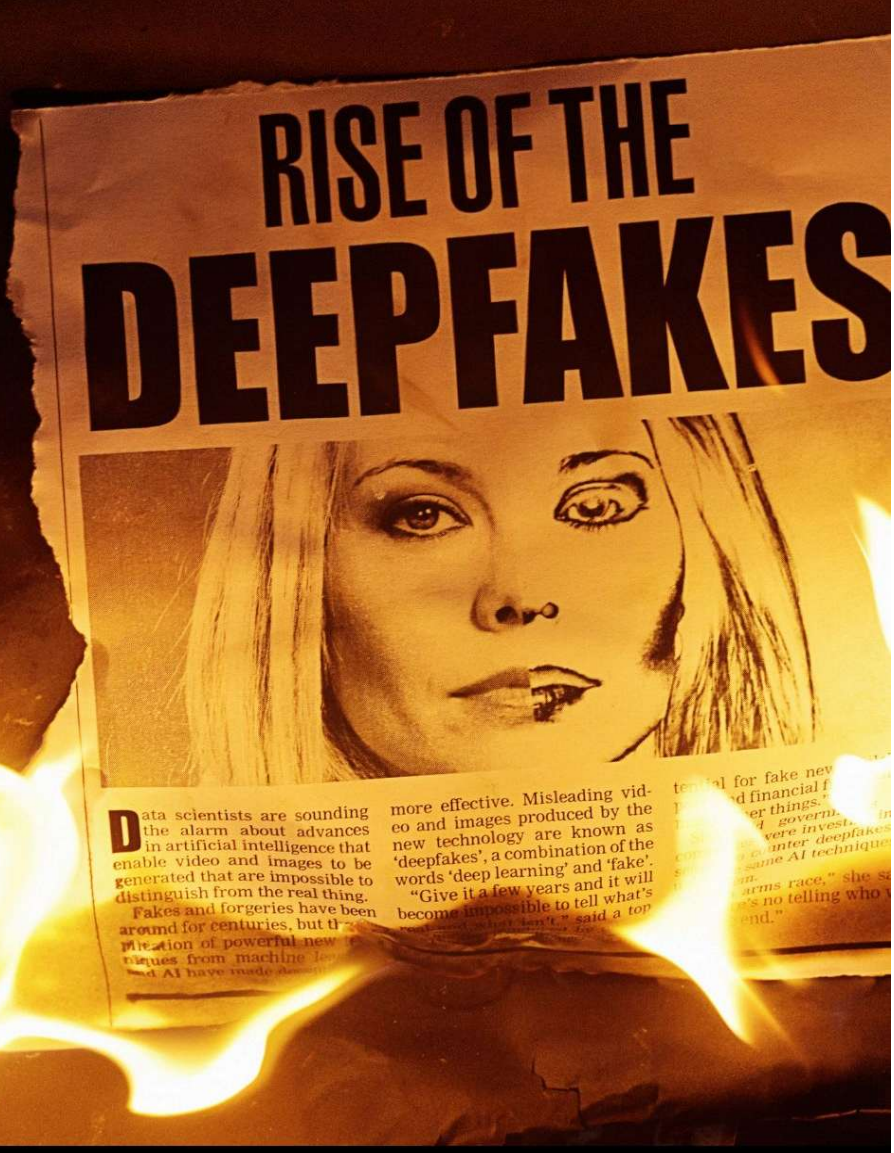
CENTRAL RESERVE POLICE FORCE

JULY, 2026

CYBER BYTE

AI-DRIVEN AND DEEPFAKE PHISHING:

A Growing National Security Threat



Fake profiles, marriage promises: Government warns of rising matrimonial fraud

(COMN & IT) DTE. CRPF

1. LATEST CYBER THREAT

1. AI-Driven & Deepfake Phishing: A Growing National Security Threat

AI-driven and deepfake phishing is an advanced form of social engineering in which cybercriminals use artificial intelligence to create highly convincing emails, messages, voice calls, or videos that impersonate trusted individuals such as senior officials, commanders, or executives. The objective is to deceive victims into sharing sensitive information, approving financial transactions, or granting unauthorized access to secure systems.

How the Scam Operates

Attackers collect information from public sources and use AI to generate personalized phishing messages or clone a person's voice and appearance. These fake communications often create a sense of urgency or authority, prompting victims to act without verifying the request through official channels.

