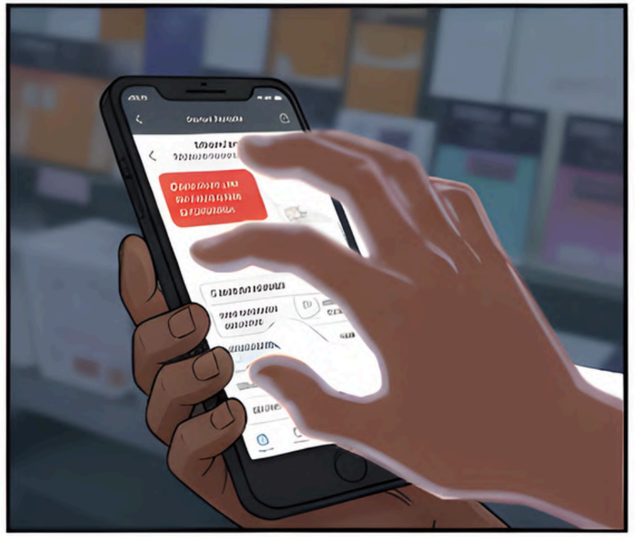
Cyber Resilience
Financial Safety

Learn More

CYBER-SECURITY AND INDIA'S GROWING DIGITAL ECONOMY

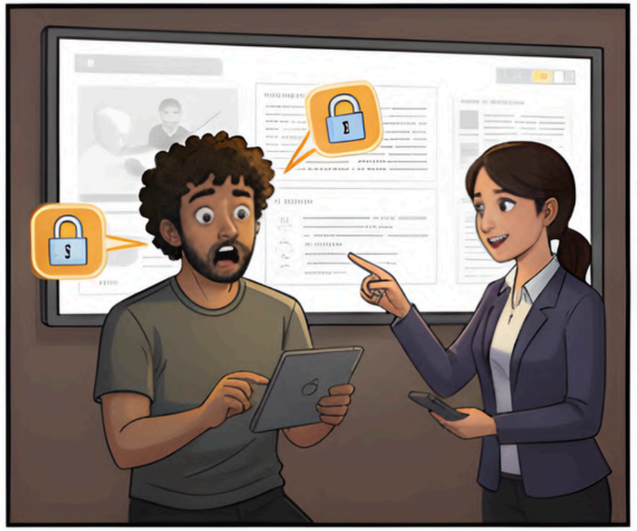
With India's growing digital economy, traders are increasingly relying on online transactions, mobile payments, and digital platforms.



Cybersecurity is crucial to protect financial data, business assets, and customer information from cyber threats.

A security breach can lead to financial losses, reputational damage, and regulatory penalties.

As cyber threats continue to evolve, businesses must stay alert and adapt.

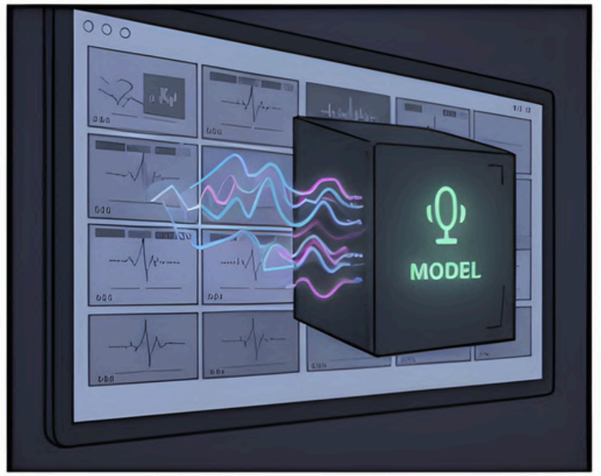


Invest in cybersecurity awareness, implement strong authentication, and ensure compliance with data protection laws.

Cyber resilience is not just an option but a necessity for long-term business sustainability in the digital age.

