

Handling of Cybersecurity Frauds by Veterans and Veer Naris

Commander P Rajagopal Tampi IN (R)

A Brief idea of AI

- AI and Large Language Models
- What is the difference between software and AI?
- What is an agent?
- How does an agent differ from an LLM?
- What are some important AI benefits?
  - Rapid progress in scientific discoveries
  - New materials, new molecules, productivity benefits
  - Weather predictions
  - Software coding
  - Robots and automation
- What are the major risks of AI?
  - Deception, power seeking and self -preservation
  - Deepfakes
  - Loss of control
  - Recursive self-improvement (RSI)
  - Self replication

Major AI risks causing cybersecurity impact

- Huggingface incident, Anthropic IoT prediction
- Hacking refrigeration plants in France – mid Oct 2026
- Government web-sites down (PHP bugs) – 21st Oct 2026
- Inherently a dual-use technology – great dangers in autonomous weapon, CBRN and wartime use.
- AI is an enabler and defender of cybersecurity
- More powerful computing engine than our brains (faster and unlimited resources). We wont be able to catch up or understand them
- Agents run 24x7 and in hundreds can brute force encryption, find bugs in software.
- AI systems can be up and running at full knowledge after training on power on, can migrate anywhere and we may not detect them till it is too late.
- Near term harm can come from AI taking over the internet and hacking infrastructure systems and utilities.

Protecting ourselves from AI harm

- Approach AI systems with scepticism and low levels of trust:
- Do not trust what is obtained from social media.
- Keep Siri or equivalent conversation monitoring apps disabled.
- If you use AI tools like Chat GPT or Claude switch off the “Improve model for everyone” option and the location option.
- Avoid using commercially available AI agents except if you can reliably verify how it handles your personal data. Use it for low risk applications only if you absolutely need to.
- Do not handover your thoughts and intentions to any AI agent especially your diary or private journal
- Do not give access to AI agents for automating transactions in your bank accounts, bill, payments, other financial matters and transactions.
- Do not provide access to your folders, email services and card information.
- Always “think for yourself”, do not ask AI to do your thinking for you.
- Verify your thought process with a trusted friend not AI systems.
- Use privacy controls effectively, upload medical and financial records only on inescapable need.

Protecting against AI impersonation and deception

- Never trust a caller merely because the voice sounds exactly like a family member.
- If someone claims to be a relative in an emergency and asks for money, disconnect and call back that person on their previously saved number.
- Agree on a private family verification phrase for emergencies. Do not share it on social media.
- Do not assume a video call is genuine simply because you recognize the person's face.
- Treat urgent requests for money, secrecy or immediate action as warning signs.
- Do not believe messages claiming that police, CBI, customs, courts or other authorities have placed you under digital arrest.
- Do not trust caller ID, WhatsApp profile photographs or displayed organization names as proof of identity.
- Reduce your online data profile and footprint to the minimum possible
- Impersonation example ($25 mn transferred due to fake video call approval).

Protecting your identity and privacy

- Avoid sharing identity documents without a legitimate purpose.
- Where appropriate, add a purpose-specific watermark to copies of identity documents.
- Review privacy settings on WhatsApp, Facebook, Instagram and other social platforms.
- Restrict who can add you to messaging groups, try and minimize group memberships.
- Limit publicly available voice recordings and personal videos where practical.
- Avoid publishing detailed family relationships, routines and financial circumstances.
- Remove unnecessary personal information from public online profiles.
- Use UIDAI's official Aadhaar authentication-history and biometric-locking facilities where suitable.
- Check your mobile connections through official government telecom services where available.
- Use a separate email address for low-trust subscriptions and registrations.
- Review cloud-sharing links and remove public access when no longer needed.

