Cybercriminals Are Targeting Digital Identity of Singapore Citizens

21-27 minutes

Intro

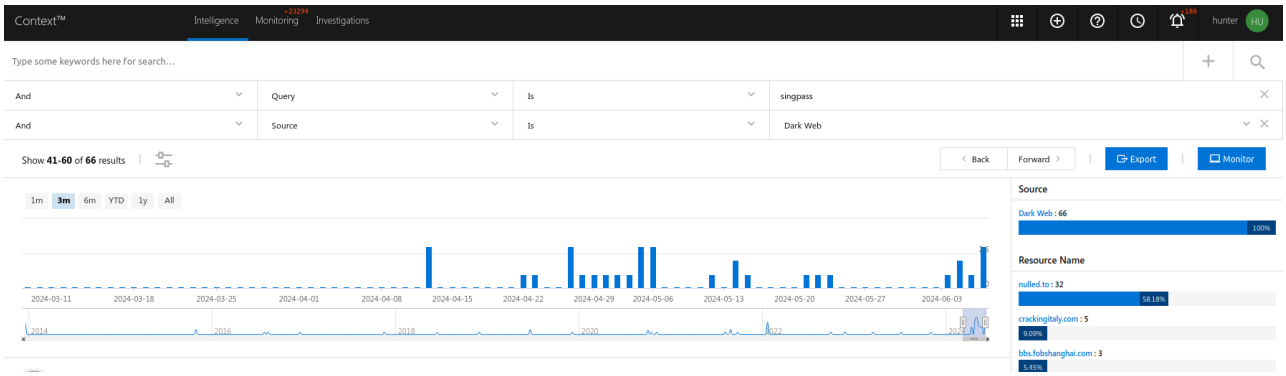
Resecurity identified a spike of Dark Web activity related to stolen identity information of Singapore citizens. Cybercriminals are selling stolen identity documents that may be used for fraud, identity theft, impersonation scams, and KYC bypass. It is crucial to detect such activity at an early stage to safeguard citizens from the risk of identity theft. By providing comprehensive Digital Identity Protection, Resecurity empowers individuals and businesses to stay one step ahead of cybercriminals. With a population of 6 million people, Singapore remains one of the leading global financial and trade hubs in the Asia-Pacific (APAC) region, attracting foreign investors and tourists from all over the world. Singapore is also known for its rapidly growing e-commerce and fintech industry, which processes millions of transactions and payment data records, making it an especially attractive target for cybercriminals.

Underground Market of Stolen Identities

Numerous instances of stolen identity information belonging to Singapore citizens and residents were found on the Dark Web. The prices for such data range from $8, with varying costs depending on the source and quality (of images). One such service was identified on XSS, a major underground forum and marketplace for stolen data. The total number of underground vendors offering stolen identity data belonging to Singapore citizens has increased by 230% compared to the previous year by the end of Q2 2024. One of the root causes is the growth of data breaches affecting consumers. Cybercriminals compromise various online platforms that store consumer information, leading to further proliferation of stolen data on the Dark Web.

The identification of the spike is based on the following metrics:

- The number of mentions of "Singpass" on the Dark Web (underground forums, communities, and invite-only Telegram groups), where cybercriminals frequently operate.
- The availability of records for sale from underground sellers; our statistics show that, starting from April 15th, 2024, we have registered a significant increase in data dumps with significant number of records (from 10,000 and more) being offered by multiple actors this month. This suggests that there have been undisclosed data breaches affecting Singapore citizens, which is why we are seeing a surge in leaked KYC documents primarily involving selfies."



The stolen data contains biometric information, such as fingerprints and facial data, of victims. This type of information is illegally reused for forged documents, access manipulation, and other malicious

scenarios leveraged by cybercriminals using Deep Fakes and AI-powered techniques for fraudulent purposes. In addition to cybercriminals, this data is highly coveted by nation-state and foreign actors conducting intelligence gathering and infiltration activities leveraging stolen identities.

