Dear Mr Sid

Re: Phishing Blame in a Scam Storm

Scams are everywhere. I should know because I am chairman of a bank recently hit by a deluge. Regrettably, some of our customers have been duped, granting scammers access to their accounts and funds.

While I am sympathetic to their plights, it was their gullibility (and sometimes their greed) that allowed it to happen in the first place. Yet, instead of accepting responsibility and pursuing the fraudsters, some are demanding refunds from us. Unlike my son, who lost $50,000 as a result of a phishing email from a purported fellow doctor but accepted his misfortune with dignity and without public complaint or private grievance.

The uproar from these incidents has echoed across the media. Worse, certain "do-gooders" have gained media attention by attributing the blame for the scam pandemic to banks and holding the board and management accountable. They even suggest we should somehow be responsible for covering the losses.

Just to be clear, our bank systems are absolutely secure. We spend millions on cyber security.

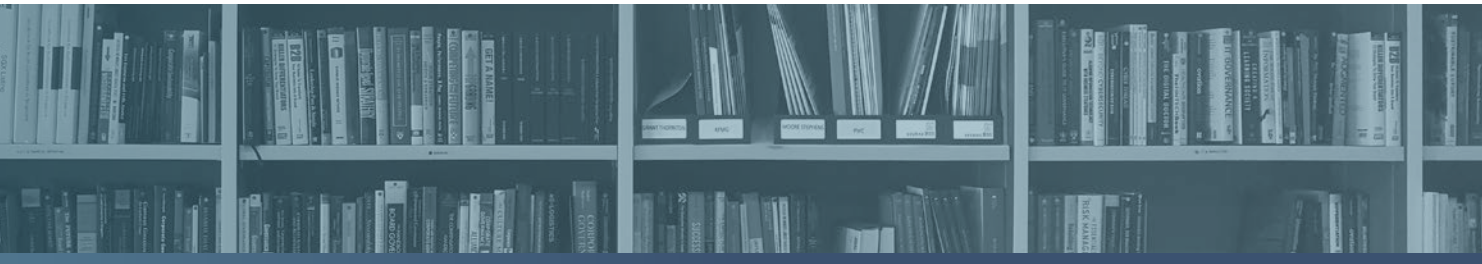
But we can't help it if our customers respond to the phishing scams. Our stance is clear: if you want the convenience of online banking, then you must be careful, sensible and alert. If you open the vault door for scammers to come in, please don't blame the vault owner!

My board members believe we should hire a public relations agency to reinforce the message that our bank is safe, even though customers sometimes are not. We aim to enhance customer education on cyber awareness, akin to the success we have seen internally. With heightened consciousness of the risks and penalties, our corporate phishing simulation exercises consistently yield a click rate below 10 per cent.

Are there any further measures you would recommend to tackle this troubling situation?

Yours sincerely

Mr Scamwise



Dear Mr Scamwise

The current scam-laden environment poses a significant concern for institutions and individuals. I empathise deeply with the unfortunate incidents that have affected your customers and even touched your own family, underscoring the indiscriminate nature of such fraud.

Understanding phishing

Allow me to delve deeper into phishing, as it is the prevalent method behind financial scams.

Phishing is the digital equivalent of social engineering, where scammers impersonate trustworthy entities to trick individuals into divulging sensitive information. Even the most astute and vigilant can fall victim. The incident where your son, a doctor, fell prey demonstrates that susceptibility transcends professional expertise and educational background. With advancements in artificial intelligence, the efficacy and complexity of scams will likely escalate.

Your bank's achievement in maintaining a phishing simulation click rate (the percentage of employees who fall victim to a phishing exercise) below 10 per cent is commendable. Yet, the best-in-class mature programmes achieve rates consistently below 5 per cent.

While click rate as a metric is useful, you should go beyond it for good cyber hygiene:

- Reporting rate: Do employees who spot phishing attempts report them to IT or security? This would be a positive sign of successful training.
- Targeted training: Do not just punish clickers. You should analyse why people fell for the simulation and provide tailored training to address these root causes.
- Behavioural change: The ultimate aim is to alter the culture and behaviours towards fraud and risks. Monitoring repeat offenders and implementing additional interventions for high-risk individuals towards this goal.

Nevertheless, the fact that the click rate may never reach zero highlights a crucial adage of cyber security: "It's not a question of if, but when."

Moral responsibility

While you hold the customers responsible for falling prey to scams and the scammers for their crimes, you seem to have absolved the bank of any responsibility.

Extending your analogy of a vault, consider a hypothetical scenario where your bank has located a branch in a high-crime neighbourhood. Although security within the bank's premises is robust, customers are vulnerable the moment they step outside. It would be overly simplistic – and indeed unfair – to blame customers for being robbed right outside the branch. Surely, you would want to provide security services for them and secure means for transporting their funds to maintain their trust and continued business.

Similarly, the bank's responsibility extends beyond its digital walls. Just as physical and other protection measures might be warranted in the high-crime scenario, digital protection and customer education are paramount in the current digital landscape.

Legal responsibility and liability

Your experience of victims, activists and the media calling for greater accountability and liability mirrors a broader global shift from moral to legal responsibility in cyber attacks.

