वित्तीय सेवाएं विभाग
DEPARTMENT OF
FINANCIAL SERVICES

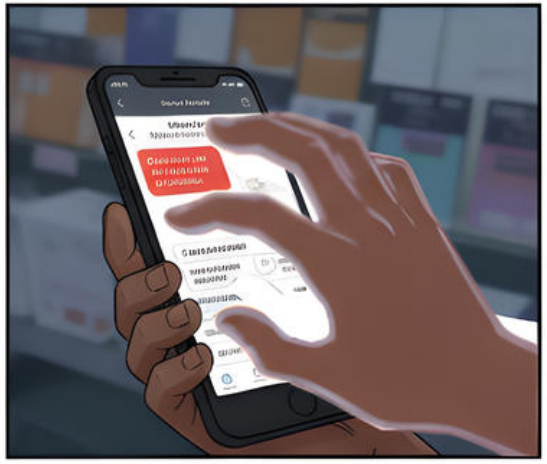
CyberPeace

Cyber Resilience
Financial Safety

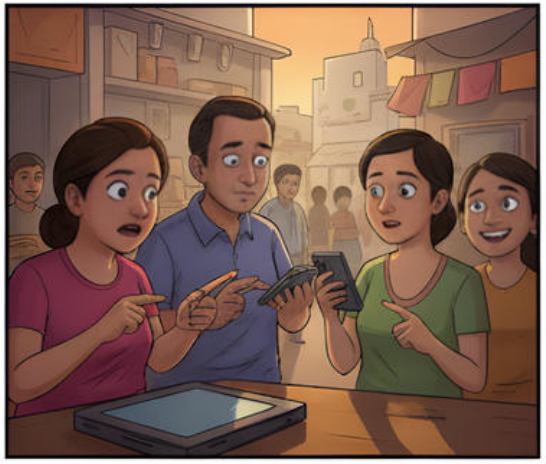
Learn More

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.

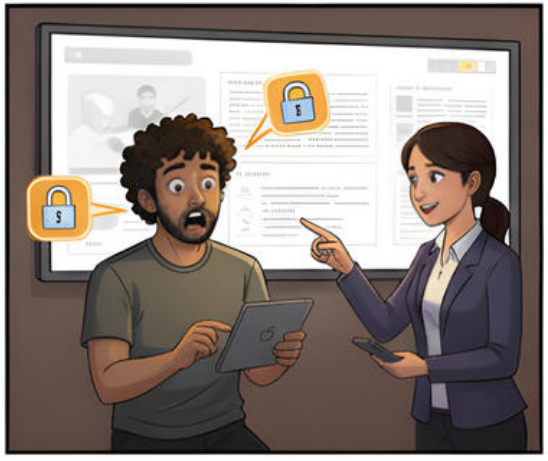


Cybersecurity is crucial to protect financial data, business assets, and customer information from cyber threats.



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

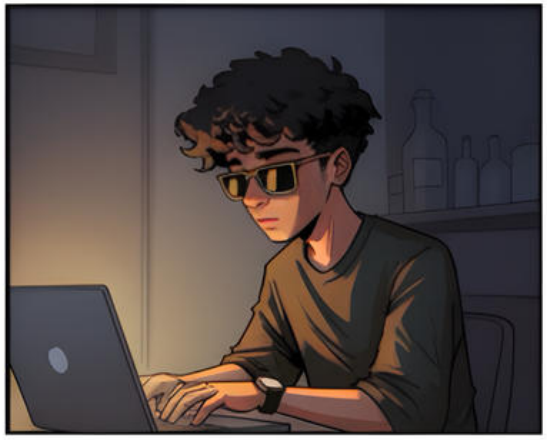
As cyber threats continue to evolve, businesses must stay alert and adapt.