AI VOICE CLONING

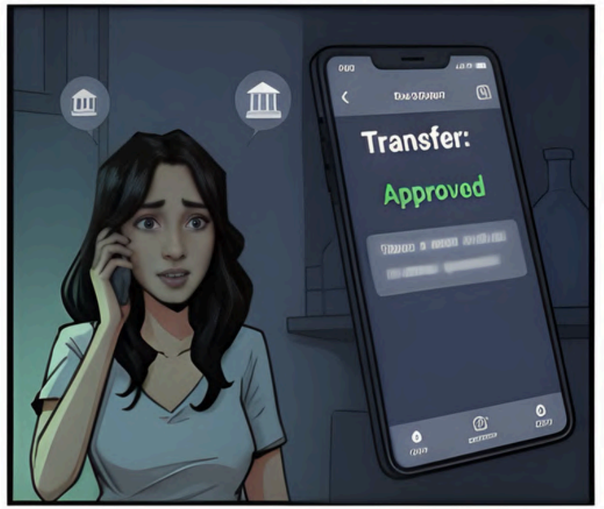
Audio clips are everywhere public videos, voicemail snippets, social posts. Plenty to work with...



An AI model learns the voice's patterns tone, pace, timbre in a black-box process."

Armed with a convincing voice, the attacker calls pretending to be someone they know.

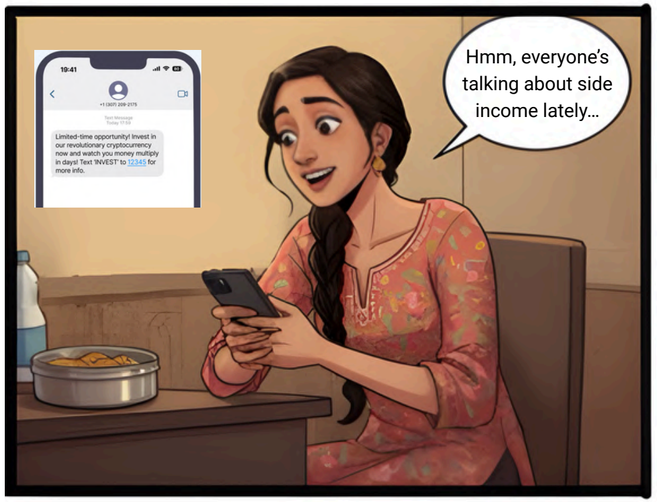
The trick isn't just sound it's timing, urgency, and familiarity.



Trust used against them: money, access, or private info can be lost before anyone realises.

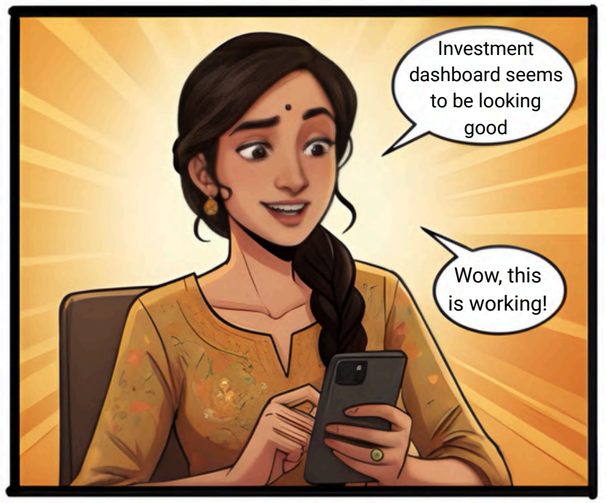
Never act on urgent voice-only requests; always verify via a second trusted channel, use transaction checks with separate-device OTPs, and immediately report suspicious calls to your bank and cybercrime authorities.