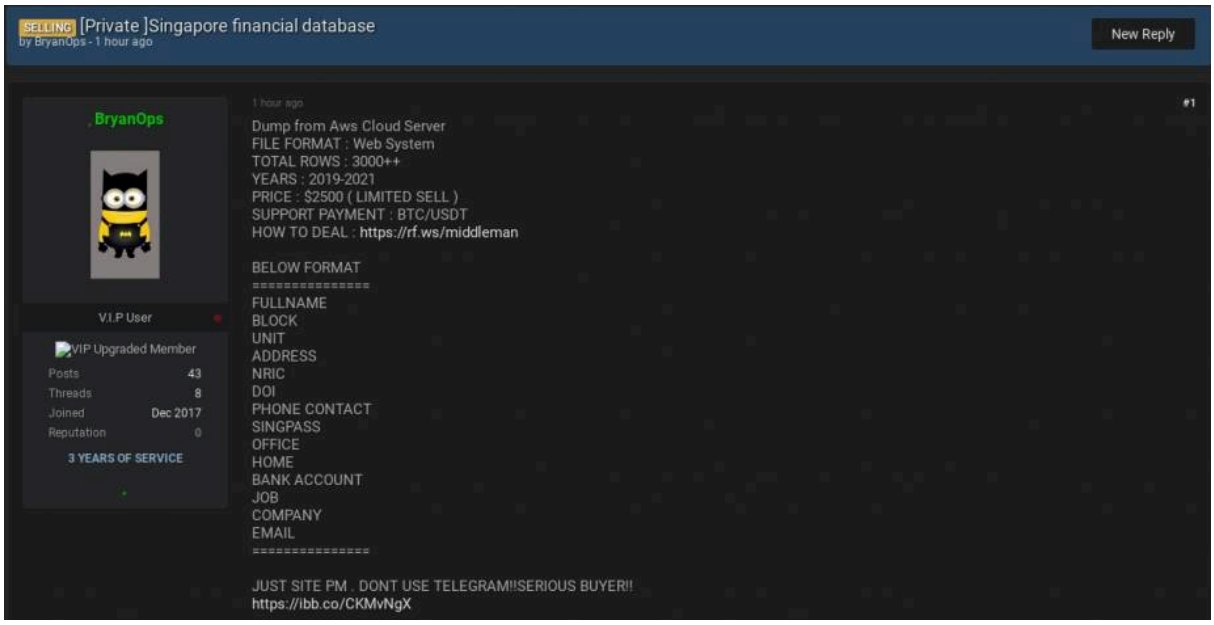
According to a previous threat research publication, Resecurity detailed how state-sponsored actors from North Korea, in collaboration with their associates, attempted to infiltrate the supply chain of major U.S.-based corporations by posing as remote IT workers with stolen identities. The Asia-Pacific region is particularly vulnerable to such scenarios, as they are increasingly common. As a result, it is crucial to identify and track stolen identities that are being traded on the Dark Web. Estimates suggest that the total number of stolen identities circulating on the Dark Web is with hundreds of thousands in Singapore and millions across the Asia-Pacific region.

Resecurity identified several major underground vendors monetizing stolen identity data from Singapore around October 2023. Examples of ads on the Dark Web included stolen identity data from Singaporean citizens, offering services such as passports, identity cards, and driving licenses (sanitized).

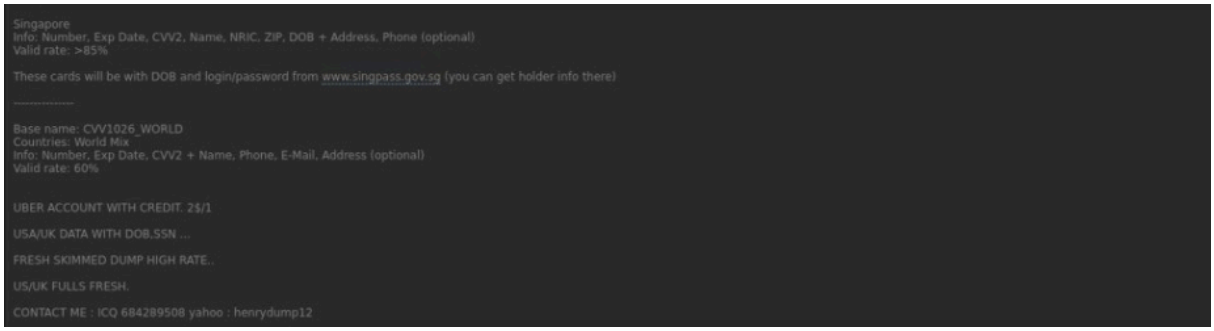
Around June 2024, several underground vendors offered for sale large volumes of compromised identity data, announcing updates. Resecurity acquired sample data sets for further analysis to identify impacted organizations and trace the leaks.