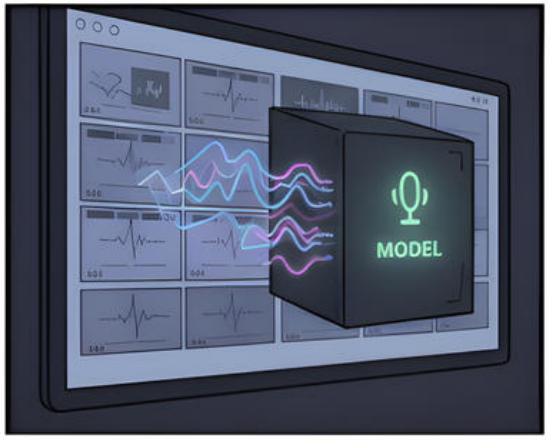
Invest in cybersecurity awareness, implement strong authentication, and ensure compliance with data protection laws.

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

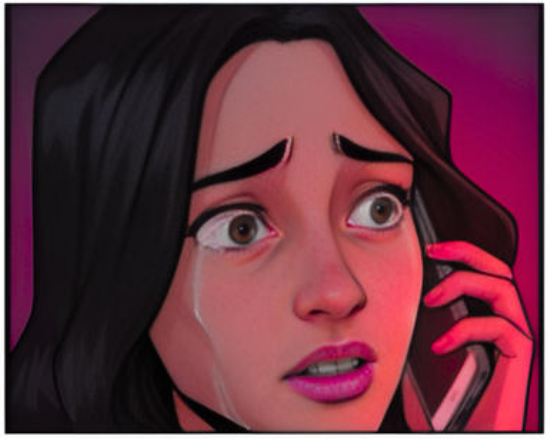
AI VOICE CLONING



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

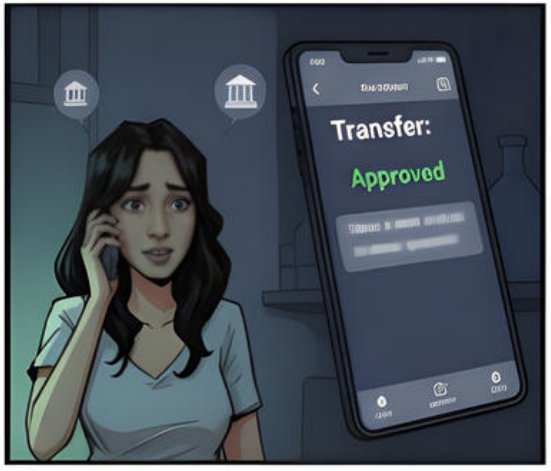


An AI model learns the voice's patterns tone, pace, timbre in a black-box process."



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

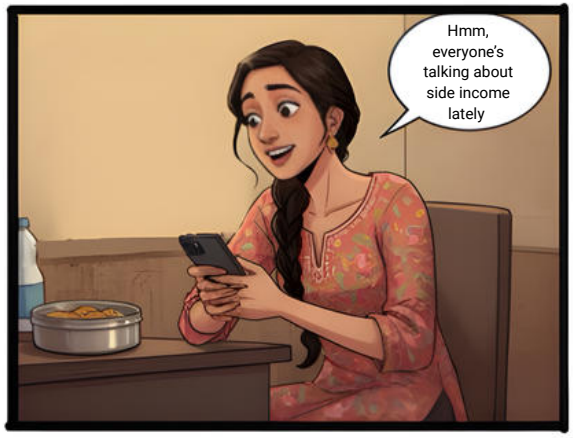
The trick isn't just sound it's timing, urgency, and familiarity.



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

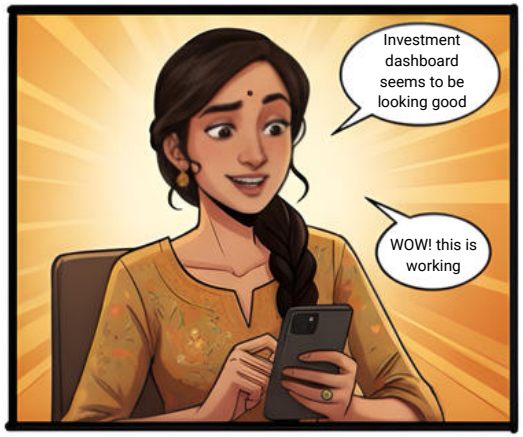
Never act on urgent voice-only requests; always verify via a second trusted channel, use transaction checks with separate-device OTPs, and immediately report suspicious calls to your bank and cybercrime authorities.