INVESTMENT FRAUD

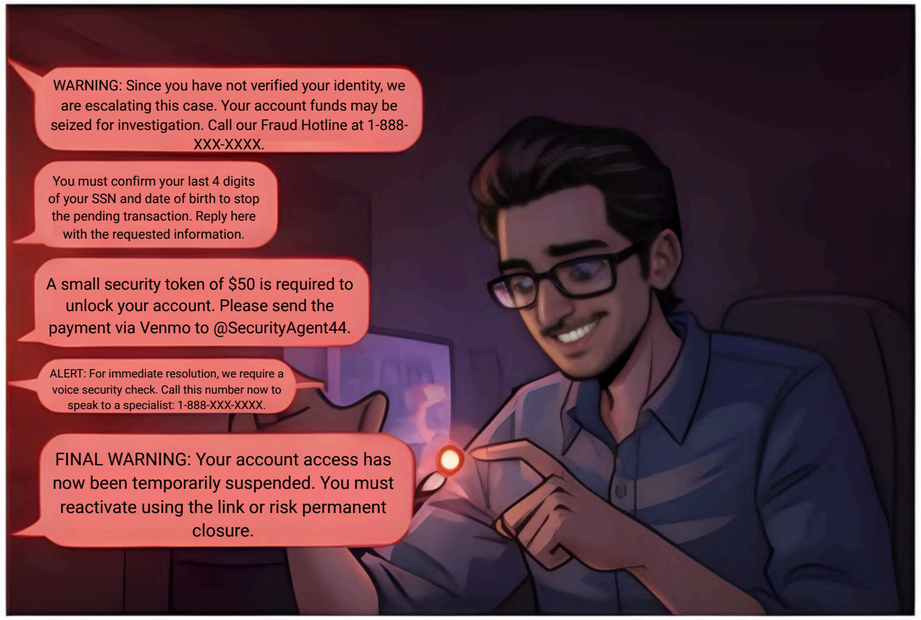


Scams don't always look shady. They look meticulously designed.

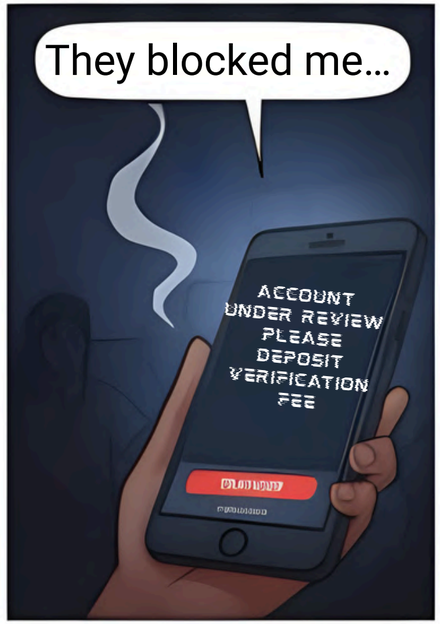
The fraudster builds credibility fake certificates, testimonials, even small early 'profits



Nothing hooks faster than seeing numbers rise.



& Urgency kills judgment.



When reality hits, the account, and the advisor both disappear.

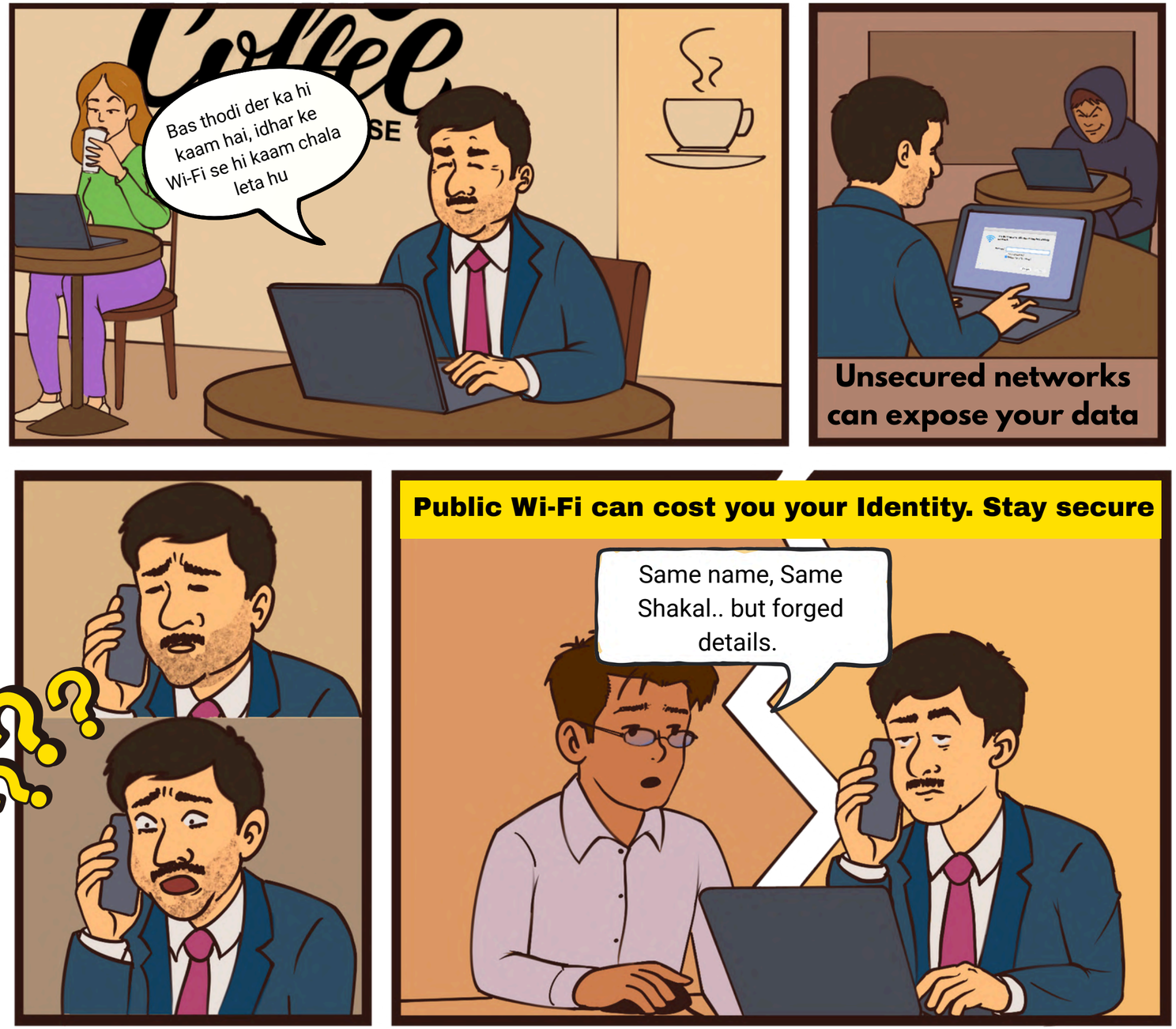
Real investments don't ask for secrecy, pressure, or direct transfers

