BE CYBER SAFE

WEEKLY DIGEST OF CYBER SCAMS TO HELP YOU STAY AHEAD

Telecom Spoofing Scam: Misuse of SIM Cards and SMS Headers

Victim's Experience:
Authorities uncovered a widespread telecom fraud involving the misuse of SIM cards, SMS headers, and IP addresses. Fraudsters obtained SIM cards using fake documents and tampered with mobile numbers to send deceptive messages. Many victims received spoofed international calls, appearing as legitimate local numbers, luring them into scams.

Key Takeaway:

- **Caller ID can be faked:** Do not trust phone calls or messages based on the displayed number. Scammers can spoof legitimate-looking numbers.
- **Verify suspicious calls:** If you receive calls claiming to be from banks or government agencies, verify the authenticity by calling their official helpline.
- **Report suspicious messages:** Use platforms like the Cyber Crime Helpline (1930) or the DoT portal to report suspicious telecom activities.

Digital Arrest' Scam: ₹44.5 Lakh Lost by Delhi Resident

Victim's Experience:
A man from Delhi fell victim to a 'digital arrest' scam after receiving a call from someone posing as a government official. The scammers accused him of involvement in criminal activities and threatened him with immediate arrest. Under pressure, the victim transferred ₹44.5 lakh to multiple bank accounts. Later, he realized it was a scam and reported it to the police, leading to the arrest of four cyber criminals.

Key Takeaway:

- **Scammers use fear tactics:** Fraudsters exploit legal threats to manipulate victims into making quick payments.
- **Stay calm and verify:** If you receive such calls, avoid making impulsive financial transfers. Verify with local police or legal authorities.
- **Do not share sensitive information:** Government agencies will never demand payments over calls.

Fake Vehicle Registration Websites: Maharashtra Transport Scam

Victim's Experience:
Vehicle owners in Maharashtra were targeted by scammers through fake websites offering High-Security Registration Plates (HSRP). Victims paid for fake plates through fraudulent portals, only to realize they had been scammed. The state transport department identified six fake websites deceiving vehicle owners.

Key Takeaway:

- **Verify official websites:** When booking services like HSRP installation, only use government-authorized portals.
- **Beware of unofficial payment links:** Scammers often create near-identical fake websites. Always double-check the URL before making payments.
- **Report fraudulent websites:** If you suspect a fake website, report it to the Cyber Crime Portal (www.cybercrime.gov.in).

Share Trading Scam: Retired Pilot Loses ₹1.45 Crore

Victim's Experience:
A 63-year-old retired Air Commodore from Mumbai was lured into an online share trading scam via WhatsApp. He was added to a group discussing stock tips and was persuaded to download a trading app. Over time, he transferred ₹1.45 crore into fraudulent bank accounts. When he tried to withdraw ₹8 crore shown as his 'profits,' he was unable to do so. Upon realizing the scam, he reported it to the cyber police.

Key Takeaway:

- **Beware of WhatsApp investment groups:** Scammers often create fake groups promising high returns to lure victims.
- **Do not download unknown apps:** Avoid installing financial apps from unknown sources or links sent via messages.
- **Verify trading platforms:** Invest only through SEBI-registered brokers and verify the authenticity of the platform.

Himachal Pradesh Cyber Crime Cell's Fight Against Online Fraud

Victim's Experience:
The Himachal Pradesh Cyber Crime Cell reported handling 12,000 online fraud cases in the past year, with victims losing a combined ₹114 crore. The cell successfully recovered ₹15 crore through real-time coordination with banks. Many victims were targeted through phishing scams, fake job offers, and social media frauds.

Key Takeaway:

- **Prompt reporting helps recovery:** Victims who reported fraud early had a better chance of recovering their lost money.
- **Use official channels:** If you fall victim to online fraud, immediately report it to the National Cyber Crime Reporting Portal (NCRP).
- **Stay alert on social media:** Scammers often impersonate companies and individuals on social platforms to lure victims.

Tips to Protect Yourself from Cyber Fraud:

- **Think before you click:** Avoid clicking on suspicious links, especially those sent via SMS, email, or WhatsApp.
- **Use strong passwords:** Use unique and complex passwords for online accounts and enable two-factor authentication.
- **Stay informed:** Follow updates from the Cyber Crime Department and learn about the latest scams.

Cyber scams are increasing in India, but awareness is your best defense!
Share this with friends & family to keep them safe.