INVESTMENT FRAUD

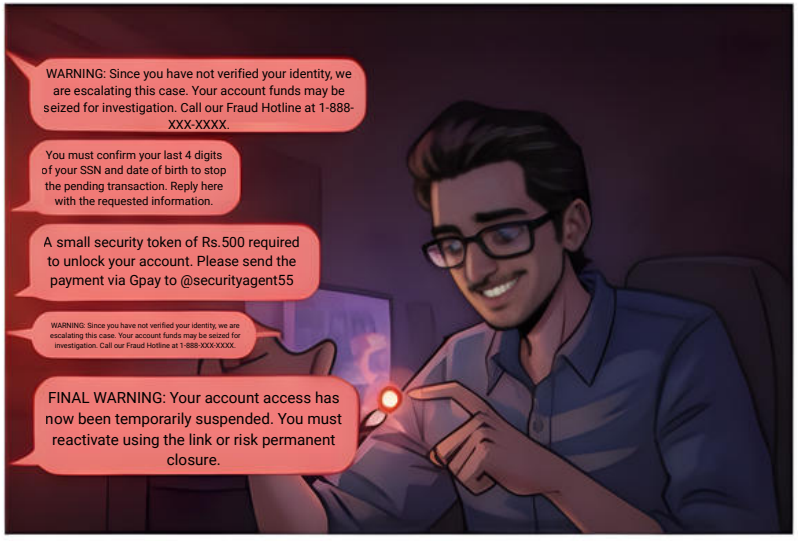


Scams don't always look shady. They look meticulously designed.

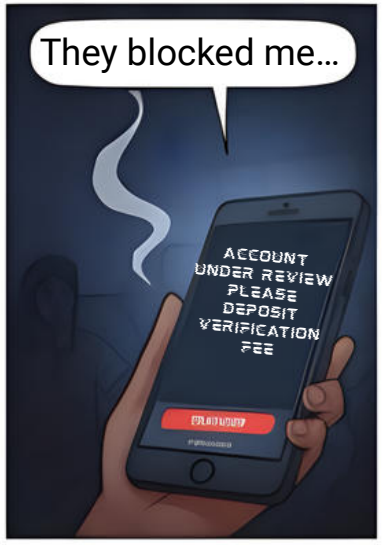
The fraudster builds credibility fake certificates, testimonials, even small early 'profits



Nothing hooks faster than seeing numbers rise.



& Urgency kills judgment.