Banking and financial safeguards

- Never disclose your banking PIN, UPI PIN, ATM PIN, CVV, password, date of birth or OTP.
- Remember: You do not need to enter a UPI PIN to receive money. Entering it generally authorizes a payment.
- Never scan a QR code sent by a stranger to receive money.
- Never approve an unexpected UPI collect request.
- Do not trust investment schemes promising guaranteed high returns or extraordinary profits using AI.
- Never allow agents and strangers to operate your banking application remotely.
- Do not share photographs of bank cards, cheques or financial documents with unknown people.
- Enable transaction alerts on all important accounts.
- Set daily transfer limits appropriate to your needs, where your bank permits.
- Cards care: Don't store card details if you can avoid it online. Avoid automatic filling up procedure of card details.
- Reduce credit-card online transaction limits when high limits are not required anymore.
- Disable international card transactions when not required.
- Disable contactless transactions when travelling abroad specially – Amsterdam incident
- Keep substantial savings separate from accounts used for frequent online/UPI payments.

Protecting phones and passwords

- Use different passwords for banking, email and important accounts.
- Use long passwords or passphrases that are difficult to guess.
- Enable two-factor authentication or FIDO2 authentication wherever available.
- Lock your phone with a PIN, fingerprint or face authentication.
- Keep your phone and applications updated with the latest release.
- Download applications only from official app stores.
- Do not install an APK or application sent through WhatsApp, SMS or email by an unknown person.
- Do not install screen-sharing or remote-access applications at a stranger's request.
- Do not click unexpected links claiming that your KYC, PAN, Aadhaar, bank account, electricity supply or delivery will be blocked.
- Open the official banking or service application yourself instead of clicking links in messages.

Protecting your home and accounts

- Register a backup security key for accounts if possible and keep it securely stored.
- Avoid putting up personal, family, relationship details and photographs on social media.
- Do not publish your travel itinerary or daily routine on social media.
- Do not expose your likes, dislikes, political leanings, financial purchases and private activities on social media.
- For home wifi use WPA2 AES or WPA 3 encryption with strong passwords.
- If you use home cameras and IoT devices make sure that the data stays on your data card. Do not transfer it to the cloud.
- Block and report impersonation accounts on social media.

What to do if fraud has happened?

1. Call 1930 immediately - India's national cyber financial fraud helpline.
2. Report the incident online at National Cyber Crime Reporting Portal
3. Contact your bank immediately
4. Request blocking of affected cards, accounts or payment access as appropriate.
5. Early reporting improves the opportunity to stop further transfers, although recovery is not guaranteed.

Also take these steps:

1. Stop communicating with the suspected fraudster.
2. Disconnect remote-access sessions and seek help removing unauthorized software.
3. Change compromised passwords using a trusted device.
4. Revoke suspicious login sessions and reset authentication methods where necessary.
5. Preserve messages, screenshots, phone numbers, transaction references and other evidence.
6. Report fake profiles, deepfakes and impersonation content to the relevant platforms and authorities.
7. Warn affected contacts if your account has been used to send fraudulent messages.

Final words: Personal safety, security checklist

1. Never trust a familiar voice or face without independent verification.
2. Never disclose an OTP, PIN, password or banking credential.
3. Never transfer money because of threats, urgency or secrecy.
4. Never believe claims of digital arrest or police safe accounts.
5. Never scan a QR code or enter a UPI PIN to receive money.
6. Never install software or share your screen at a stranger's request.
7. Never trust unexpected links, investment offers or pension-related messages.
8. Keep phones updated and enable strong account authentication.
9. Consult a trusted person before making unusual financial decisions.
10. If fraud occurs, contact your bank and call 1930 immediately.
11. The single most effective principle to remember is:
12. Never trust a voice, face, message or video merely because it appears genuine. Verify the identity and the request independently before taking action.

Mobile phone settings

Mobile phone security and settings		
SETTINGS	RECOMMENDED SETTING	SENSITIVITY
location	only when using the app	very high
camera	only when using the app	very high
microphone	ask every time	very high
contacts and sms	ask every time	high
calendar	ask every time	very high
health data	no	very high
photos and videos	no	high
physical activity	no	very high
notifications	no	high
bluetooth	only when using	high
AI apps	do not use data for training	very high

LUCK IS WHERE OPPORTUNITY AND PREPAREDNESS MEET

AIP Research web-site HTTPS:AIPATHFINDER.ORG

APPLIED HUMAN-CENTRIC AI – HTTPS://www.amazon.com/dp/B0CYXHYPHC

POWER UP YOUR INTELLIGENCE - https://www.amazon.in/dp/B0D3WZXY99

THANK YOU!