BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Ahmedabad Tech Professional Duped of ₹52 Lakh Through Fake Criminal Case

Modus Operandi: Scammers posed as law enforcement agents, falsely accused the victim of drug trafficking, and orchestrated a fake investigation. They isolated him in a hotel and coerced him into transferring nearly all his savings.

Lessons Learned:

- **Never trust unsolicited law enforcement calls:** Real agencies follow proper legal procedures and do not demand money transfers.
- **Verify identities:** If contacted by authorities, call official helplines to confirm legitimacy.
- **Avoid isolation tactics:** Scammers often push victims to cut communication with family to reduce external intervention.

Lucknow Family's Devices Hacked and Monitored

Modus Operandi: Hackers compromised the family's mobile phones, gaining access to personal data and attempting to misuse it.

Lessons Learned:

- **Use strong security measures:** Enable two-factor authentication (2FA) and install antivirus software on all devices.
- **Watch for unusual behavior:** Unexpected battery drain, slow performance, or unfamiliar apps can indicate a breach.
- **Regular device audits:** Review app permissions and delete suspicious apps.

Doctor Loses ₹6 Lakh Through Malicious APK File

Modus Operandi: The victim downloaded a fake KYC update APK file, granting scammers access to his device. They exploited this access to generate and use 30 OTPs, draining his accounts.

Lessons Learned:

- **Avoid APK downloads from unknown sources:** APKs can easily contain malware. Always download apps from trusted stores (Google Play, App Store).
- **Be wary of KYC fraud:** Banks do not send KYC updates through random links.
- **Check for suspicious permissions:** Avoid apps requesting access to messages, calls, or financial data without justification.

Agra Woman Trapped in a 'Digital Arrest' for Four Days

Modus Operandi: Scammers posed as law enforcement officers, accused her of criminal involvement, and placed her under a virtual house arrest. They extorted ₹13.42 lakh under the pretext of clearing her name.

Lessons Learned:

- **Law enforcement doesn't conduct digital arrests:** Real authorities follow proper legal channels.
- **Fake Skype calls and documents:** Video calls and documents can be forged. Verify identities with official contacts.
- **Don't comply under pressure:** Scammers use intimidation tactics. Pause and consult with trusted individuals before acting.

Retired Bank Manager in Pune Scammed of ₹2.22 Crore in Fake Insurance Schemes

Modus Operandi: Fraudsters impersonated government officials and convinced the victim to invest in fake insurance policies, charging her repeatedly for taxes, processing fees, and verification charges.

Lessons Learned:

- **Verify all investment opportunities:** Cross-check with official financial institutions before purchasing policies.
- **Beware of excessive charges:** Scammers often fabricate fees (GST, income tax, verification) to extort more money.
- **Don't trust random government calls:** Legitimate agencies rarely make cold calls regarding personal investments.

Key Takeaways to Protect Yourself:

1. **Stay Skeptical of Unknown Callers:** Scammers often impersonate law enforcement or government officials to instill fear and coerce victims into compliance.
2. **Never Share Sensitive Information:** Avoid sharing Aadhaar, PAN, or bank details over phone calls or unverified platforms.
3. **Verify Before You Act:** If someone claims to be from the police, bank, or government, verify their identity through official websites or helplines.
4. **Use Strong Cybersecurity Practices:**
   - Enable two-factor authentication (2FA).
   - Regularly update devices and apps.
   - Use anti-malware tools.
5. **Don't Transfer Money Under Pressure:** Scammers create urgency to prevent victims from verifying claims. Always take time to cross-check.

Stay alert, verify before you trust, and protect your digital identity.

Powered by GRAMAX
A GMR GROUP ENTERPRISE