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

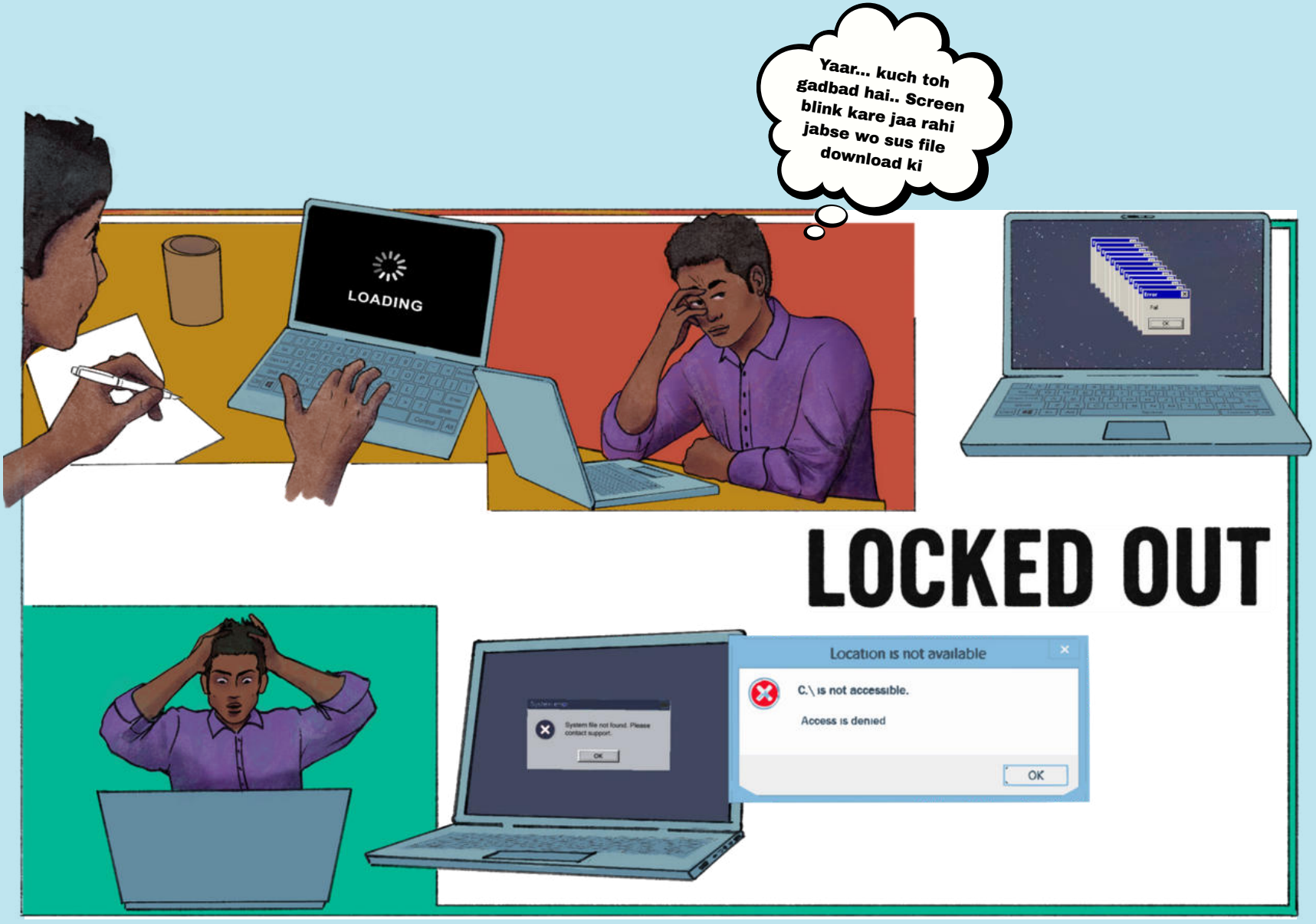
Real investments don't ask for secrecy, pressure, or direct transfers