QR CODE SCAM


Just a quick coffee...
Wait... that's not the cafe's name?!?
₹250
Paid to Karan Gupta
PhonePe • 9876543210@ybl
7 Jan, 3:21 PM
UPI transaction ID: 189273980087
AREY RUKO BHAI!! ye QR Code KAUN chipka gaya???
Money GONE, NO coffee?
Always double-check QR codes. Avoid scanning stickers that look pasted
Thank You!
Home

MALWARE & RANSOMWARE

IDENTITY THEFT



Social Engineering Attacks

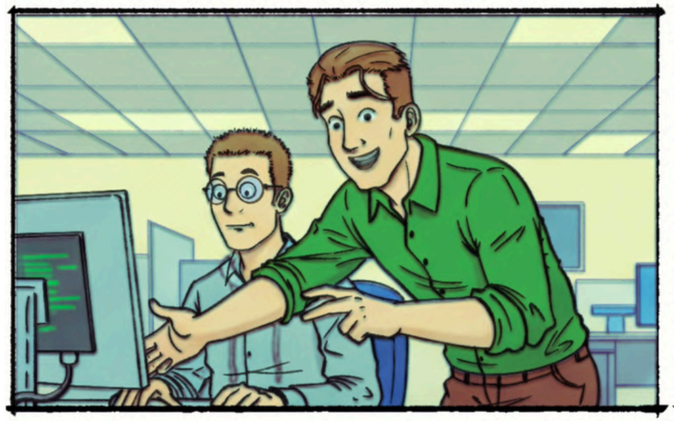
A stranger claiming to be from IT, makes his rounds in the office

Suspicious activity begins as the imposter accesses sensitive data.

The employee realizes too late, data is already being stolen!

Always verify identity before allowing access — stay alert and report suspicious behavior.

SUPPLY CHAIN ATTACKS

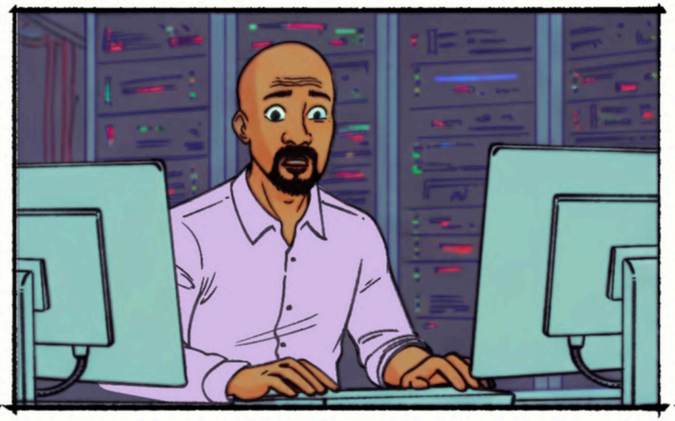


It started like any other day... a routine software update, from a trusted vendor.