How to escape: -

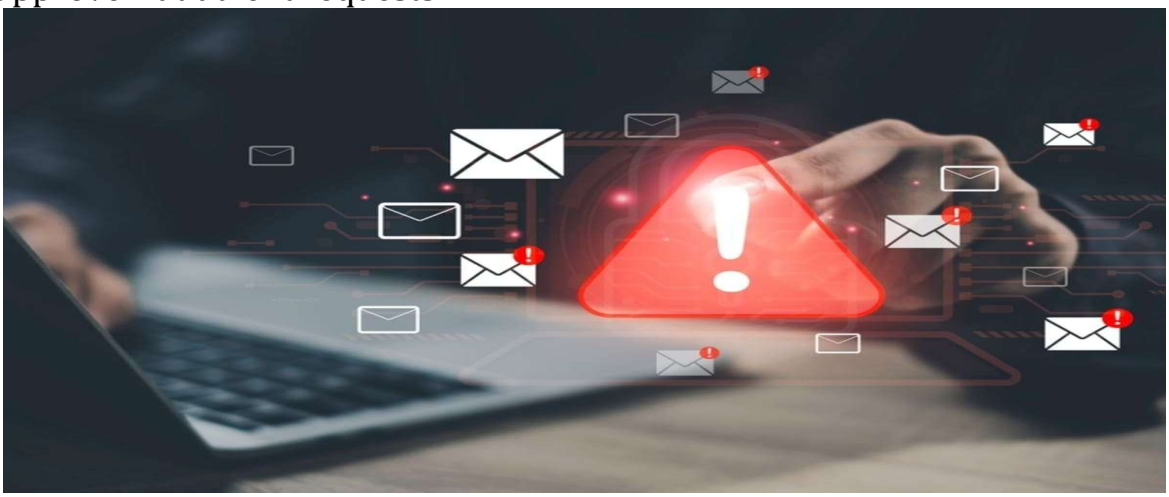
- Cross-check sensitive requests before action.
- Never rely solely on voice or video for authentication.
- Enable Multi-Factor Authentication (MFA) on all official accounts.
- Follow established approval and verification procedures for financial or operational decisions.

- Report any suspicious communication immediately to the cybersecurity or IT security team.

Key Message: *In the era of AI-generated deception, trust must always be verified before action is taken.*

2. Compromised Trusted Channels threat

Compromised Trusted Channels are communication or software delivery channels that users and organizations normally trust but have been taken over or manipulated by cybercriminals. Instead of attacking directly, threat actors exploit trusted platforms such as official email accounts, messaging applications, software update mechanisms, cloud services, or remote access systems to distribute malware, steal credentials, or deceive users. Because these channels appear legitimate, victims are more likely to open attachments, click malicious links, or approve fraudulent requests.



How Does It Operate?

Once a trusted channel is compromised, attackers can bypass traditional security measures and gain unauthorized access to sensitive systems and information. Common examples include phishing emails sent from hacked corporate accounts, malicious software updates from compromised vendors (supply chain attacks), fake messages on collaboration platforms, and misuse of VPN or remote desktop connections with stolen credentials. These attacks can lead to data breaches, ransomware infections, financial losses, operational disruption, and damage to an organization's reputation.

How to Stay Protected?

Organizations can reduce the risk of compromised trusted channels by adopting a layered cybersecurity approach. This includes implementing Multi-Factor Authentication (MFA), verifying software updates through digital signatures, applying the Zero Trust security model, continuously monitoring user and network activities, and conducting regular security awareness training. Timely patch management, email security solutions, endpoint detection and response (EDR), and incident response planning also help detect and contain threats before they cause significant damage.

Key Message: Always verify the sender and confirm requests before opening links, attachments, or sharing confidential data. Report any suspicious activity immediately to help prevent cyber attacks and protect organizational security.

2. KNOWLEDGE BANK

1. Government introduces e-Zero FIR system for cybercrime cases in 18 states and UTs

The government has introduced the system of registering e-Zero FIRs in cybercrime cases across eighteen states and Union Territories. The e-Zero FIR platform enables complaints reported through the **National Cyber Crime Reporting Portal (NCRP)** or the **1930 Cyber Helpline** to be automatically converted into an e-Zero FIR for eligible cyber financial fraud cases, enabling faster police action and investigation.

2. Fake profiles, marriage promises: Government warns of rising matrimonial fraud

The Ministry of Home Affairs' Indian Cyber Crime Coordination Centre (I4C) has warned people against a sharp rise in online matrimonial frauds, saying cybercriminals are exploiting matrimonial websites and apps by posing as wealthy professionals or NRIs, gaining victims' trust with promises of marriage and then duping them of large sums of money. In an advisory, the agency said the growing popularity of digital matrimonial platforms has created fresh opportunities for fraudsters.