वित्तीय सेवाएं विभाग
DEPARTMENT OF
FINANCIAL SERVICES

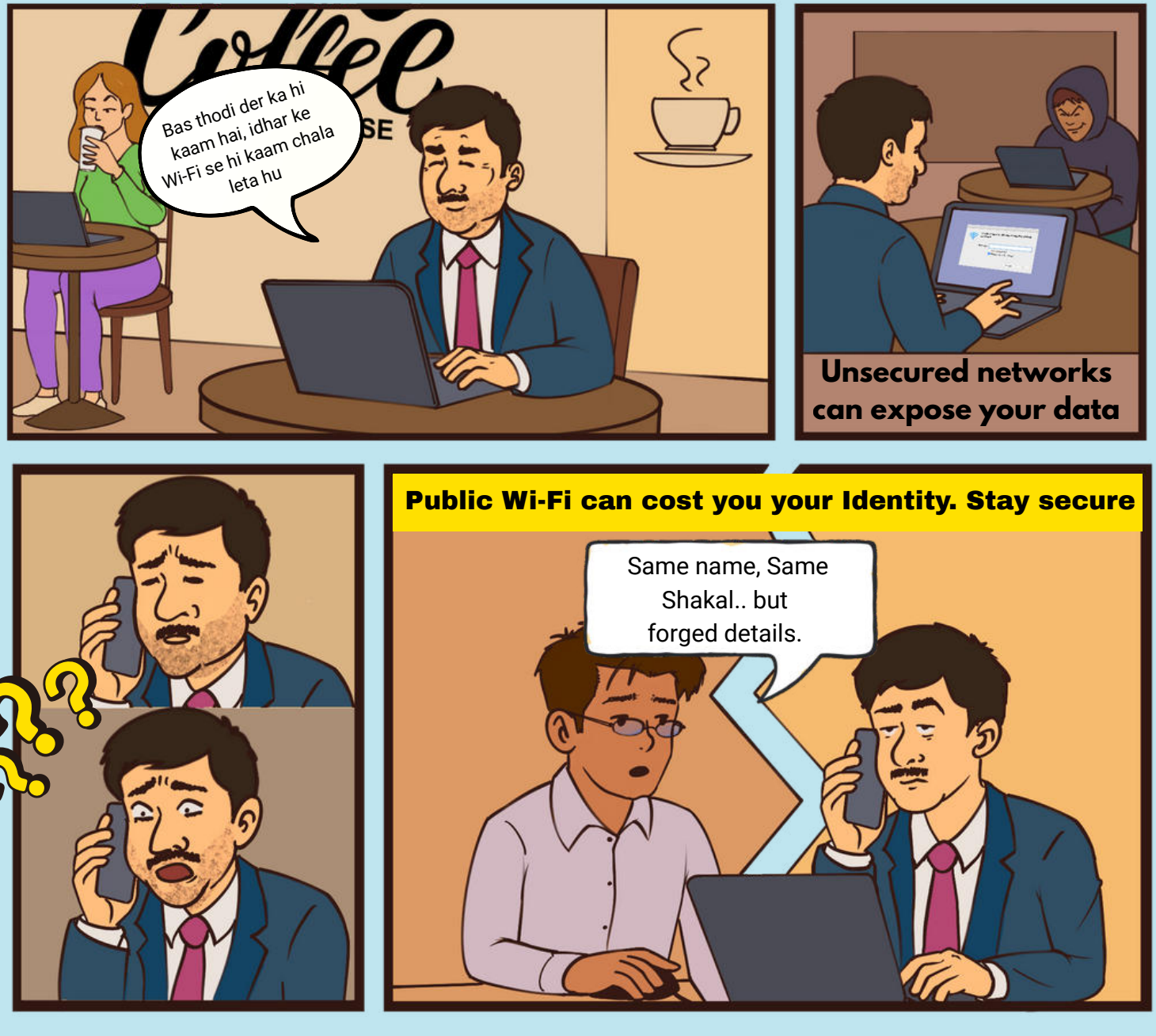
CyberPeace

QR CODE SCAM

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.

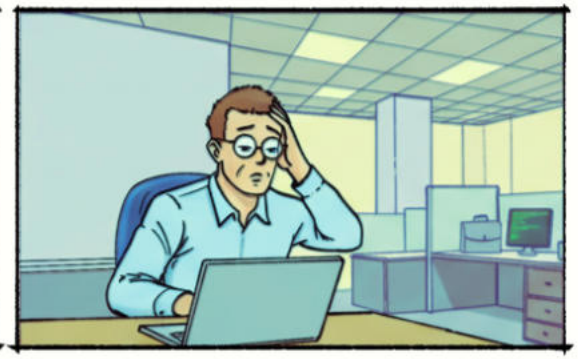
The employee realizes too late, data is already being stolen!

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

SUPPLY CHAIN ATTACKS

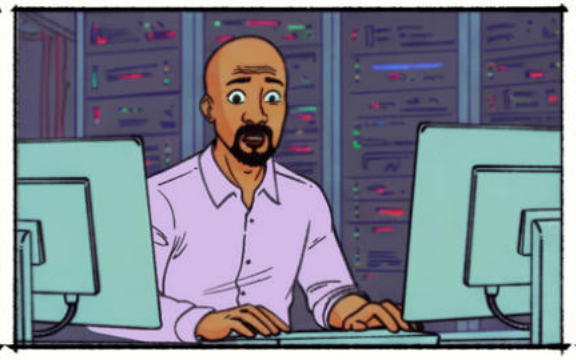
It started like any other day... a routine software update, from a trusted vendor.

