Date : 01.03.2026

Vol 2 Issue 23

MEGHALAYA RURAL BANK

Cybersecurity Digest

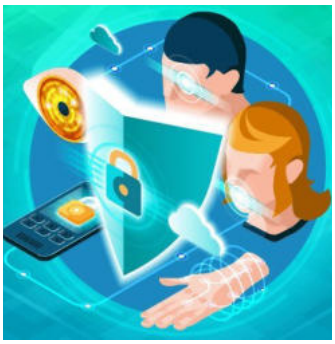
Bi-Weekly update by the O/o CISO of Meghalaya Rural Bank

Claude Code Security

Claude Code Security is an AI-assisted vulnerability detection system embedded within Claude Code, an AI programming assistant developed by Anthropic. The core idea is to use AI reasoning rather than traditional pattern matching to scan codebases and surface potential security flaws that could be exploited in software applications.

Unlike conventional static analysis or signature-based scanners that look for known patterns of insecure code, Claude Code Security uses large language models to reason about how data flows through a codebase and how different parts of a program interact. This can help in identifying more complex issues such as logic errors, insecure data handling and configuration weaknesses

AI Based-Biometric Scam



A new tactic by cybercriminals has emerged where fraudsters are targeting not only financial assets but also citizens' biometric identity data. Experts have warned that AI-based biometric scams are spreading rapidly, with criminals attempting to steal sensitive identity information such as facial and voice data.

Fraudsters often approach people in crowded public places such as malls, metro stations, or markets. They may pretend to need help and request mobile phones under the pretext of checking pension status, government benefits, or technical settings in an app. During such interactions, the victim's photograph, voice, or other biometric data may be secretly recorded.

In some cases, criminals may use video calls or screen recording techniques to capture biometric information. If a person unknowingly grants camera or microphone permissions, biometric data can be stolen within seconds.

The stolen biometric data can be used to create AI-generated fake identities. Criminals may conduct social engineering attacks and attempt to bypass verification systems by generating synthetic voice or facial imitations. Such misuse of technology is increasingly associated with financial fraud and identity theft.

Security experts advise citizens not to hand over their mobile phones to unknown persons and to avoid keeping their face visible for long periods during unknown video calls. In crowded places, people should remain cautious if strangers ask for quick assistance and avoid sharing screen or camera access.

Parents are also advised to educate children and elderly family members about such cyber threats, as criminals often target individuals who are less familiar with digital security practices.

Cybersecurity specialists believe that biometric data theft cases may increase in the future as deepfake technology is being misused. Fraudsters can generate fake videos and voices to deceive people using advanced AI tools.

Citizens are advised to disable unnecessary app permissions on their mobile devices and immediately report suspicious activities to cyber helpline numbers. Special caution is recommended during digital interactions with strangers in public spaces.

Experts say that biometric data protection is no longer limited to financial security but has become an essential part of personal safety. Awareness and vigilance are considered the most effective measures to prevent such emerging digital threats.

Deepfakes and Digital Safety: A Citizen's Guide to AI Scams

Introduction: The Double-Edged Sword of AI

India is one of the world's fastest-growing digital economies. While AI is driving progress in healthcare and agriculture, it has also given rise to a new breed of cybercrime: Synthetic Media Fraud, commonly known as "Deepfakes."

Deepfakes are realistic-looking images, videos, or audio recordings created by AI algorithms. Scammers use these to impersonate family members, bank officials, or government authorities. To stay safe in the Digital India era, every citizen must practice "Cyber Hygiene."

The "Voice Clone" Scam (The Emergency Call)

The Threat: Scammers can now clone a person's voice using just 3 to 10 seconds of audio taken from social media (Instagram Reels or Facebook videos). They use this AI-generated voice to call parents or spouses, claiming to be in an emergency (kidnapping, accident, or arrest) and demanding an immediate money transfer.

How to Spot It:

- **Urgency:** The caller will always demand immediate action to panic you.
- **Audio Quality:** Listen for robotic pauses or unnatural background noise

The "Family Password" Defense:

- **Action:** Establish a secret "Code Word" with your family members today.
- If you receive a distress call from a loved one, ask for the code word. An AI bot cannot know your family secret.
- Always disconnect and call the person's original mobile number to verify.

Video KYC and Deepfake Calls

The Threat: With the rise of Video-KYC for banking, fraudsters use Deepfake videos to impersonate bank officials or law enforcement officers. They may claim your account is "blocked" and ask you to reveal OTPs over a video call.

How to Spot a Deepfake Video:

- **Unnatural Blinking:** AI models often struggle to replicate natural eye blinking patterns.
- **Blurry Edges:** Look at the edges of the face or hair; deepfakes often look "glitchy" or blurry around the borders.

The "Hand Wave" Test:

- **Action:** If you suspect a video caller is fake, ask them to wave their hand in front of their face or turn their head side-to-side.
- Deepfake filters usually "break" or glitch when an object (like a hand) passes over the face.

The "Zero Trust" Rule for UPI & Aadhaar

AI can automate attacks, but it cannot bypass the fundamental rules of banking if users are alert.

A. UPI Safety (The Golden Rule)

- **Fact:** You never need to enter your UPI PIN to receive money.
- If a caller asks you to scan a QR code or enter a PIN to "receive a refund" or "win a prize," it is 100% a scam.

B. Aadhaar Biometric Lock

- **Fact:** Scammers use silicon fingerprints to breach Aadhaar-enabled Payment Systems (AePS).
- **Action:** Download the official **mAadhaar App** or visit the UIDAI website and enable "**Biometric Lock**". Unlock it only when you need to perform a verification. This creates a hard shield against identity theft.

SANCHAR SAATHI

The Government of India has launched specific portals to help citizens fight these threats:

Sanchar Saathi (Chakshu Facility): *Visit* ***sancharsaathi.gov.in to report suspected fraud communications (calls or SMS) received on your mobile.***

CyberCrime.gov.in: ***Use this portal or dial 1930 immediately if you have lost money to a financial scam. The "Golden Hour"*** *(reporting within 1 hour) increases the chances of recovering lost funds.*