

# CYBERSECURITY BOOTCAMP CAPSTONE PROJECT

**Project Scope :** Singapore has seen an increase in the number of digital banks and financial technology (FinTech) companies

**Security Risk Analysis & Recommendations**

**By Hing Ken Wong , Steven (819Z)**



# TABLE OF CONTENTS

1. Introductions (Page 3 – 5)
2. Cybersecurity Crimes Statistical trends in Singapore (Page 6 – 12)
3. Incidents Response Management - Spoofing and Information Disclosure threats (Page 13 – 18)
4. Security Risk and Recommendation (Page 19 – 21)





# INTRODUCTIONS



# Overviews

- Banking Industry in Singapore has been transforming to a digital bank operation concept rapidly along with the State of Art Information Technology, with the aim of providing a seamless banking experience for its customers to achieve goal of customer delight and to meet ever demanding customer satisfaction needs.
- As a digital bank, which will eventually reduce the number or eliminate the presence of physical branches to further optimize the operation cost, be operating solely through its mobile and web applications. The Bank offers a range of financial products and services through its mobile and web applications.
- Customers can easily open an account with just a few clicks in the app, which is designed to be user-friendly and intuitive. The account opening process is entirely online, and customers can verify their identity through thumbprint and facial recognition technology along with Sing Pass. To ensure the security of its customers' data and transactions, Bank has implemented the latest security protocols and encryption technologies. The APP features two-factor authentication, ensuring that only authorized users can access their accounts. The bank also provides 24/7 customer support, which is available through the APP.
- As a digital bank, it is susceptible to various type and more sophisticated of cyber attack. It is mandatory for the banking sector to put up a task force to address this ongoing and will be never ending episode of cyber attack by the scammers.
- Cybersecurity risks in the Singapore banking industry include data breaches, phishing attacks, ransomware threats, and advanced persistent threats. Additionally, vulnerabilities in third-party systems, insider threats, and the increasing sophistication of cyber crimes pose ongoing challenges. Frequent security assessments, employee training, and robust incident response plans are crucial for mitigating these risks.



# The banking industry in Singapore employs various cybersecurity countermeasures to protect against threats.

These measures typically include:

1. **Firewalls and Intrusion Detection/Prevention Systems:** Implementing robust firewalls and systems to detect and prevent unauthorized access.
2. **Encryption:** Ensuring that sensitive data is encrypted to safeguard it from unauthorized access during transmission or storage.
3. **Multi-factor Authentication (MFA):** Requiring users to provide multiple forms of identification to access systems, adding an extra layer of security.
4. **Regular Security Audits:** Conducting periodic assessments and audits of systems to identify vulnerabilities and address them promptly.
5. **Employee Training:** Providing cybersecurity awareness training to staff to recognize and respond to potential threats like phishing attacks.
6. **Incident Response Plans:** Developing and regularly testing plans to respond effectively in case of a cybersecurity incident, minimizing damage and downtime.
7. **Endpoint Security:** Implementing security measures on devices (endpoints) to protect against malware, unauthorized access, and other threats.
8. **Continuous Monitoring:** Employing real-time monitoring systems to detect and respond to potential threats promptly.
9. **Collaboration with Authorities:** Collaborating with regulatory bodies and law enforcement to stay informed about emerging threats and regulatory requirements.
10. **Regular Software Updates:** Keeping all software, including security software, up-to-date to patch vulnerabilities.

However, it is important to note that the landscape of cybersecurity is dynamic, and organizations continually adapt their strategies to address evolving threats.

