unknown numbers.
- +** Enable two-factor authentication (2FA) for all important accounts like email, social media, and banking apps.
- +** Never share your SIM card or phone with anyone, **even for a short time.**

3. TIPS OF THE MONTH

(A) Have I Been Pwned: A Free Tool to Check for Online Data Breaches : -

Have I Been Pwned is a free and easy-to-use website that helps you find out if your personal information, like your **email ID, password, or phone number** has been **leaked in a data breach**. In simple words, when a website or online service gets hacked, hackers sometimes steal users' login details and sell or share them on the internet. This website lets you **check if your data is part of any such leak**.

You just need to visit <https://haveibeenpwned.com> and type your email address or phone number in the search box. The site will instantly tell you whether your information has appeared in any known data breaches and from which websites.



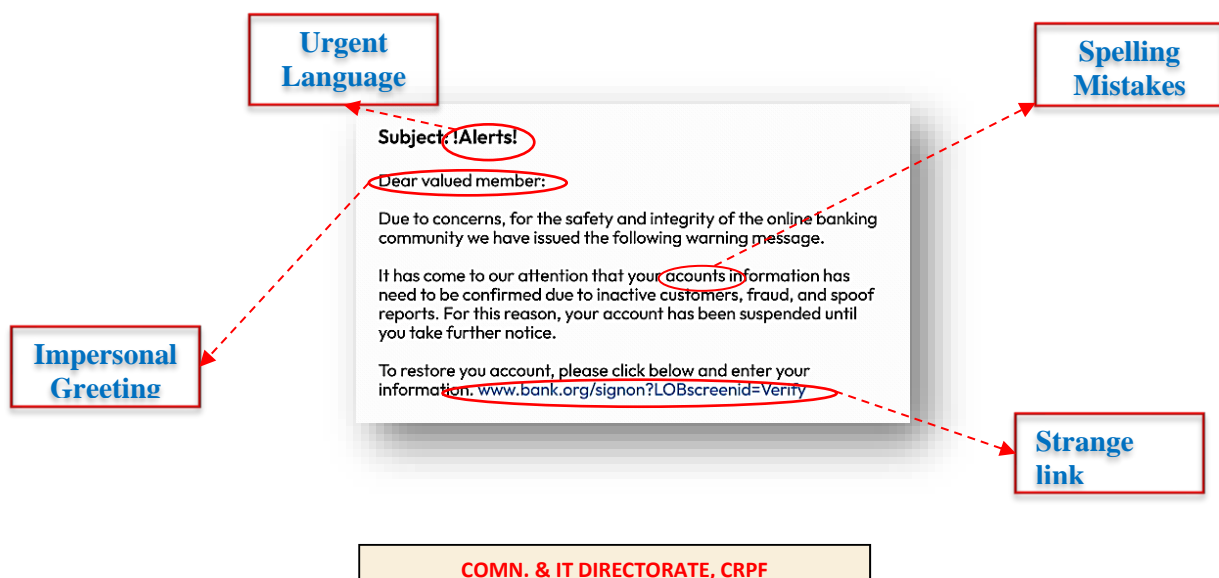
- ✚ When using **Have I Been Pwned**, always visit the **official website** haveibeenpwned.com. There are fake copies online, so double-check the address before entering your details.
- ✚ Never share your passwords there, this site only needs your **email ID or phone number** to check if your information has been leaked in any data breach.
- ✚ If the website shows that your data has been leaked (Pwned), **change your passwords immediately** on the affected accounts and make sure each account has a **unique, strong password**.
- ✚ Enable **two-factor authentication (2FA)** wherever possible, so even if someone gets your password, they can't log in without your verification code.

(B) Smart Ways to Detect a Phishing Email: -

Phishing emails are fake messages that pretend to be from trusted sources like your bank, a government office, or popular websites. The goal is to trick you into sharing personal details, such as passwords, OTPs, or bank information. To spot them easily, here's what to look for -



- ✚ Check the sender's email address carefully. Phishing emails often come from fake addresses that look similar to real ones for example, **support@sbi-secure.com** instead of **support@sbi.bank.in**. Always look for spelling mistakes or extra words in the domain.
- ✚ Look for spelling or grammar errors. Genuine companies use professional language. If you notice poor grammar, awkward phrasing, or random capital letters, it's likely fake.
- ✚ Beware of urgent or scary messages. Phrases like **"Your account will be blocked!"** or **"Click now to avoid penalty!"** are common tricks to make you panic and act fast. Real organizations don't threaten customers through email.
- ✚ Always hover over links before clicking them; if the website address looks odd or unfamiliar, don't open it.
- ✚ **Never download attachments from unknown emails, they probably might contain viruses.**
- ✚ Phishing emails often start with generic greetings like **"Dear user"** or **"Dear customer"**. Real companies usually address you by your **full name**.



4. New Development in IT DTE

1.) POWER BI

- ✚ Ayushman card status report
- ✚ E-bill status report
- ✚ WARP (welfare and rehabilitation board) list of retired personnel

2.) PPMS (Paperless Process Management System)

- ✚ Appointment Correction Order (For Non-active personnel)
- ✚ Posting Order (Updation)
- ✚ Recovery Order NGO (Updation)





Celebrating 150 years of composure of the National Song VandeMataram was sung by personnel of CRPF across all units, offices and institutions including the Force HQ in New Delhi.



Release of the SANIDHYA Book



CRPF school Annual function.



MoU with PNB bank.