# BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

## Three cyber fraudsters held for duping investors.

**Incident:**
Mumbai Police arrested three cyber fraudsters, including their handler, from Bandra for allegedly duping investors of crores of rupees by promising high returns from share trading. The case came to light after a 49-year-old Goregaon resident lodged a complaint stating he had been defrauded of ₹2.77 crore.

**Modus Operandi:**
The victim was added to a WhatsApp group by an unidentified individual. The group admin and other members shared seemingly credible stock market investment tips. The complainant was persuaded to transfer funds to multiple bank accounts provided through the app. A significant portion of the funds, amounting to ₹71.22 lakh, was deposited into one of these accounts.

**Action Taken:**
Police arrested the three suspects from Bandra. Further investigation revealed 28 additional cases registered against the same individuals, with total investor losses estimated at ₹18 crore across various states.

**Key Concern:**
The cross-state spread of the fraud and the use of encrypted social messaging platforms for executing financial scams underscore the growing challenge of combating cyber-enabled investment frauds and the urgent need for public awareness and preventive measures.

## Gujrat Cyber Crime busts ₹2 crores Instagram gaming app fraud, 7 arrested.

**Incident:**
A group of individuals was arrested in connection with a fraudulent scheme involving a gaming application promoted through a social media platform. Authorities seized ₹2 crore from 17 different bank accounts linked to the operation. The case surfaced following multiple complaints filed across various regions in the country.

**Modus Operandi:**
The accused were using social media to lure individuals by offering in-game coins for a gaming app. They created fake profiles and gaming application IDs, enticing users to engage in transactions. Once users accepted the offer and received coins—transactions tied to bank entries—they were subsequently threatened with false criminal implications to extort more money or silence.

**Action Taken:**
Acting on a tip-off regarding large-scale fraudulent activity using active mobile numbers, cyber-crime officials launched an investigation. Multiple investigative teams were deployed, leading to the discovery of suspicious financial activity across several bank accounts. The operation led to the arrest of seven suspects and the seizure of substantial funds.

**Key Concern:**
The case highlights a growing trend of cyber-enabled financial fraud using popular social platforms to exploit unsuspecting individuals. The use of threats and intimidation after luring victims into seemingly innocuous gaming-related transactions reflects a dangerous shift in online fraud tactics.

## Biopharma firm targeted by ransomware: Cyber attackers demand 80,000 USD

**Incident:**
A ransomware attack targeted a multinational biopharmaceutical organization based in Pune. The attackers compromised and encrypted critical data across several servers and demanded a ransom of 80,000 USD for the decryption key. They also threatened to sell the organization's proprietary data on the dark web if the ransom was not paid.

**Modus Operandi:**
The initial investigation indicates that the attackers infiltrated the internal network by compromising an endpoint device, likely through a phishing attack that delivered a malicious payload via a deceptive link. Once access was gained, ransomware was deployed to the primary server and subsequently spread to over a dozen secondary servers, encrypting sensitive data across the network.

**Action Taken:**
Following the incident, a formal complaint was filed by a senior official of the affected organization, prompting an investigation by the local cyber-crime police. The probe began immediately after the attack was reported and is currently ongoing.

**Key Concern:**
The incident underscores significant vulnerabilities in endpoint security and highlights the growing risk of targeted cyber-attacks against critical infrastructure and intellectual property. It also reflects the increasing use of ransomware as a tool for financial extortion and data theft in high-value sectors.

Powered by GRAMAX
A GMR GROUP ENTERPRISE

## Cyber crooks dupe Hyderabad woman to tune of Rs. 1.3 lakh in house rental scam

**Incident:**
A woman was duped of ₹1.30 lakh in a cyber fraud case involving a fake rental transaction. The fraud occurred after she posted an advertisement for renting her flat on an online platform and was contacted by individuals posing as potential tenants.

**Modus Operandi:**
The fraudsters contacted the woman under the guise of being from a defense background and claimed that an "accountant" would handle the financial transactions. Using a deceptive method called the "reversal model," the supposed accountant first convinced the woman to transfer a small amount (₹5), which was immediately reversed to build trust. After this initial trust-building step, the woman was persuaded to transfer a significantly larger amount, which was not returned.

**Action Taken:**
Following the incident, the victim approached the cybercrime authorities and lodged a formal complaint. An investigation into the matter has been initiated by the concerned law enforcement team.

**Key Concern:**
The case highlights how fraudsters exploit trust-building tactics and impersonation to deceive individuals in online financial transactions. It also underlines the risks associated with sharing personal information and engaging in monetary exchanges with unknown individuals over digital platforms.

## Education Department website hacked; homepage defaced with provocative and politically charged messages.

**Incident:**
A government education department's official portal was compromised in a cyber-attack. The homepage was defaced and replaced with provocative and inflammatory messages aimed at spreading misinformation and inciting public unrest.

**Modus Operandi:**
The attackers gained unauthorized access to the website and altered its homepage to display politically charged and divisive content. The messages included unverified claims related to national security incidents and personal attacks on individuals associated with recent events shared widely on social media.

**Action Taken:**
Authorities became aware of the breach shortly after the defacement occurred. Investigative and technical teams were likely deployed to assess the breach, restore the website, and identify the source of the attack. Further official response details are awaited.

**Key Concern:**
This incident highlights the vulnerability of official government websites to cyber intrusions and the potential misuse of such platforms for spreading disinformation. It also underscores the threat posed by cyber-attacks aimed at destabilizing social harmony and targeting individuals for psychological or political manipulation.