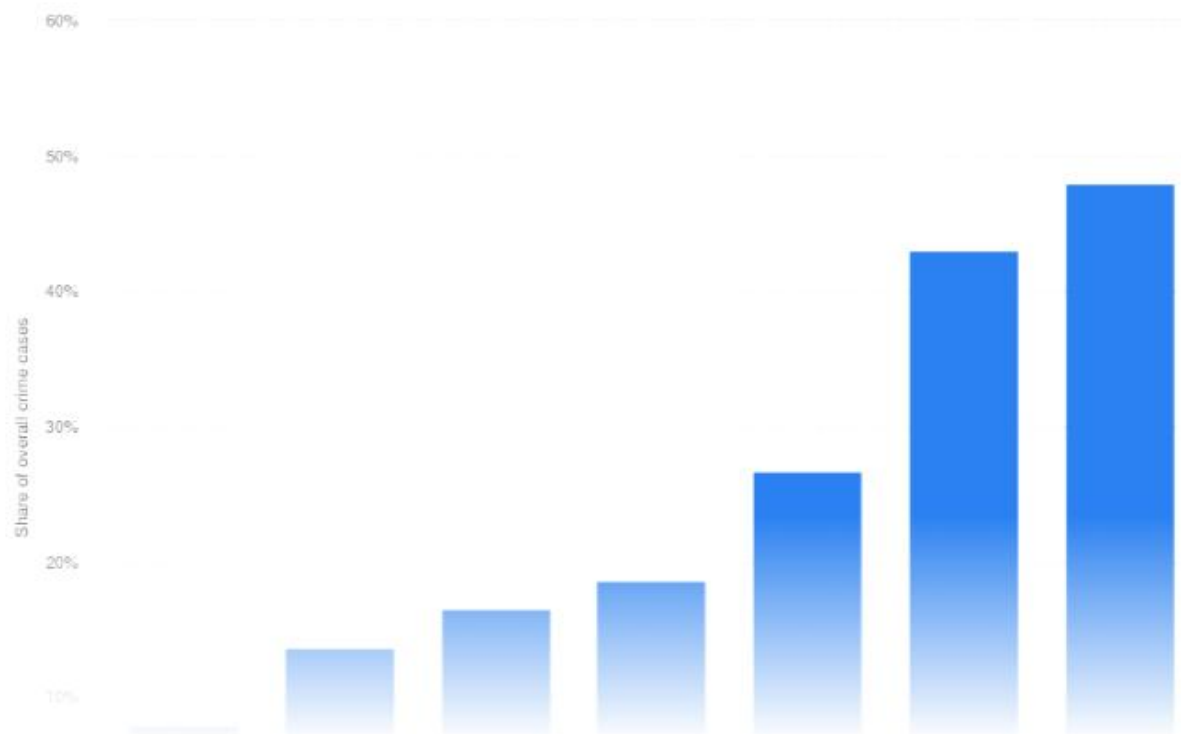




# Cybersecurity Crimes Statistical trend in Singapore



## Cybercrime as a share of total crimes in Singapore from 2014 to 2021



[Additional Information](#)

© Statista 2024

[Show source](#)

### DOWNLOAD



PDF



XLS



PNG



PPT

### Source

- [→ Show sources information](#)
- [→ Show publisher information](#)
- [→ Use Ask Statista Research Service](#)