But hidden inside that “trusted” code — danger was waiting to strike.

In seconds, chaos spread. Systems crashed. Data vanished. Panic set in.

The IT team rushed to respond — but the damage was already done.



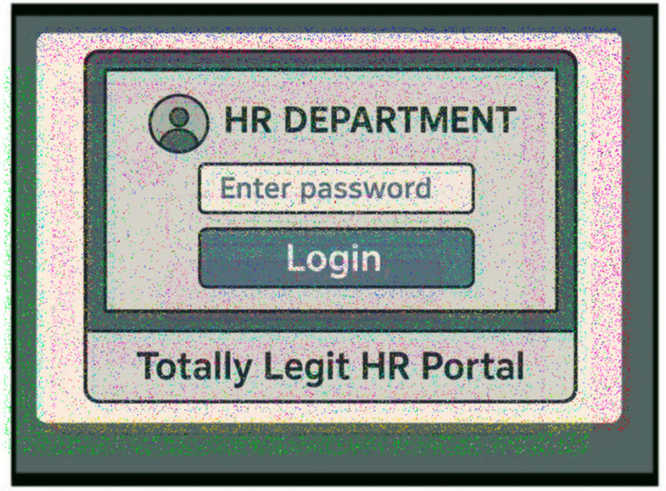
The truth hit hard: the breach came through the supply chain itself.

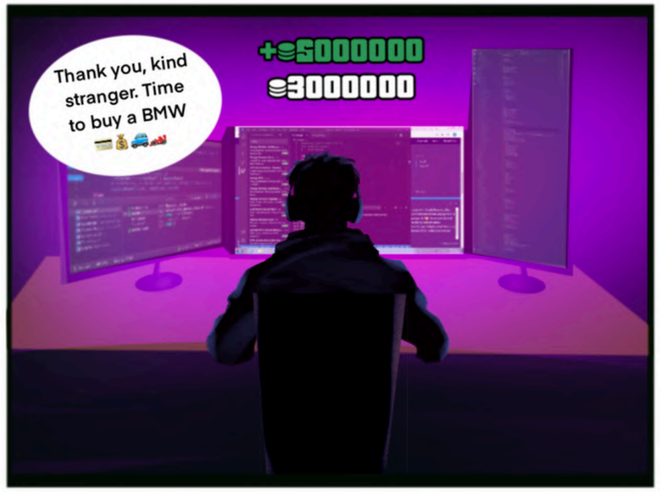
Now, they know better — every link in the chain must be secure.

ALWAYS VERIFY YOUR SOURCES.

Phishing


HR wants my password? Weird... but hey, promotions don't click themselves.


HR DEPARTMENT
Enter password
Login
Totally Legit HR Portal

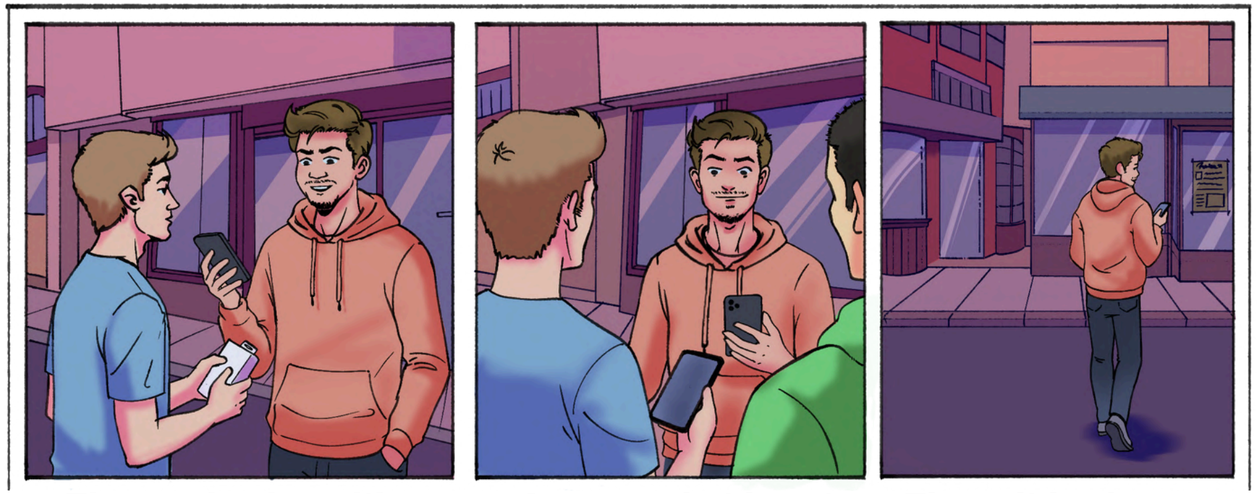

Thank you, kind stranger. Time to buy a BMW
+$5000000
$3000000


$500000


Relax. It's just a phishing attack. We'll reset your account
Next time, don't feed the phish.