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



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

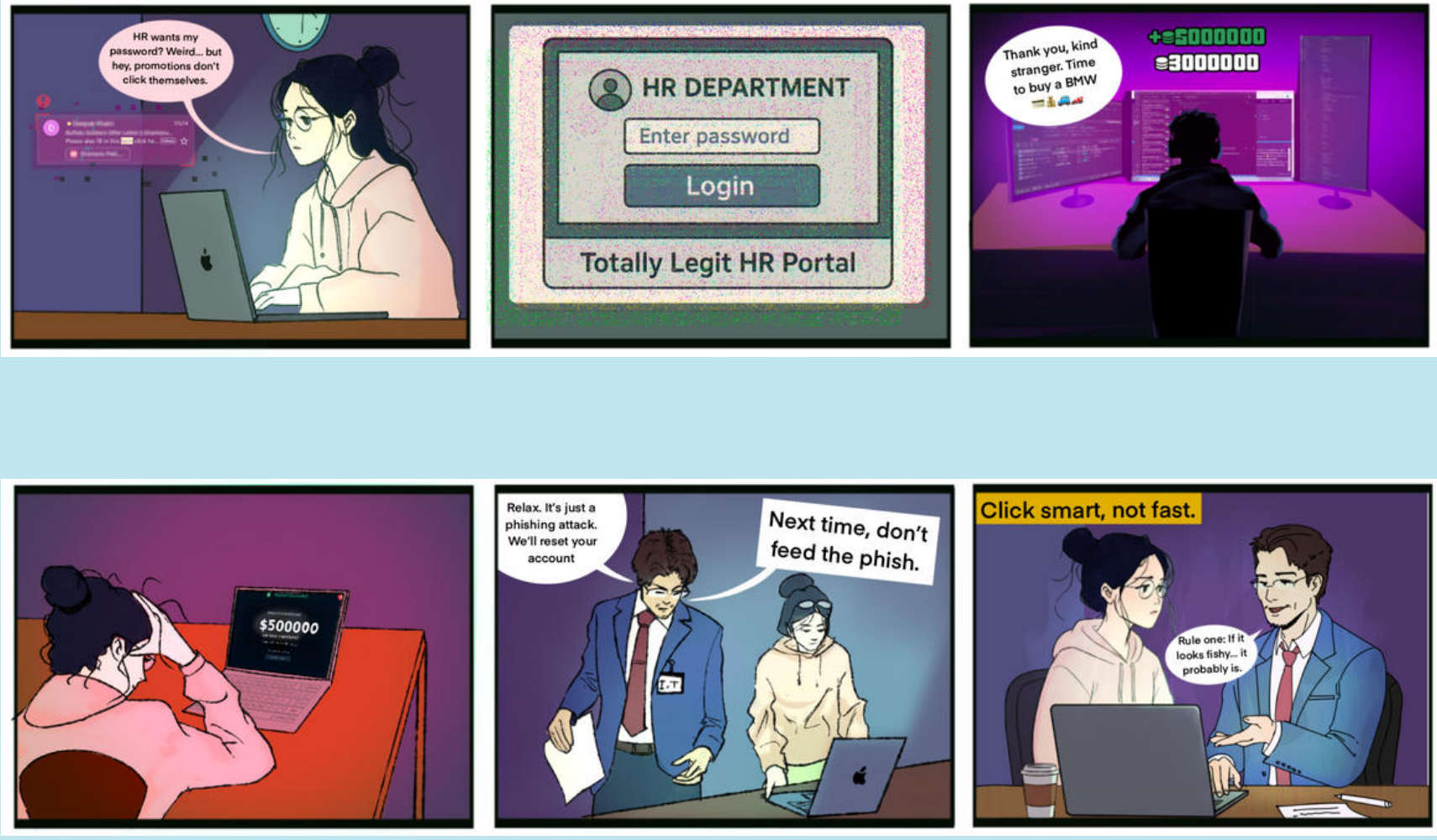
The IT team rushed to respond — but the damage was already done.