### Release date

August 2022

### Region

Singapore

### Survey time period

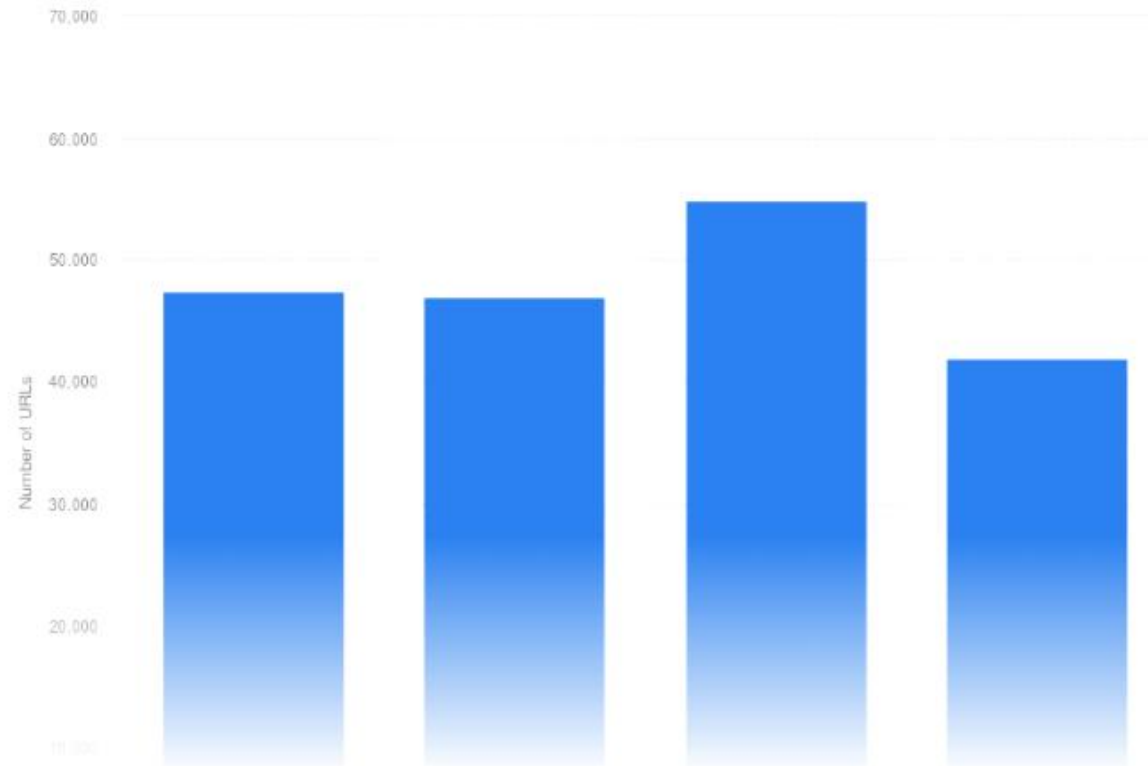
2014 to 2021

### Citation formats

- [→ View options](#)



## Number of phishing URLs detected in Singapore from 2019 to 2022



[Additional Information](#)

© Statista 2024

[Show source](#)

### DOWNLOAD



PDF



XLS



PNG



PPT



### Source

- [→ Show sources information](#)
- [→ Show publisher information](#)
- [→ Use Ask Statista Research Service](#)

### Release date

June 2023

### Region

Singapore

### Survey time period

2019 to 2022

### Supplementary notes

URLs with a ".SG" domain.

### Citation formats

- [→ View options](#)



# State of Singapore's Cyberspace



**8,500 cases**  
**174% ↑ from 2021**

(such as bit.ly) to mask their intent and track the "performance" of their phishing campaigns.

## ■ Top Spoofed Sectors:

I. The top spoofed sector was Banking and Financial Services, which made up more than 80% of all phishing attempts on organisations.

- Since 2016, it has consistently been in the top three sectors with the highest number of phishing attempts.

- They are often targeted by phishing attacks as they are trusted institutions which hold sensitive and valuable information (such as personal details and login credentials). Such information potentially allows threat actors to commit identity theft and other forms of fraud. Moreover, increasing digitalisation has expanded attack surfaces. Largely precipitated by the COVID-19 pandemic, customers have been moving to online banking in considerably larger numbers, leading to an uptick of malicious cyber activities, targeting organisations and individuals.

- June and September 2022 saw the highest number of phishing attempts from the sector. More than half of these attempts saw China-based banks spoofed. Interestingly, several of these banks — Agricultural Bank of China, Zhongyuan Bank, and China Minsheng Bank — have little to no presence in the Singapore retail banking scene

## Phishing Attempts

A form of social engineering attack, and a common avenue for scams. According to data released by the Singapore Police Force (SPF), phishing scams remains the top scam type in Singapore, with more than 7,000 reported cases in 2022 (a 41% increase from 2021).

- Close to 8,500 phishing attempts were reported to CSA in 2022. This is more than double the 3,100 cases reported in 2021, mirroring global trends. This substantial increase highlights the need for individuals and organisations to remain vigilant to guard against phishing attempts.

- **Vector:** More than 50 percent of phishing attempts involved links with the ".xyz" domain. This is likely because .xyz domain registrations are relatively cheap (as little as US\$1 compared to US\$3 for .com domains), and can be purchased by malicious actors in bulk for use as part of the same phishing campaign.

- **Format:** The average length of reported phishing links was observed to have decreased by almost half, from 44 characters in 2021 to 26 characters in 2022. This could indicate that threat actors are using URL shortener services

Number of phishing incidents reported to CSA in 2022



and are unknown to most retail banking customers in Singapore. The threat actors were likely mass-targeting victims utilising the 'spray and pray' tactic, which capitalises on anxieties and concerns over developments in China's banking sector. A sharp spike in reported phishing attempts involving China-based banks was observed, coinciding with China's rural bank scandal<sup>3</sup> in June 2022. These attempts represented nearly 50% of all banking-related phishing attempts within 2022.