Click smart, not fast.
Rule one: If it looks fishy... it probably is.

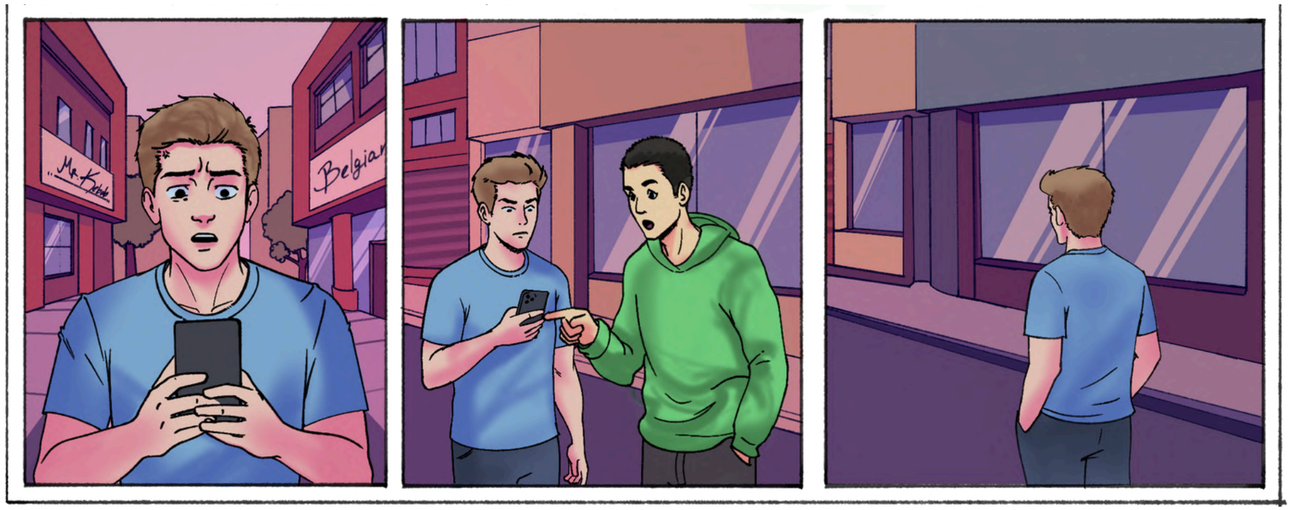
PAYMENT FRAUD



The con begins with a smile. Don't let charm distract you from your safety.

A screenshot is not payment. Never trust a picture when your money is on the line

The exit is always hurried. If they rush, alarm bells should be screaming.



THE TRUTH: ZERO BALANCE. The sinking feeling of knowing you've been scammed

STOP! The ONLY proof is the money in your account. Everything else is a lie.

PAYMENT FRAUD IS REAL. Verify every transfer. Don't be the next victim.

E-COMMERCE SCAM

Another late night, another order packed with care. Small business, big dreams.

“Payment received!” — the message flashes bright. A screenshot. ₹2,000. Relief.

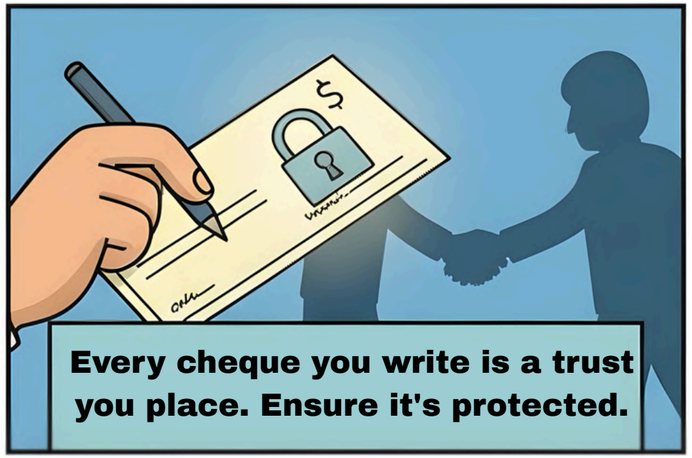
Trusting the customer, he ships the product off — no questions asked.