The Identity Card (IC) is a compulsory document that Singapore citizens and permanent residents must re-register for when they reach the age of 30 (before their 31st birthday) and again when they reach the age of 55 (before their 56th birthday), unless they have been issued a replacement IC within the last 10 years. Once acquired by a threat actor, it becomes a "long-lasting" product in bad hands. Notably, the expiry date is not printed on the document. With recent regulatory updates, the validity of the Singapore passport has also been increased from five years to ten years for Singapore citizens aged 16 and above. Victims typically remain unaware because the breached organizations rarely disclose the incident publicly, often due to reputation and compliance risks, and thus fail to inform them, making it difficult for victims to replace their identity documents timely.

The source of such data leaks can vary, but multiple offerings on the Dark Web have been identified, selling compromised access to sensitive data from healthcare, lending, e-commerce, and financial platforms.



Cybercriminals are also profiting from the sale of stolen Singpass credentials on the dark web.



Besides stolen documents, cybercriminals are also selling templates of national IDs, including those typically required for Know Your Customer (KYC) purposes, such as passports, driving licenses, utility bills and banking statements. Cybercriminals also provide services enabling the creation of forged documents using such templates. Notably, some of the observed templates were remarkably lifelike, featuring holograms and other advanced security features commonly used on national identification documents, such as watermarks and microprinting.

Beyond manufacturing forged documents, cybercriminals also offer verification services by helping other cybercriminals use stolen identities to pass through KYC checks and activate accounts. Financial institutions, e-commerce platforms, and fintech services typically request users to upload personal information accompanied by supporting documents and may require a selfie or physical verification. To evade detection, cybercriminals exploit vulnerabilities in the KYC process or collude with insiders within these organizations.

In addition to the threats mentioned earlier, another notable issue is leaks of identity information through third parties. For example, many fintech and e-commerce services ask users to upload documents along with a selfie as a KYC measure, which can also put their sensitive information at risk if compromised. In fact, there is no specific mandatory requirement to share a selfie, and some third-party organizations use it as per their own guidelines.

Example:

Why is selfie compulsory for Singapore-based account verification?
https://support.straitsx.com/hc/en-us/articles/4410446534553-Why-is-selfie-compulsory-for-Singapore-...

Cybercriminals are taking advantage of this vulnerability by attacking third-party providers storing KYC information. They are also employing advanced social engineering tactics to obtain this sensitive data.

