Singtel

Do you know where your data is? **Combatting digital fraud with Telco APIs**

Personal data is a treasure trove of critical and sensitive information, which is a hot commodity in the eyes of cybercriminals.

In the wrong hands, a customer's personally identifiable information (PII) can be abused to launch targeted attacks, which can have costly consequences for businesses. Explore how SingVerify can help financial organisations fight digital fraud and keep their clients' data secure.

What is digital fraud?

Digital fraud, also referred to as online or internet fraud, occurs when cybercriminals steal personal data or scam victims into giving them money via illicit ways, including the use of malware and social engineering schemes.[1]

The most common types of digital fraud include[2]:

Denial of service (DoS)

Threat actors interrupt access to an online service, system, or network for malicious purposes.

Data breach

Cybercriminals steal confidential and critical data from users and organisations for ill gain.

Malware

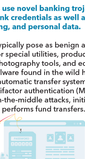
Cybercriminals launch attacks on users and organisations to steal personal and sensitive data.

Phishing and spoofing

Malicious actors use email and online messaging platforms to fool victims into giving them PII, login credentials, or financial details.

Business email compromise

Malicious actors target organisations that frequently make wire payments. This scam compromises legitimate email accounts via social engineering tactics to make unauthorised payments straight to cybercriminals.



Ransomware

Attackers use ransomware, a type of malware, that prevents users and organisations from accessing critical data if a ransom amount is not paid.

How digital fraud is evolving

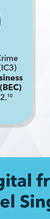
Innovation is the name of the game when it comes to digital fraud. Cybercriminals are upping the ante by launching evolved versions of scams that focus on high-stakes targets.

The following are new digital fraud attacks that can be used by malicious actors to target financial institutions:

QR phishing or quishing[3]

Scammers use QR codes to distribute malicious URLs in targeted emails. With this attack, cybercriminals can launch phishing campaigns without being flagged by email security solutions.

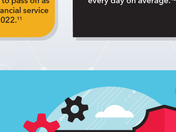
Scammers can impersonate banking institutions and send malicious QR codes that lead to a phishing site. Victims who input their banking credentials on the fraudulent site will unwittingly hand them over to malicious actors.



New banking malware[4]

Malicious actors use novel banking trojans to steal victims' bank credentials as well as social media, messaging, and personal data.

These malware typically pose as benign apps, including ones for special utilities, productivity, entertainment, photography tools, and education. New banking malware found in the wild has been seen to have an automatic transfer system (ATS) that collects multifactor authentication (MFA) tokens for man-in-the-middle attacks, initiates transactions, and performs fund transfers.



Virtual credit card fraud[5, 6]

A virtual credit card (VCC) is a digital version of a physical credit card that has a disposable number – one that differs from the number on the physical card. VCCs are useful for online transactions and are meant to provide an extra layer of protection against fraud and data breaches.

However, cybercriminals have already found a way to compromise VCCs: Cybercriminals employ SMS spoofing to make the message appear to be coming from the bank, inform the victim that someone from the bank will call them, and send a fake security code that the cybercriminal will provide during the call. During the call, the scammer will ask for the victim's credentials to address the fake VCC issue on their end. The scammer can then use the stolen credentials for nefarious purposes.

Fraud in numbers

The following concerning numbers highlight how important it is for banks and financial organisations to stay protected against digital fraud:

The financial services industry is the **second-most targeted industry** by cyber security incidents resulting in data compromise.[7]

The global average cost per data breach amounted to **US$4.45M** in 2023.[8]

The number of ransomware attacks in financial services rose to **64% in 2023** from 55% in 2022.[9]

The FBI's Internet Crime Complaint Center (IC3) received **21,832 Business email compromise (BEC)** complaints in 2022.[10]

According to Singapore's Cyber Security Agency (CSA), more than **80% of phishing sites** attempted to pass off as banking and financial service sites in 2022.[11]

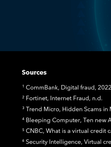
Google blocks **15 billion** spam, phishing, and malware-laden emails every day on average.[12]

Thwart digital fraud with Singtel SingVerify

Financial institutions can leverage Application Programming Interfaces (APIs) to improve their fraud prevention and detection capabilities via enhanced authentication. With APIs, organisations can easily see, analyse, and scrutinise transactions in real-time.

SingVerify is an authentication solution that helps enterprises enhance their cybersecurity posture and mitigate scams. It's an effective tool to enhance existing authentication processes and minimise the human risk in authentication. This solution gives businesses access to a basket of APIs, allowing them to verify a customer's digital identity through real-time telco network data.

Provides a seamless approach to authenticating digital identities through the mobile network. It confirms whether the user's mobile number accessing the service matches the declared mobile phone number.



Number Verify

Number Verify minimises the human risk in authentication, preventing hackers from hijacking the authentication process via man-in-the-middle attacks. This can be used to authenticate and stop fraudulent online transactions.

Allows enterprises to verify if a mobile device is near a specified location by informing organisations if a device's location is within the accuracy range of the MSISDN's last known location.

Device Location

Device Location can easily allow financial institutions to see if a transaction, bank withdrawal, or credit card usage emanates from an unexpected location.

Empowers businesses to verify if users are on calls and detect unusually lengthy calls during large bank transactions, which could potentially signal Authorised Push Payment (APP) frauds.

Scam Sniffer

With Scam Sniffer, clients of financial institutions can be protected against APP scams, or ones that use social engineering tactics to deceive users from authorising or "pushing" fraudulent money transfers.

Learn how SingVerify can secure your business.

Contact us

Sources

[1] CommBank, Digital fraud, 2022.
[2] Fortinet, Internet Fraud, n.d.
[3] Trend Micro, Hidden Scams in Malicious Scans: How to Use QR Codes Safely, 2022.
[4] Bleeping Computer, Ten new Android banking trojans targeted 985 bank apps in 2023, 2023.
[5] CNBC, What is a virtual credit card — and how do you get one?, 2024.
[6] Security Intelligence, Virtual credit card fraud: An old scam reinvented, 2023.
[7] Statista, Number of cases of data violation due to cyber attacks in financial services industry in the United States from 2019 to 2023, 2024.
[8] Statista, Average cost of a data breach worldwide from 2014 to 2023 (in million U.S. dollars), 2023.
[9] Sophos, The State of Ransomware in Financial Services 2023, 2024.
[10] US Bank, Business email compromise: The ABCs of BEC, 2023.
[11] ZDNet, Ransomware and phishing attacks continue to plague businesses in Singapore, 2023.
[12] Dark Reading, Google Blocks 231B Spam, Phishing Emails in Past 2 Weeks, 2022.