Consider the travails of the following financial institutions in recent years:

- **Morgan Stanley** settled a class-action lawsuit for U$60 million (S$80 million) in January 2024 for a data breach affecting 15 million customers.
- **Citibank** was sued by the New York Attorney General in February 2024 for not adequately protecting customers against fraudsters who had stolen millions and for refusing to reimburse victims.
- **Medibank**, an Australian bank, is currently battling at least four class-action lawsuits over an October 2022 cyber attack that exposed the personal data of nearly 10 million customers.
- **OCBC**, after over 460 customers fell victim to an SMS phishing scam and lost S$8.5 million collectively in December 2021, opted to fully compensate the victims in "a one-off gesture of goodwill" even though it was not then legally obligated to do so.

No longer will banks be able to simply take the position that scam victims should have known better or that their customers had signed the small print absolving the institution of any blame and liability.

One emerging trend is that of a shared responsibility model mandated by regulators.

For example, in the UK, from 2024 onwards, banks and other payment service providers are required to reimburse their customers who fall victim to authorised push payment fraud if certain conditions are met.

Australia and the European Union are in various stages of schemes for sharing losses or reimbursement to scam victims.

In Singapore, the Monetary Authority of Singapore and the Infocomm Media Development Authority introduced a Shared Responsibility Framework whereby financial institutions and telecom companies would have to compensate their customers for lapses in their prescribed duties to protect customers from phishing scams. Singapore is the first country to include telecom companies in the loss-sharing framework, which was proposed in October 2023 and set to be implemented in the first half of 2024.

Scam wisdom

Being wise to scams does not mean just knowing how they work and who to blame. It should also mean taking measures to prevent scams, support victims and help them recover. These include:

- **Customer education.** While educating customers about cyber hygiene is vital, it should not be a public relations exercise or the sole measure, and certainly should not stop at one-off and general messages.
- **Enhanced authentication.** Multi-factor authentication and biometric authentication, particularly for high-risk transactions, provide additional customer protection.
- **Transaction alerts.** Warnings tailored to transaction type and customer profile are more effective than general cautions about scams.

- **Limits and cooling-off periods.** Customer-defined limits with multiple alerts and cooling-off periods add layers of protection and have safeguarded numerous potential victims from scams, albeit at the cost of increased friction in customer processes.
- **Customer behaviour.** Utilising artificial intelligence to profile customers and their behaviours can preemptively identify scams, and allow for interventions to verify and stop the transactions.
- **Scam intelligence.** Monitoring social media platforms and collaborating with industry players and law enforcement on emerging scam tactics can help build defences and educate customers before scammers attack at scale.
- **Customer support.** Measures such as kill switches, rapid response teams, hotlines and support centres can help customers report and stop scams and potentially recover losses.
- **Enhanced cyber security.** Real-time surveillance and improvements in the bank's cyber security defences remain essential.

In conclusion, an integrated strategy that encompasses proactive education, innovative security measures and responsive support is required. Nevertheless, it is crucial that your board first acknowledges and accepts your moral and increasingly legal obligations to effectively safeguard your customers against scams and fraud.

All the best.

Yours sincerely

Mr Sid

Who is Mr Sid?

Mr Sid is a meek, mild-mannered geek who resides in the deep recesses of the reference archives of the Singapore Institute of Directors.

Burrowed among his favourite *Corporate Governance Guides for Boards in Singapore*, he relishes answering members' questions on corporate governance and directorship matters. But when the questions are too difficult, he transforms into Super SID, and flies out to his super network of boardroom kakis to find the answers.

Mr Sid's References (for this question)

Audit Committee Guide
Section 3.3: Fraud Risk Management

Board Risk Committee Guide
Section 3.9: Information Technology Risks

Boardroom Matters
Vol 1, Chapter 24: "Should Failing to Act Diligently be a Crime" by Adrian Chan
Vol 1, Chapter 37: "Are Your IT Controls Truly Adequate" by Gerard Tan
Vol 2, Chapter 30: "Safeguarding Businesses from Digital Threats" by Yeoh Oon Jin
Vol 3, Chapter 25: "Risk Governance for IT Outsourcing" by Marcus Chow
Vol 4, Chapter 41: "Data Protection: Taking the 'It Will Happen' Approach" by Lyn Boxall
14 February 2022: "Ransomware: To Pay or Not To Pay" by Gerard Tan

SID Directors Bulletin
2016 Q4: "Cyber Attacks: Staying Ahead of the Bad Guys" by Benedict Tan
2021 Q4: "What Recent Cyber Slips Mean for Boards" by Eric Hoh
2021 Q4: "Tackling Fraud in a Pandemic" by David Toh
2022 Q4: "Cyber Security in a Decentralised World" by Lee Wee Lee and Clemence Tan
2024 Q2: "Combating the Escalating Tide of Scams" by Ong Leong Seng
2024 Q2: "The Psychology of Scams" by Ho Yew Kee
2024 Q2: "Cultivating the Right Mindset for Digital Defence" by Alvin Rodrigues
2024 Q2: "The Rise of AI in Cyber Attacks and Defence" by Tan Yuh Woei
2024 Q2: "Curbing Cyber Risk with AI-Powered Governance" by Mark Tham
2024 Q2: "From Prevention to Recovery: Confronting Inevitable Cyber Threats" by Foo Siang-tse and Howie Lau

SID Courses
Listed Entity Director course: LED6 Board Risk Committee Essentials
Board Readiness Programme: Digital Risk