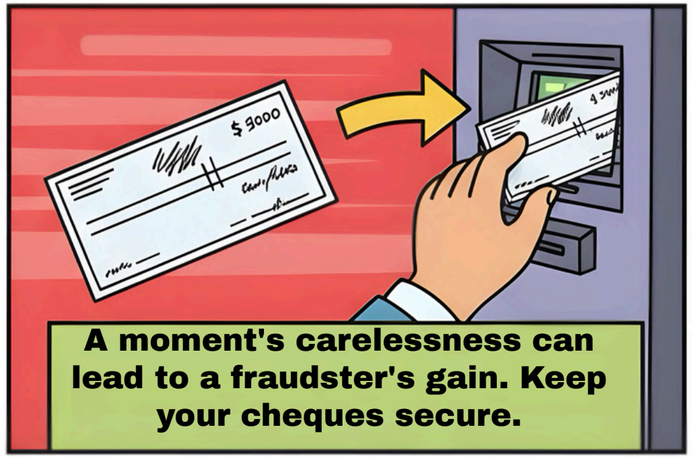
Hours later, he checks again. Something feels off... the payment never arrived.

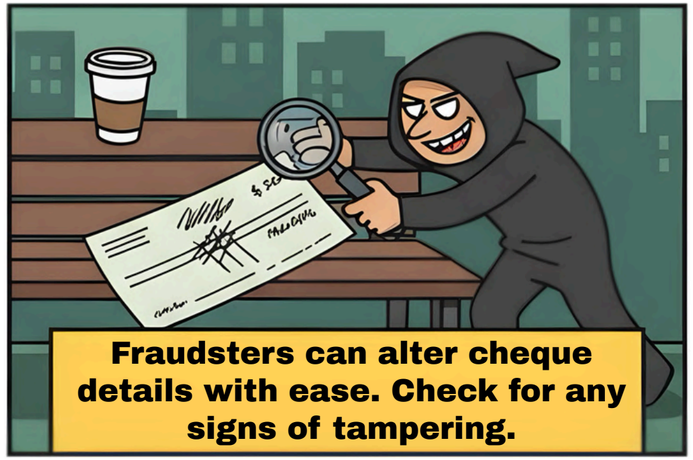
His smile fades. The “proof” was fake. His product — gone.

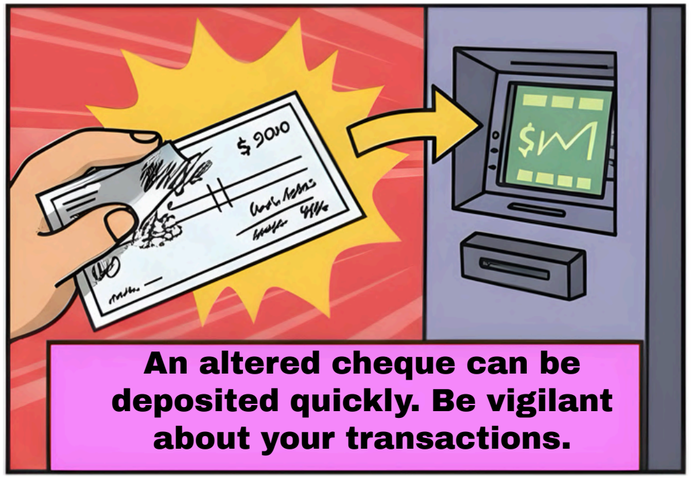
He stares at the screen... lesson learnt the hard way. “Always verify before you trust.