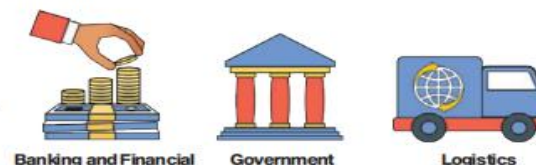
II. The second most spoofed sector was Government. The three most spoofed Singapore government-related organisations/services were the Land Transport Authority (LTA), Singpass, and Inland Revenue Authority of Singapore (IRAS). Many of these cases involved phishing emails or SMS messages exploiting the victims' trust in and tendency to comply with the authorities. The relevant

government organisations have since issued advisories through various channels to warn the public of such phishing attempts.

- There was a rising trend of phishing attempts targeting LTA from October to December 2022. These attempts used lures such as vehicle-related bills or fines, which proved compelling as a larger number of people returned to work following easing pandemic restrictions.

III. The third most spoofed sector was Logistics, with SingPost accounting for more than 80% of logistics-related phishing attempts via fake websites or SMS alerts. These phishing scams could be designed to target the online shopping habits of customers, with emails serving as fake notifications relating to incoming delivery, shipment issues, missing packages, etc.

## Most spoofed industries





## OVERVIEW OF CYBER THREATS OBSERVED IN SINGAPORE IN 2022



### Phishing Attempts: 8,500 cases

#### WHAT DOES THIS MEAN?

- As a result of CSA's consistent outreach and engagement efforts, public awareness of phishing threats is growing. More members of the public are actively reporting phishing cases to SingCERT.
- Nonetheless, the continued rise in phishing cases, both in Singapore and worldwide, highlights the need for individuals and organisations to remain vigilant.

#### KEY TRENDS

- Around **8,500 phishing attempts** handled by SingCERT in 2022, **more than double** the 3,100 cases handled in 2021, mirroring global trends<sup>1</sup>.
- Most spoofed: **Banking & Financial Services, Government, and Logistics**.

#### WHAT CAN WE DO?

- SingCERT **investigates reported cases** and reports malicious URLs to relevant parties for takedown and/or blocking, and will publish an alert/advisory if a mass phishing campaign targeting Singapore is detected.
- In 2022, SingCERT facilitated the takedown of 2,918 malicious phishing sites, and published 98 alerts and advisories.
- Individuals and organisations can do your part to keep our cyberspace safe by **reporting suspicious emails or websites via SingCERT's incident reporting form**.

### Ransomware Incidents: 132 cases

#### KEY TRENDS

- Number of reported ransomware cases remains high**, with 132 cases in 2022 (a 4% drop from 137 cases in 2021), amidst a continued growth in ransomware cases observed globally.
- Top targets: SMEs in **Manufacturing** and **Retail**.

#### WHAT CAN WE DO?

- The Government convened an inter-agency CRTF to develop recommendations that will serve as a blueprint for Singapore to counter ransomware effectively (see pages 49 to 51 for more info).
- Prevention is key to avoid falling victim to ransomware**. Organisations should take steps to secure their systems and backup critical data regularly.



#### WHAT DOES THIS MEAN?

- Ransomware remains a major issue both in Singapore and globally**, with cybersecurity vendors reporting a 13% increase in ransomware incidents worldwide in 2022.



### Infected Infrastructure: 81,500 systems

#### KEY TRENDS

- 13% **decrease** in infected infrastructure in Singapore, from 94,000 in 2021 to 81,500 in 2022, despite a sharp growth of infected infrastructure observed worldwide.
- Singapore's **global share of infected infrastructure fell** from 0.84% in 2021 to 0.34% in 2022.

#### WHAT DOES THIS MEAN?

- Marks an improvement in cyber hygiene levels. However, the absolute number of infected infrastructure in Singapore remains high. This is partly because Singapore is a data and digital cyber hub.
- The attack surface will continue to grow, as users continue to connect more smart devices to the Internet. The average number of connected devices in Singapore households grew from 6.5 in 2020 to 7.0 in 2021<sup>2</sup>.