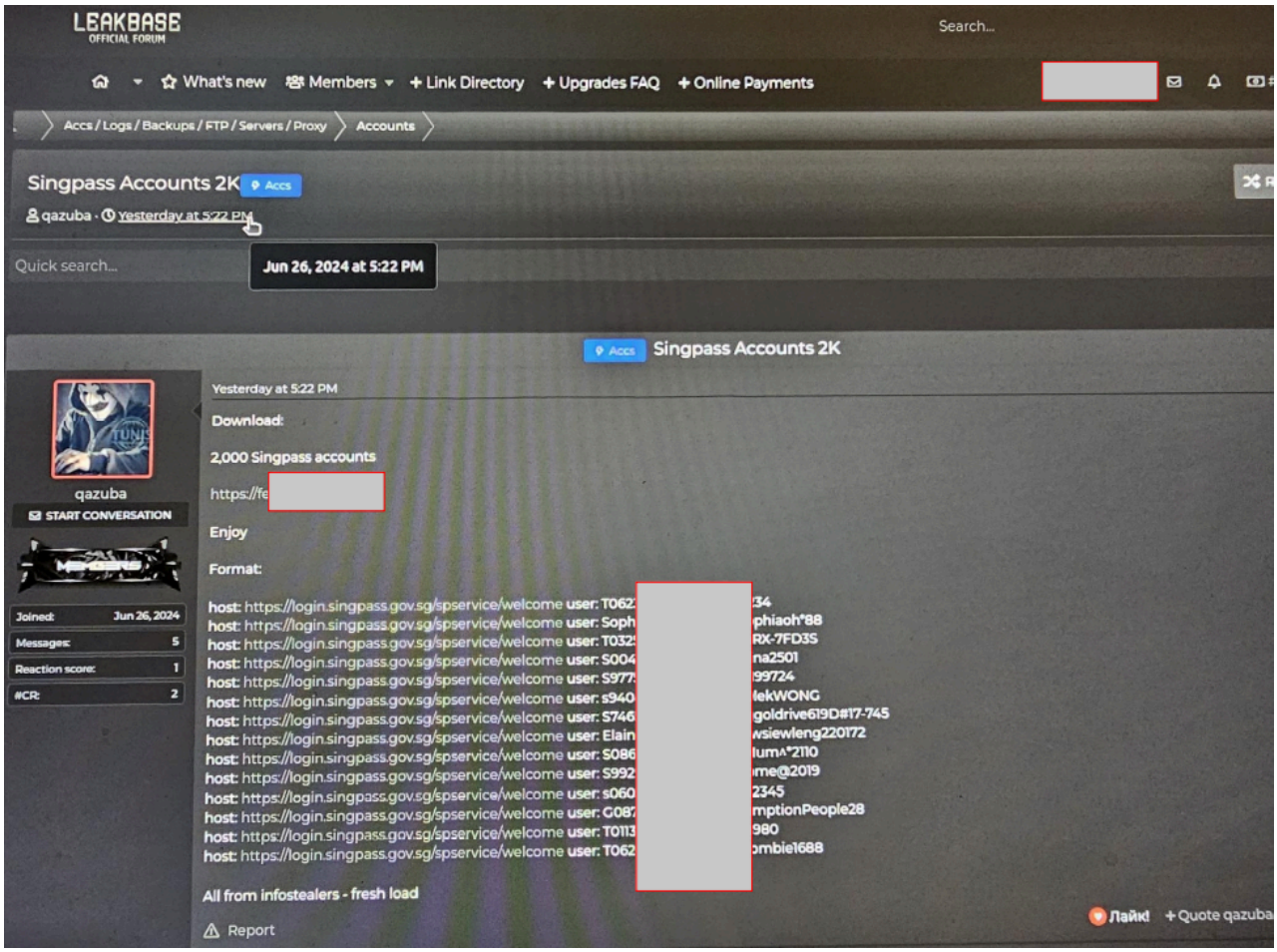
Resecurity has identified several cybercriminal groups operating illegally under the guise of telemarketing or customer support services, targeting Singapore citizens and gathering personal data on them for potential use in identity theft.

Leaks of identity information via third-party organizations collecting the information for Know Your Customer (KYC) purposes remain one of the key catalysts driving Dark Web activity and identity theft.

The Advisory Guidelines on the Personal Data Protection Act emphasize the importance of data anonymization and data minimization. The guidelines recommend leveraging these techniques to minimize data collection and storage. External providers are advised to store only the minimally necessary anonymized data attributes and instead of extracting all data from the entire database, extract only what is required. Otherwise, if breached, the third-party may put their customers at significant risk and disclose their identity information.