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

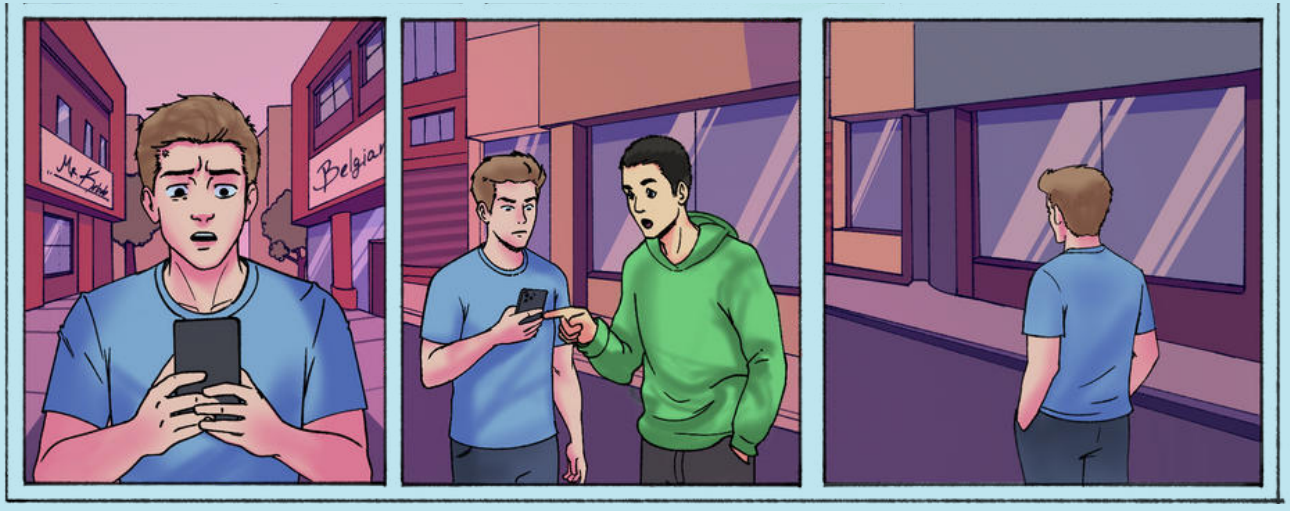

HR wants my password? Weird... but hey, promotions don't click themselves.
HR DEPARTMENT
Enter password
Login
Totally Legit HR Portal
Thank you, kind stranger. Time to buy a BMW
+$5000000
$3000000
$500000
Relax. It's just a phishing attack. We'll reset your account
Next time, don't feed the phish.
Click 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.

ATM FRAUD

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

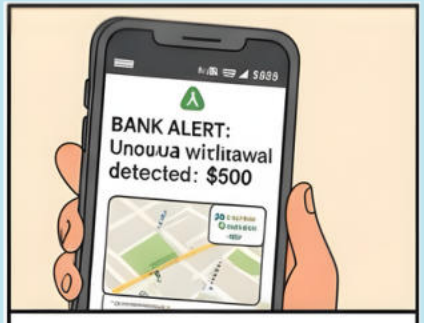
Fraudsters install devices on the card slot to steal your card details. Give the slot a tug—if it moves, don't use it.

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.



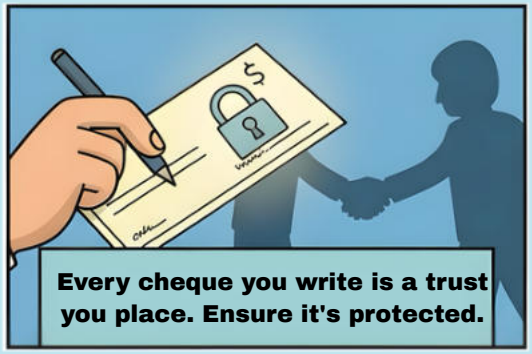
See something? Say something. Report suspicious activity or unauthorized transactions to your bank immediately.

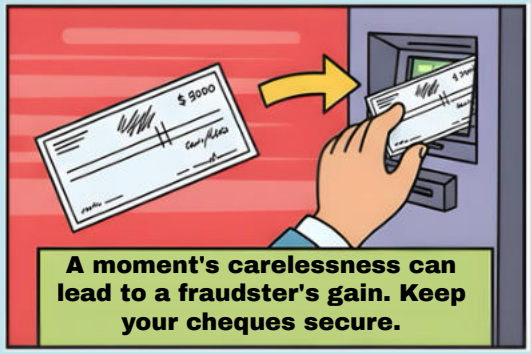
Don't wait! Report unusual devices. If an ATM looks tampered with, report it to the bank and law enforcement right away.