#### WHAT CAN WE DO?

- As a responsible member of the global community, Singapore strives to prevent the abuse of our digital infrastructure. CSA regularly **informs hosting providers and Internet service providers** of reported botnet and C&C servers for their assistance with remediation.
- Individuals and organisations are reminded to **practise good cyber hygiene** to prevent their devices from being compromised and used by threat actors for malicious purposes.

### Website Defacements: 340 websites



#### KEY TRENDS

- Drop in the number of website defacements**, with 340 defacements observed in 2022 (a 19% decrease from 419 in 2021), mirroring global trends.

#### WHAT DOES THIS MEAN?

- Continued downward trend in website defacements since 2019, as hacktivist activities continue to move to other platforms with wider reach (e.g. social media).
- Nevertheless, organisations are reminded to ensure their websites are properly configured and updated to minimise the risk of website defacements as they can lead to significant reputational and brand damage.




#### WHAT CAN WE DO?

- Organisations may use CSA's Internet Hygiene Portal (IHP) to perform a free check on the cyber health of their websites**.
- Since its launch in October 2022, **the IHP has been used by both local and overseas entities to conduct more than 60,000 (12,000 unique) website and email scans, with more than 2,300 scanned domains showing an improvement** in their Internet hygiene (see page 47 for more info).

1. For comparison, based on the old reporting method, around 42,000 phishing URLs were observed in Singapore in 2022 –



## CASE 1 - Persistence of Phishing Scams



EMERGENCIES 999 | EMERGENCY SMS 71999 | HOTLINE 1800 255 0000 | I-Witness

HOME > MEDIA ROOM > NEWS > JOINT STATEMENT BY SPF AND DBS ON THE PERSISTENCE OF PHISHING SCAMS

# JOINT STATEMENT BY SPF AND DBS ON THE PERSISTENCE OF PHISHING SCAMS

NEWS

SCAMS BULLETIN

POLICE LIFE


PUBLICATIONS

SPEECHES

Amid the persistence of SMS bank phishing scams, the Police and DBS Bank would like to alert and remind members of the public that banks will never send clickable links via SMS. Since December 2023, there has been a surge in cases where scammers would impersonate banks or bank staff to phish victims' banking credentials via SMSes. In just the first two weeks of January 2024, at least 219 victims have fallen prey, with total losses amounting to at least S\$446,000.

In these cases, victims would be misled into clicking on links in unsolicited SMSes, before losing monies. In the SMSes from the purported scammers (bearing overseas numbers, local numbers, or short codes), they claimed to represent DBS/POSB bank and warn victims of "possible unauthorised attempts to access their DBS/POSB bank accounts" before urging them to click on the embedded URL links to "verify their identities and stop the transactions". After clicking on the links, the victims were directed to spoofed DBS bank websites and misled into providing their internet banking credentials and OTP, which the scammers would use to make unauthorized withdrawals.

Since early 2022, all banks have removed clickable links in emails or SMSes to retail customers. This measure is among several other safeguards that banks implemented to combat the spate of phishing scams in 2022, such as lowering the default threshold for funds transfer transaction notifications to customers and increasing the frequency of its scam education alerts.



[https://www.police.gov.sg/MediaRoom/News/20240114\\_joint\\_statement\\_by\\_spf\\_and\\_dbs\\_on\\_the\\_persistence\\_of\\_phishing\\_scams](https://www.police.gov.sg/MediaRoom/News/20240114_joint_statement_by_spf_and_dbs_on_the_persistence_of_phishing_scams)



## CASE 2 – Government Official Impersonation Scams

### Government official impersonation scams in Singapore: CPF, police say at least \$13.3 million lost in December

At least 120 people have fallen prey to the elaborate scheme, which involved victims being instructed to transfer their CPF savings to their personal accounts.



**Nisha Rahim** · News and Lifestyle Producer

Updated Thu, 1 February 2024 at 11:11 pm SGT · 3-min read



Three of these scam cases collectively lost approximately S\$488,000 in CPF savings. (Photos: Getty Images)

SINGAPORE – The police and **Central Provident Fund (CPF)** Board have issued a joint warning to the public about a **growing scam** involving the impersonation of government officials. The scammers would pretend to be bank or government officials, and convince victims to transfer their CPF savings into their personal bank accounts.