Singpass Accounts Circulating on the Dark Web

SingPass, which stands for Singapore Personal Access, is a trusted digital identity system used by Singapore residents. It allows individuals to securely access over 2,000 government and private sector services online and in person. SingPass serves as a convenient and secure way for Singapore citizens and residents to make transactions involving sensitive data with various government agencies. SingPass is typically used on government services websites and is required for certain transactions, such as registering a company online with the Accounting and Corporate Regulatory Authority (ACRA) through the BizFile system. The login ID for SingPass is generally the National Registration Identity Card (NRIC) of the citizen or permanent resident. SingPass is also issued to employees and dependent pass holders in Singapore. The SingPass app is available and offers features such as SafeEntry for quicker entry into locations, accessibility features for the visually impaired, and the ability to digitally sign documents. SingPass also provides 2-Factor Authentication (2FA) for e-transactions involving sensitive data.



Cybercriminals sell SingPass accounts for various reasons, primarily to facilitate illegal activities such as scams, money laundering, and identity theft. The anonymity offered by the dark web makes it attractive for such transactions. Here are some reasons why cybercriminals engage in the sale of SingPass accounts:

1. Facilitating scams: SingPass accounts can be used to carry out scams targeting individuals and organizations. By gaining unauthorized access to SingPass accounts, cybercriminals can exploit personal information, financial data, and government services to deceive and defraud victims.

2. Money laundering: Stolen SingPass accounts can be used to open bank accounts that serve as conduits for money laundering activities. Cybercriminals can transfer illicit funds through these accounts, making it difficult to trace the origin of the money.

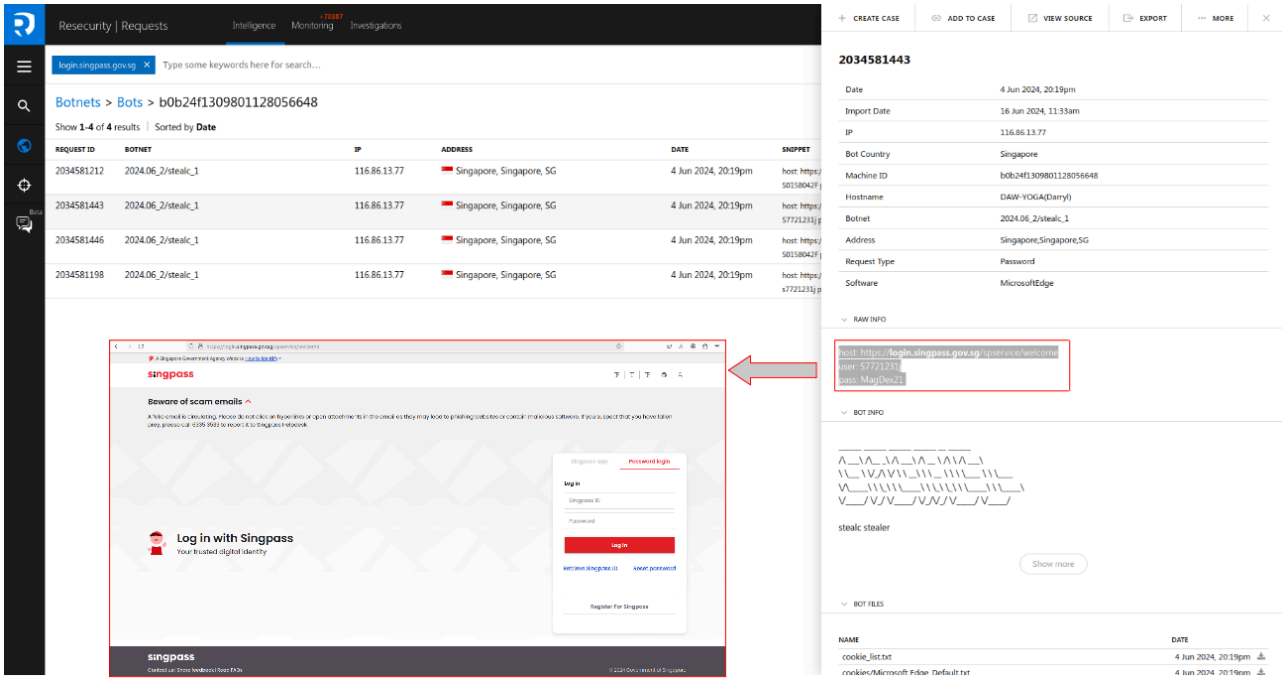
3. Identity theft: SingPass accounts contain sensitive personal information, including addresses, income details, and CPF account information. By obtaining access to SingPass accounts, cybercriminals can steal identities, commit financial fraud, and engage in other criminal activities.