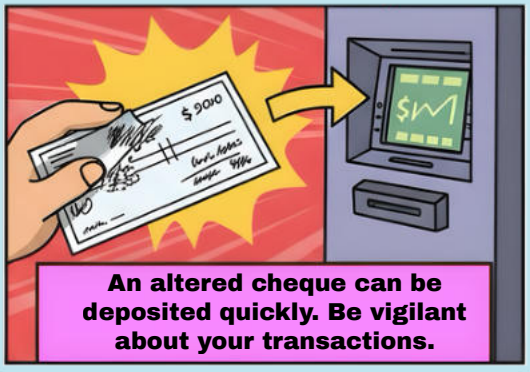
SUMMARY

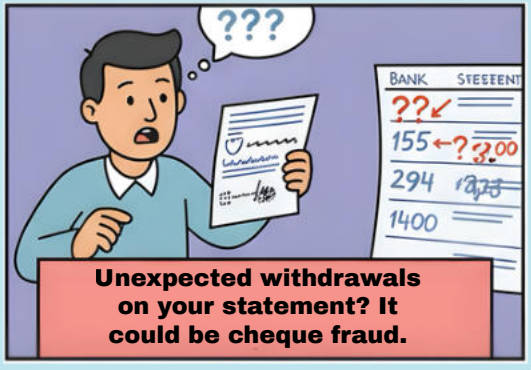
1. Use ATMS in secure, well-lit locations
2. Cover the Keypad pin
3. Check for unusual Card slots or devices
4. Enable alerts and Freeze cards whenever required

CHEQUE FRAUD









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.

Frequently Asked Questions

FREQUENTLY ASKED QUESTIONS

The Government of India has developed an accessible and comprehensive system to help citizens report and resolve cyber and financial crimes. These mechanisms are designed to ensure prompt action, transparent handling, and better protection for all digital users.

1. What is the National Cybercrime Reporting Portal (NCRP)?

The National Cybercrime Reporting Portal (NCRP) provides a unified national platform for citizens to report all types of cybercrimes, including financial fraud, identity theft, and social media misuse.
It is available round the clock at https://cybercrime.gov.in, ensuring every complaint reaches the appropriate law enforcement authority.

2. What should I do if I face online financial fraud?

If you experience a fraudulent or unauthorized transaction, take the following steps immediately:

1. Inform your bank or payment provider and report the transaction.
2. Call the National Cyber Crime Helpline (1930) or lodge a complaint at https://cybercrime.gov.in.
3. Keep an acknowledgment of your complaint for reference. Banks are required to resolve such matters within a defined period as per regulatory guidelines

3. What is the Chakshu facility and when should it be used?

Chakshu, available on the Sanchar Saathi platform, enables users to report suspicious or fraudulent communications received through calls, SMS, or messaging applications.
This includes fake messages pretending to be from banks, government departments, or relatives.
You can report such communications at https://sancharsaathi.gov.in/sfc/Home/sfc-complaint.jsp.

4. How can I report Unsolicited Commercial Communication (Spam or UCC)?

If you receive unwanted promotional or spam messages that you never consented to, you can report them within three days through the Sanchar Saathi portal at https://sancharsaathi.gov.in/sfc/Home/ucc-complaint.jsp.
You can also send SMS to 1909 to report spam calls or texts directly.

5. How can I check or report unauthorized mobile connections issued in my name?

The TAFCOP (Telecom Analytics for Fraud Management and Consumer Protection) system allows you to view all mobile connections issued in your name and report any that you did not authorize.

Visit https://tafcop.sancharsaathi.gov.in/telecomUser/ and log in with your mobile number and OTP.

6. How can I verify SMS header information or identify spam sources?

To identify the sender of an SMS or verify registered headers, visit the TRAI SMS Header Registration Portal at https://smsheader.trai.gov.in.