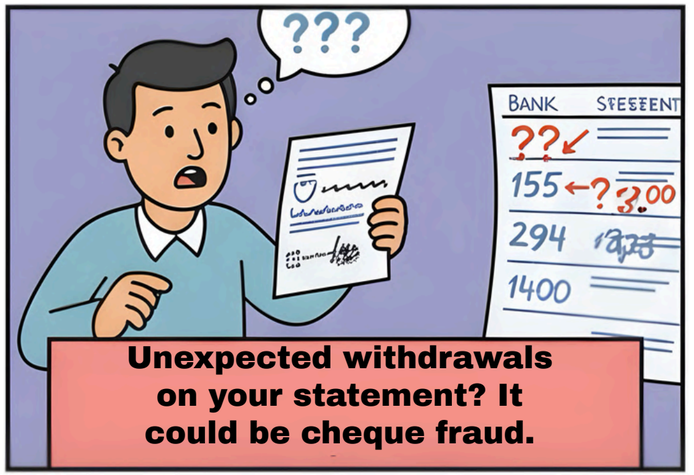
CHEQUE FRAUD











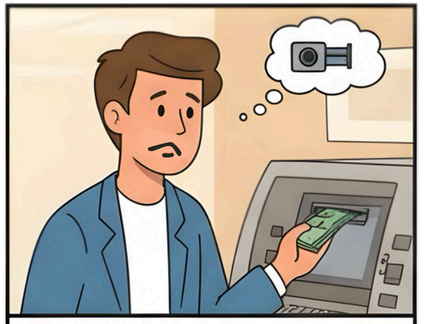
ATM FRAUD

ATMs are convenient, but stay alert! Always be aware of your surroundings for suspicious activities or people

Fraudsters install devices on the card slot to steal your card details. Give the slot a tug—if it moves, don't use it.

Stolen info is used fast. Once they have your data, thieves can quickly empty your account. Act quickly if you see something suspicious.

Cover your PIN! Always use your hand or an object to shield the keypad when entering your Personal Identification Number.



Check for hidden cameras. Fraudsters use tiny cameras to capture your PIN. Look for unusual attachments or holes near the screen or keypad.

Enable instant alerts. Transaction alerts catch suspicious activity early, giving you time to stop fraudulent withdrawals.

See something? Say something. Report suspicious activity or unauthorized transactions to your bank immediately.

Don't wait! Report unusual devices. If an ATM looks tampered with, report it to the bank and law enforcement right away.

SUMMARY

1. Use ATMS in secure, well-lit locations
2. Cover the Keypad pin
3. Check for unusual Card slots or devices
4. Enable alerts and Freeze cards whenever required

Frequently Asked Questions

FREQUENTLY ASKED QUESTIONS

1. What is Cyber Resilience?

Cyber resilience is the ability to prepare for, withstand, and recover from cyber incidents. It ensures that individuals and institutions continue operating safely even when facing digital threats or attacks.

2. Why is Cyber Resilience important in today's financial environment?

With financial systems becoming increasingly digital, the risk of cyberattacks, fraud, and data breaches has grown. Cyber resilience helps maintain trust, protect sensitive information, and ensure uninterrupted access to financial services.

3. What is Financial Safety in the context of cyberspace?

Financial safety means protecting one's money, identity, and data from cyber-enabled crimes such as phishing, fake investment schemes, or unauthorized access. It involves responsible online behavior, awareness, and secure use of digital tools.

4. What are some common cyber threats that affect financial users?

Common threats include phishing emails or messages, card skimming, UPI and QR code frauds, identity theft, ransomware, fake loan apps, and social engineering scams that trick users into sharing personal details.

5. How can individuals strengthen their personal cyber resilience?

- Use strong and unique passwords for all accounts.
- Enable two-factor authentication.
- Avoid clicking unknown links or downloading attachments.
- Keep devices and software updated.

Regularly monitor bank statements and transaction alerts.

FREQUENTLY ASKED QUESTIONS

6. What steps should be taken immediately if someone experiences online financial fraud?

Report the fraud to the bank or payment provider, block the affected account or card, and register the complaint at the National Cybercrime Reporting Portal (www.cybercrime.gov.in) or by calling 1930. Collect and save all relevant evidence.

7. How can financial institutions enhance their cyber resilience?

They can adopt advanced fraud detection systems, conduct regular security audits, train employees and customers on safe digital practices, and maintain strong encryption and incident response protocols.

8. What role does awareness play in preventing financial cybercrime?

Awareness empowers users to recognize and avoid scams. Many frauds occur due to human error or lack of caution. Educated and alert users form the strongest defense against cybercriminals.

9. What are some national efforts to promote cyber safety and resilience?

Government programs such as Cyber Surakshit Bharat, Digital India, and various public advisories promote secure digital practices, financial literacy, and responsible use of technology across the country.

10. How does cyber resilience contribute to national and economic security?

A resilient cyber and financial ecosystem safeguards citizens, protects national infrastructure, and sustains economic growth. It ensures that digital progress continues securely, even in the face of evolving cyber threats.