It is important to note that the Singapore government and law enforcement agencies are actively working to combat these activities. They have implemented measures to raise awareness about scams and have proposed new laws to deter individuals from sharing their SingPass accounts. The Singapore government, through GovTech, continually strengthens the SingPass system against potential breaches. They conduct cybersecurity testing and implement vulnerability discovery programs to enhance security. However, it is important for individuals to remain vigilant, as the key issue leading to Singpass accounts compromise - poor network hygiene (on consumer's side) and human element.

In addition to social engineering techniques used to compromise Singpass accounts, one of the key trends reported in Q1/Q2 2024 is the activity of infostealers targeting digital identity information. Infostealers are indeed one of the key root causes of SingPass compromise. Infostealer malware is designed to steal sensitive information, including credentials, from infected devices. This type of malware resides on an infected computer and gathers data to send it to the attacker. SingPass

credentials are a valuable target for cybercriminals because they provide access to various government and private sector services.

In June 2024, Resecurity recovered over 2,377 compromised Singpass accounts from the Dark Web and notified the affected individuals.



Infostealers are a type of malware designed to steal sensitive information from victims' computers, including login credentials, browser cookies, and other personal data. Some infostealers have been known to abuse Singpass. Here are some notable infostealers that have been associated with Singpass abuse:

1. Stealc: Stealc is an emerging infostealer that has gained popularity in recent years. It exfiltrates files one by one using POST requests on a server gate. It can collect data from web browsers, including forms and cookies, and manipulate them. Stealc is fully featured and customizable, allowing attackers to choose the data they want to steal.

2. Azorult: Azorult is a spyware that collects information by recording keystrokes and user interactions. It can steal cookies, browser autofill information, and other data from the victim's computer. Based on acquired artifacts from multiple actors, Azorult has been known to target Singpass credentials in the past.

3. Racoon: Racoon is another infostealer that has been associated with Singpass abuse. It downloads legitimate third-party DLLs to assist in stealing sensitive data. Racoon's command and control communications share similarities with other infostealers like Vidar and Mars. It has attracted the interest of cybercriminals, with multiple C2 servers and samples found in the wild.

4. Nexus: Nexus is a banking trojan that targets Android operating systems (OSes) and primarily focuses on stealing banking and finance-related information. It is a rebranded version of the S.O.V.A. banking trojan. Nexus has a variety of malicious functionalities and poses threats beyond just banking and finance. Nexus collects device information, such as phone model, OS version, IMEI, battery status, IP address, SIM card ID, and phone number.

Despite the fact that accounts may be protected by two-factor authentication, there is no guarantee of full protection, given the existence of phishing kits that can bypass 2FA. Recent threat research publications by Resecurity have described examples of phishing kits capable of bypassing two-factor authentication, which highlight the ongoing challenge of ensuring complete security for consumers:

- EvilProxy Phishing-as-a-Service with MFA Bypass Emerged in Dark Web
https://www.resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-

d...

- New V3B Phishing Kit Steals Logins and OTPs from EU Banking Users
https://www.resecurity.com/blog/article/cybercriminals-attack-banking-customers-in-eu-with-v3b-phish...

- Welcome “Frappo” – The new Phishing-as-a-Service used by Cybercriminals to attack customers of major financial institutions and online-retailers
https://www.resecurity.com/blog/article/welcome-frappo-the-new-phishing-as-a-service-used-by-cybercr...

Identity Theft and Shadow Economy

Cybercriminals use stolen digital identities for fraud by illegally acquiring personal information and using it for identity theft and other criminal activities. They typically obtain information such as social security numbers, credit card details, and date of birth, which they then use to clone credit cards, apply for loans, extort victims, or engage in other fraudulent activities.