In December 2023, at least 120 individuals had fallen victim to this scheme, resulting in total losses exceeding \$13.3 million, the CPF and the police said in a press release **on Thursday (1 Feb).**

Three of these cases, which involved withdrawals made between November and December 2023, collectively lost approximately \$488,000 in CPF savings.



#### TRENDING

Counterfeit currency syndicate in Indonesia busted after fake S\$10,000 notes surface in...

Yahoo News Singap... · 2-min read

Arcade and fun fair operators in Singapore advised to inform customers about upcoming cap...

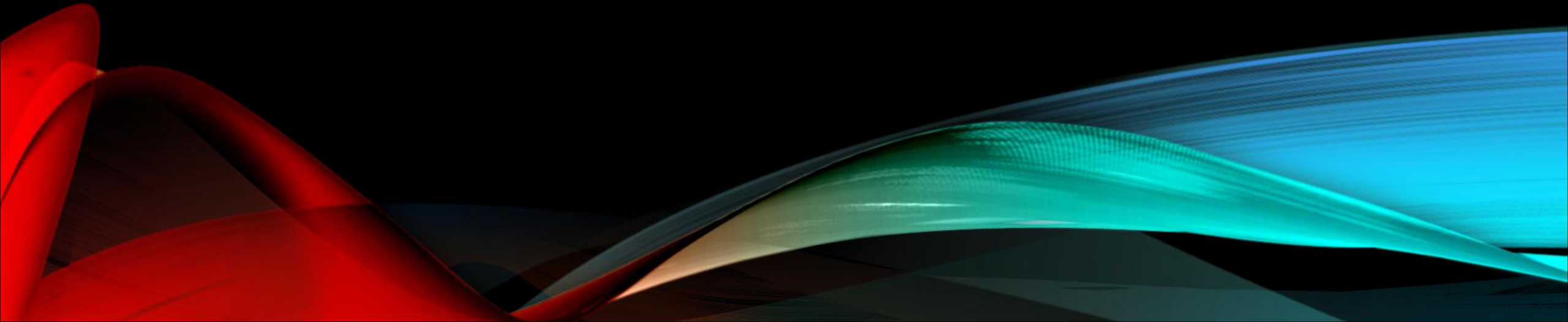
Yahoo News Singap... · 2-min read

Kim inspects warships as North



# INCIDENTS RESPONSE MANAGEMENT

(SPOOFING AND INFORMATION DISCLOSURE THREATS)





# SUMMARY

- Based on the information gathered from case 1 and 2, despite of the existing security control measures put in place, Singapore is still seeing an increase in the number of financial frauds, scams, and security incidents. In last December, at least \$13.3 million was lost related to impersonation of government official scam in which 3 of the cases collectively lost \$488,000 and in the first two weeks of 2024, at least 219 victims have fallen prey with total losses amounted to at least S\$446,000 on the persistence of Phishing scams.
- The threat so far is commonly identified as spoofing through phishing email or SMS messages and information disclosure through impersonation of government officials and the risk involved lost of funds as some of the population is unaware of the various type of scam tactics evolve from time to time.
- While the Government, MAS and police force are leading the relevant legislation and promoting the public awareness by educating and sharing the various type of scams in public periodically, there are still area for improvement can be done from the banking industry.
- Let's walk through the recent incidents report relating to Case 1 (Spoofing due to Phishing messages to the victims) and Case 2 (Information disclosure due to impersonation of government officials to the victims) resulting in lost of huge funds to the scammers from the bank account holders through their personal bank transfer activities mentioned above for a robust corrective actions.



## Section (A) Items 1 to 3

### 1. Particulars:

- Date and Time of Notification to MAS 3-Feb-24
- Full Name of Institution Vertical Bank
- Name of Caller/Reporting Staff Steven Wong
- Designation/Department Finance Manager / IT
- Contact details (e.g. email, mobile) +65 9126 6597