3. How to protect IT infrastructure

1. Implement Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) strengthens security by requiring users to verify their identity using two or more authentication factors, such as a password, a one-time password (OTP), a biometric (fingerprint or facial recognition), or a hardware security key. Even if a password is compromised through phishing, malware, or brute-force attacks, MFA provides an additional layer of protection that significantly reduces the risk of unauthorized access.

Government organizations should mandate MFA for all privileged and administrative accounts, remote access, Virtual Private Network (VPN) connections, cloud-based applications, and critical information systems. Where possible, phishing-resistant authentication methods such as FIDO2 security keys or passkeys should be adopted for enhanced security. Regular monitoring of authentication logs and periodic review of user access privileges further strengthen the effectiveness of MFA.

Actions Required

- Enforce Multi-Factor Authentication (MFA) for all privileged, administrative, VPN, remote access, and cloud accounts.
- Prefer phishing-resistant authentication methods, such as hardware security keys or passkeys, for high-risk users.
- Disable legacy authentication protocols that do not support MFA.
- Periodically review user accounts and remove unnecessary privileges.
- Continuously monitor authentication logs to detect suspicious login attempts and unauthorized access.
- Conduct regular user awareness programs on secure authentication practices and the risks of credential theft.

Key Message

Passwords alone are no longer sufficient to protect government systems. Implementing Multi-Factor Authentication (MFA) significantly reduces the risk of unauthorized access, safeguards sensitive information, and strengthens the overall cyber resilience of government IT infrastructure.

4. CYBER GUPSHUP

1. Bank of Baroda Faces Alleged Massive Data Leak; 1,000 GB of Customer Information Reportedly Expose

Bank of Baroda has come under the spotlight following claims by a hacking group that it has leaked nearly 1TB of sensitive customer and internal banking data on the dark web. The alleged incident has drawn significant attention from cybersecurity researchers and threat intelligence platforms. However, Bank of Baroda has not officially confirmed that any data breach has occurred, and no government agency has so far verified the authenticity of the claims.

2. Five cyber criminals held in Varanasi: Police seize 43 ATM cards and 12 passbooks

The Cyber Crime Police of Varanasi Commissionerate has busted an interstate gang involved in cyber fraud. The gang used mule bank accounts and APK files to defraud unsuspecting people. Five gang members have been arrested. Police recovered 15 Android mobiles, three iPhones, 43 ATM cards, 12 passbooks, 10 chequebooks, 11 QR codes, 12 SIM cards, one laptop, one diary, two four-wheelers (Mahindra Thar and Hyundai i-20), and ₹12,060 cash from the possession of the accused.

3. Cybercrime body warns of fake investment scams using PM, Union Ministers' photos

The Indian Cyber Crime Coordination Centre (I4C) has warned people to stay alert against fake investment advertisements circulating on Facebook and Instagram, saying cybercriminals are increasingly using social media to lure victims with false promises of high returns. According to I4C, fraudsters misuse the names, photographs and videos of the Prime Minister, Union ministers, leading industrialists, investment experts, film celebrities and other well-known personalities

5. CYBER HYGIENE

- Use strong, unique passwords and enable Multi-Factor Authentication (MFA) for all official accounts.
- Keep operating systems, applications, and antivirus software updated with the latest security patches.
- Be cautious of phishing emails, suspicious links, and unknown attachments.
- Regularly back up important government data and verify that backups can be restored.
- Follow the principle of least privilege by granting users only the access they need.
- Use only authorized USB devices and scan all removable media before use.
- Lock computers when unattended and protect sensitive information through encryption and secure storage.
- Report any suspicious activity, security incident, or data breach immediately to the IT wing.

6. New development in IT WING

1. Developed PT / Parade / Game Data Entry Screen under the Training Module.
2. Added Leave Planning functionality in the Sambhav Mobile App.


DG CRPF Shri G.P. Singh (IPS) interacted with Jawans & Officers of 209 CoBRA at GC Ranchi and joined in 'Bada Khana' .

CRPF Family Welfare Association (CWA) signed a MoU with HDFC Life under its CSR initiative to provide ₹25 lakh for establishing and equipping the Saksham School at GC CRPF Pinjore.

DG CRPF Shri G.P. Singh (IPS) presenting Memento to Jawan on VRS at a grand farewell party at Dte. Genl.