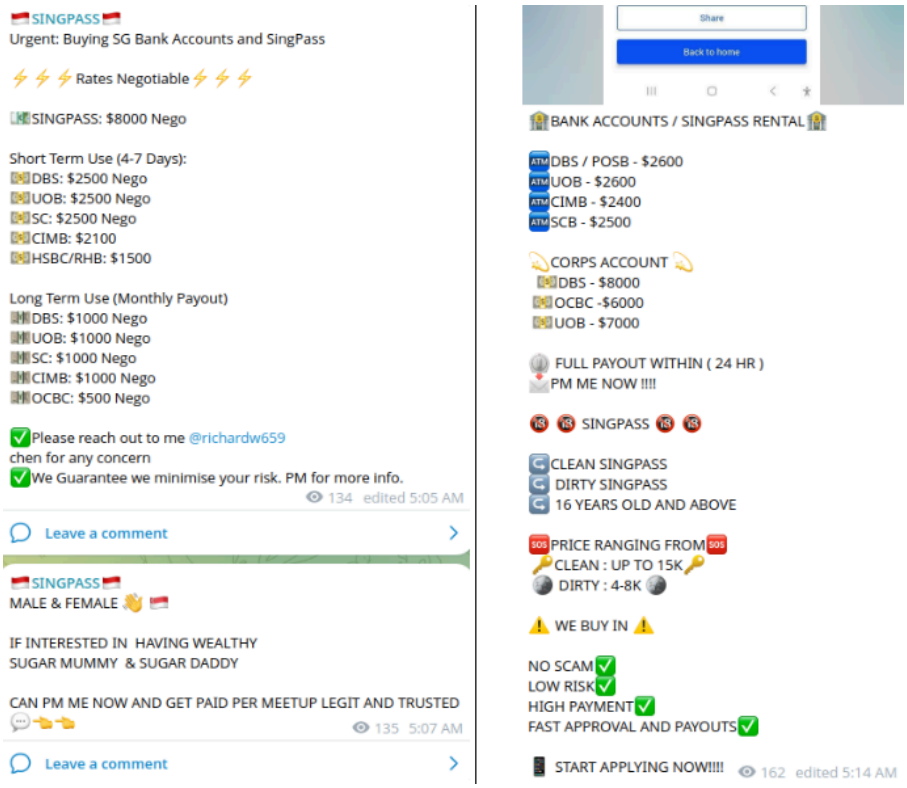
One common form of digital identity theft is credit card fraud, which accounts for a significant portion of identity theft cases. Cybercriminals use stolen credit card information to make unauthorized purchases or engage in online shopping and payment account fraud. Another type of identity theft is when cybercriminals use a minor's identity for illegal personal gains. This can involve using a child's social security number to secure employment, establish lines of credit, obtain driver's licenses, or even buy property. Cybercriminals also sell stolen data, including social security numbers and credit card numbers, on underground markets. This allows scammers to gain access to sensitive information and use it for identity fraud.

The shift towards digital platforms has made it easier for cybercriminals to carry out identity theft. They leverage stolen identity information to devise sophisticated schemes, complicating fraud mitigation efforts. With the increasing frequency of cybersecurity incidents, organizations face significant challenges in combating identity theft and other forms of cyber-fraud. It's important to note that identity theft can have long-term damaging effects on individuals whose identities have been stolen. They may suffer adverse consequences, especially if they are falsely held responsible for the perpetrator's actions.

Stolen Identity as a Catalyst of Money Laundering

One common scenario in which cybercriminals use stolen identities is money laundering. This involves tricking victims into selling their digital identity, such as a Singpass account, which is a government-issued digital identity card in Singapore. Cybercriminals then use this stolen identity to open new banking accounts, making it difficult to track and trace the illegal activities. One of the victims, Lee Jing Yu Reign sold his Singpass account which was used to open bank accounts that scammers used to launder about $220,000. A similar incident has been repeated. A teenager with three associates were charged with sharing Singpass credentials for financial gain. The victim responded to a Telegram advertisement offering him $3,000 to share his Singpass credentials. His credentials were then used to open a bank account to launder proceeds from a phishing scam.

