

Scammers hack people, not just systems

The vulnerable human layer

For decades, attackers have exploited human behaviour—curiosity, fear, urgency—to slip past even the strongest defences. Phishing emails and social engineering tactics may be old tricks, but they still work alarmingly well. Fraud exploits human instincts more than technical flaws.

The effectiveness of even the most advanced defences is shaped by a crucial factor: human judgement.

7 in 10 victims who lost money to a scam were manipulated into giving away Personally Identifiable Information (PII).¹

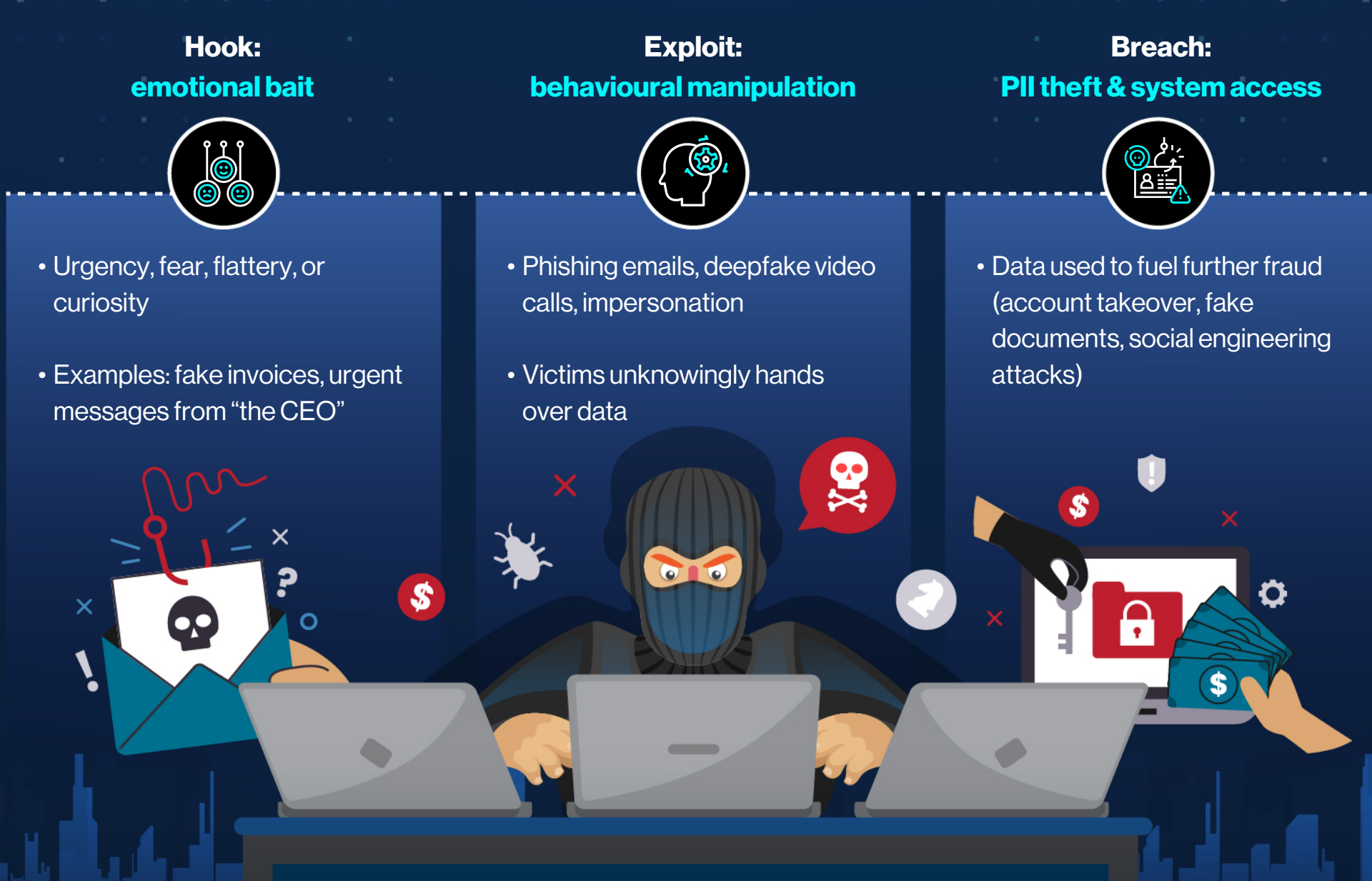
43% of stolen data is an email address. That's often all it takes to unlock your digital life.¹

Phone numbers (38%) and banking details (28%) follow close behind, giving fraudsters the keys to both financial and non-financial accounts.¹

Phishing attempts surged by **76% in 2024.**²

The scam lifecycle

No matter how secure your infrastructure is, it takes just one click and one moment of trust to break through. A phone number or email can become the digital key to your systems.



What's at stake

The cost of fraud goes beyond stolen funds or leaked data. It disrupts teams, dents confidence, and leaves a lasting mark on reputation, making it harder to bounce back.

Globally, deepfake attacks now occur **every five minutes.**²

Fake ID and biometric fraud have risen **42% year over year.**²

A family office **lost USD \$55 million** to forged documents.³

In Singapore, a finance director was nearly duped into transferring **SGD 670,000** in a deepfake scam.³

Cutting the chain with SingVerify

Scams rely on human input—clicking a link, entering an OTP, trusting a voice. SingVerify breaks that chain. Removing vulnerable steps like passwords and codes shuts scammers out before they get in.

SingVerify works silently in the background, verifying identities through telco data in real time. It helps fight cyber crimes, protecting users without sacrificing seamless customer experience.



SingVerify API ecosystem snapshot

58% of organisations are concerned that implementing stricter controls might have a negative impact on user experience.³ SingVerify proves it doesn't have to. Its basket of APIs works quietly in the background—detecting fraud, verifying identity, and protecting users without adding more steps.

Number Verify API

Authenticates digital identities by confirming if the device's phone number matches the declared number, enhancing security without relying on OTPs or passwords.

Device Location API

Verifies if a mobile device is near a specified location, aiding in fraud prevention by confirming the proximity of the device to expected locations.

Scam Sniffer API

Detects ongoing calls and unusually lengthy calls during large transactions, helping to identify and prevent Authorised Push Payment (APP) frauds.

Protect people to protect your business

Strong systems aren't enough if the people using them remain exposed. Resilient businesses start with smart, silent authentication that protects users without slowing them down.

SingVerify helps combat cybercrime without slowing you down by making authentication silent and secure. For decision-makers, it's beyond a security upgrade. It's a strategic move toward lasting business resilience.

Cyber threats target people. Equip yours to stay secure.

[Discover SingVerify](#)

References

- ¹ Javelin Strategy & Research, Compromised Today, Exploited Tomorrow: Innovation Can Stop the Fraud Cycle, 2025
- ² SDX Central, AuthenticID report reveals a surge in identity-based fraud across businesses, 2025
- ³ SecurityBrief, Identity fraud costs firms USD \$7 million annually worldwide, 2025