### 2. Details of Incident:

- Discovery date and time of incident 14-Jan-2024
- Nature of incidents, affected areas:
  - (1) **Outage of IT system** (e.g. core banking systems, ATMs, payment systems such as EFTPOS, CTS, GIRO, MEPS+, CLS etc) (1) Internet Banking Transfer
  - (2) **Signs of cyber-attack** (e.g. Hacking or malware infection against FI's system, web defacement, distributed denial of service attacks)? (2) Spoofing and information disclosure
  - (3) **Theft or Loss of Information** (e.g. sensitive/important/customer information stolen or missing from business locations) (3) Lost of funds to scammers
  - (4) **Unavailability of Infrastructure or work premises** (e.g. Power blackout, telecommunication linkages down, fire in office building and the affected locations.)? (4) NA
  - (5) **Financial** (e.g. liquidity, bank run)? (5) Lost \$446,000 through phishing with 219 victims and at least \$13.3 million of which 3 cases collectively lost \$488,000 through impersonation related information disclosure
- (5) **Unavailability of Staff** (e.g. High absenteeism or loss of staff affecting BAU due to infectious diseases, physical attack, prolonged MRT breakdowns leading to BCP activation etc)? (6) NA
- (6) **Others** (e.g. Unavailability of service providers, breach of laws and regulations)



- What actions or responses have been taken by the institution?

- (1) Launch a report with the police force department and freeze the affected bank accounts immediately.
- (2) Affected victims are advised to renew the bank account
- (3) Establish a tighter control system to monitor large funds transfer activities to seek confirmation from account holder through personal phone call
- (4) Tighten maximum fund transfer limit change by imposing 24 hours banking system approval
- (5) Seeking insurance of the lost funds from bank account holders related to scam activities

### 3. Impact Assessment (examples are given but not exhaustive):

- |   |   |
|---|---|
| • Business impact including availability of services – Treasury Services, Cash Management, Trade Finance, Branches, ATMs, Internet Banking, Clearing and Settlement activities etc. | Lost of millions of customer funds to the scammers  |
| • Stakeholders' impact – affected retail/corporate customers, affected participants including operator, settlement institution and service providers etc.                           | Bank reputation and customer dissatisfaction  |
| • Financial and market impact – Trading activities, transaction volumes and values, monetary losses, liquidity impact, bank run, withdrawal of funds etc.                           | Lost of millions of customer funds to the scammers  |
| • Reputational impact – is incident likely to attract media attention?  | Yes, large victims and funds lost incurred  |
| • Regulatory and Legal impact   | Yes, withdrawing of funds from CPF to personal banking account and transfer to third party without limit control measures |



#### 4. Detailed chronological order of events:

- |  |   |
|--|---|
| <ul style="list-style-type: none"> <li>• Date of incident, start time and duration</li> </ul>  | <p>14-Jan-2024, 20 days ago</p>   |
| <ul style="list-style-type: none"> <li>• Escalation steps taken, including approvals sought on interim measures to mitigate the event, and reasons for taking such measures</li> </ul> | <p><u>15-Jan-2024</u></p> <p>Initiate task force team to address the incidents.</p> <p>Tighten transfer maximum limit change by imposing 24 hours banking system approval so as to delay the intended transfer to gain time</p> <p>Impose bank personal call to validate maximum fund transfer limit &gt; \$50,000 request so as to review and evaluate account holder is genuine</p> |
| <ul style="list-style-type: none"> <li>• Stakeholders informed or involved</li> </ul>  | <p><u>16-Jan-2024</u></p> <p>Informed stakeholders and update incident report team to track the event development</p>   |
| <ul style="list-style-type: none"> <li>• Various channels of communications involved</li> </ul>  | <p><u>17-Jan-2024</u></p> <p>(1) Monitor and update police report upon customer feedback</p> <p>(2) Inform customers to freeze the affected bank accounts immediately.</p> <p>(3) Work with IT department to tighten transfer maximum limit change by imposing 24 hours banking system approval</p> <p>(4) Seek insurance of fund lost related to scam activities</p>                 |
| <ul style="list-style-type: none"> <li>• Rationale on the decision/activation of BCP and/or IT DR</li> </ul>   | <p><u>18-Jan-2024</u></p> <p>To prevent further fund lost to scammer due to spoofing and information disclosure related threats</p>   |



## 5. Detailed Root Cause Analysis:

- Factors that caused the problem/ reasons for occurring
- Interim measures to mitigate/resolve the issue, and reasons for taking such measures, and
- Steps identified or to be taken to address the problem in the longer term.

## 6. Final assessment and remediation:

- Conclusion on cause and effects of incident
- List the corrective actions taken to prevent future occurrences of similar types of incident
- Target date of resolution\_\_\_\_\_ (DD/MM/YY).