Cybercriminals often disguise their illegal activities as lucrative opportunities to earn extra income from home. They may use online schemes or scams to make money, which can be attractive to those seeking easy ways to earn extra cash. Bad actors may offer victims a 'quick payout' in exchange for temporary access to their Singpass account. Other social engineering scenarios may include remote jobs as insurance agents or commission agents.



Resecurity helps financial institutions stay ahead of money mules, high-risk individuals, and businesses involved in illicit activities by leveraging Human Intelligence (HUMINT) and comprehensive Fraud Prevention solutions.

Money laundering poses a significant risk to financial institutions due to compliance violations and the potential for regulatory penalties, including criminal liability. Financial institutions are required to implement anti-money laundering (AML) programs and comply with regulations to prevent their businesses from being used for illicit activities. Violations of AML regulations can result in various penalties and consequences including criminal liability of the bank's officers and staff.

Cybercriminals and sophisticated fraudsters recruit insiders, such as employees of financial institutions, to assist them in carrying out attacks for financial gain. These insiders may be recruited through underground channels or coerced through blackmail using compromising information obtained from various sources. As reported by The Straits Times, last year, Singapore experienced a major money laundering incident involving over 3 billion dollars. This incident has raised concerns and highlighted the risks associated with money laundering in the country. According to reports, some of the biggest local and international banks in Singapore were embroiled in this money laundering case. Notably, a former relationship manager at one of the leading banks, was among those in the crosshairs, providing assistance to fraudsters. Court documents showed the former banker allegedly helped fraudsters liquidate cryptocurrency holdings and transfer more than $657,000 into the fraudster's banking accounts, understanding criminal nature of such illicit operations. The Monetary Authority of Singapore has taken action against financial firms found to have breached anti-money laundering rules.

While open-source information on sanctioned individuals, businesses, and PEPs is available, it is insufficient in today's threat landscape. To enhance AML controls, financial institutions should leverage cyber intelligence and conduct in-depth monitoring of dark web activity to gather intelligence on high-risk individuals, including stolen digital identity information.

Risk Mitigation

To protect employees and customers from the risks of account takeover and identity theft, businesses must implement effective Digital Identity Protection programs.

If you are a consumer and your Singpass account has been stolen, it is important to take immediate action to mitigate the risks. Here are some steps you can take to protect yourself:

1. Contact Singpass Support: The first step is to contact Singpass support to report the incident and secure your account. You can call +65 6335 3533 or email support@singpass.gov.sg for assistance.

2. Enable Two-Factor Authentication (2FA): Singpass offers a two-factor authentication feature that provides an extra layer of security for your account. Make sure to enable 2FA to protect your account from unauthorized access.

3. Change Passwords: Change the password for your Singpass account immediately. It is important to choose a strong, unique password that is not easily guessable. Avoid reusing passwords across multiple accounts to minimize the risk of further compromise.

4. Monitor Account Activity: Regularly monitor your Singpass account for any suspicious activity. Keep an eye out for unauthorized transactions or changes to your personal information. If you notice anything unusual, report it to Singpass support immediately.

5. Be Cautious of Phishing Attempts: Be vigilant for phishing attempts that may try to trick you into revealing your Singpass credentials. Avoid clicking on suspicious links or providing personal information to unknown sources. Singpass will never ask for your password or personal details via email or phone call.

6. Monitor Other Accounts: If you have used the same password for other accounts, it is important to change those passwords as well. This will help prevent unauthorized access to your other accounts in case your stolen Singpass credentials are used elsewhere.

Remember, taking prompt action and following these risk mitigation steps can help protect your personal information and minimize the potential impact of a stolen Singpass account.

To report scam-related information, the public can call the police hotline on 1800-255-0000 or submit details online at www.police.gov.sg/iwitness with the assurance of confidentiality. For more information on scams, the victims can visit www.scamalert.sg or call the anti-scam hotline on 1800-722-6688.

Previous Chapter Next Chapter