- (1) Bank account holders are unaware and not tuned in and educated to the various scam tactics from time to time.
- (2) The bank security measures could be more vigilant to control abnormal large funds transfer activities of any account holders.
- (1) Impose control to relax maximum money transfer limits of account holder from immediate to 24 hours approval requirement.
- (2) Impose bank personal call to validate maximum fund transfer limit > \$50,000 request so as to review and evaluate account holder is genuine or under threat
- (1) Introduce Money Lock anti-scam security feature designed to help protect customer funds. In addition to locking the funds in current/savings account(s), one can lock Time Deposit account(s) to prevent changes to maturity instructions - or any unauthorized withdrawals before each placement matures - from being made via the Vertical Bank Digital app\*

The bank account holders are unaware of the scammers tactics and had fallen prey with multimillion dollars lost

- (1) Introduce Money Lock anti-scam security feature designed to help protect customer funds.
- (2) In addition to locking the funds in current/savings account(s), one can lock Time Deposit account(s) to prevent changes to maturity instructions - or any unauthorized withdrawals before each placement matures - from being made via the Vertical Bank Digital app\*

3-Feb-2024





# **SECURITY RISK AND MANAGEMENT**



# BANKING RISK MANAGEMENT RECOMMENDATIONS

## Risk evaluation

Probability	Impact				
	Catastrophic: 5	Major: 4	Moderate: 3	Minor: 2	Negligible: 1
Frequent: 5	25	20	15	10	5
Occasional: 4	20	16	12	8	4
Remote: 3	15	12	9	6	3
Improbable: 2	10	8	6	4	2
Highly improbable: 1	5	4	3	2	1

- The impact of the recent Case 1 and 2 resulting in multi-million dollars loss were considered Major and is Frequent of varied scammer's tactics to withdraw funds from the bank account holders which has a score of 20.
  - It's mandatory for the banking industry to explore a robust security control measures to prevent more victims fallen prey and loss of huge funds to the scammers and protect the bank reputation as a secured place for their hard earn money.
- (1) Counter measures number 1: Tighten transfer maximum limit change by imposing 24-48 hours banking system approval so as to delay the intended transfer to gain time in case of there is any suspicious detected
  - (2) Counter measures number 2: Impose bank personal call to validate maximum fund transfer limit > \$10,000 per day request so as to review and evaluate account holder is genuine. (This is also applicable to CPF organisation for double protection)
  - (3) Counter measures number 3: Introduce Money Lock anti-scam security feature designed to help protect customer funds proactively. In addition to locking the funds in current/savings account(s), one can lock Time Deposit account(s) to prevent changes to maturity instructions - or any unauthorized withdrawals before each placement matures - from being made via the Vertical Bank Digital app\*



# LEGISLATION RISK MANAGEMENT RECOMMENDATIONS

- **Regulatory Framework:** Financial regulatory bodies often provide guidelines and regulations outlining the reporting requirements for cybersecurity incidents. For example, MAS in Singapore issues guidelines for financial institutions to enhance their cybersecurity resilience.
- **Incident Classification:** Organizations are typically required to classify incidents based on severity and impact. Critical incidents may need to be reported immediately, while less severe incidents may have different reporting timelines.
- **Reporting Timelines:** Regulatory bodies may specify specific timelines for reporting incidents. Timely reporting is crucial to facilitate prompt response and mitigation measures.
- **Communication Protocols:** Financial institutions usually have established communication protocols for reporting incidents to regulatory authorities, customers, and other relevant stakeholders. Clear and concise reporting helps in coordinating responses and minimizing the impact.
- **Collaboration with Authorities:** Financial institutions may be required to collaborate with law enforcement agencies, regulatory bodies, and other stakeholders during and after a cybersecurity incident. This collaboration ensures a comprehensive and effective response.
- **Post-Incident Analysis:** Financial institutions often conduct post-incident analysis and submit reports to regulatory bodies detailing the root cause, impact, and remediation measures taken. This information helps in learning from incidents and improving cybersecurity measures.

**It's essential to note that regulations and guidelines can evolve, so it's crucial for organizations to stay informed about the latest requirements from regulatory authorities and stay tune to the various scammers tactics with periodical management review to make sure that the risk is acceptable.**