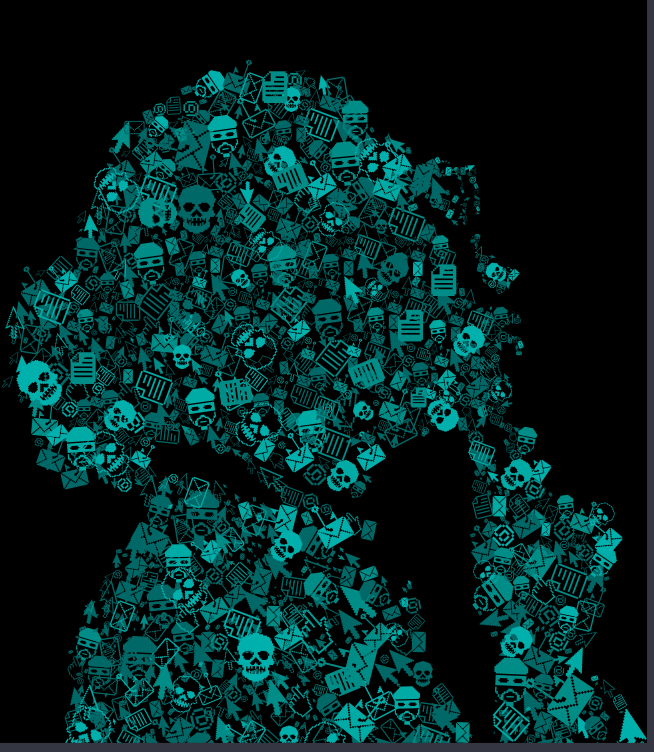

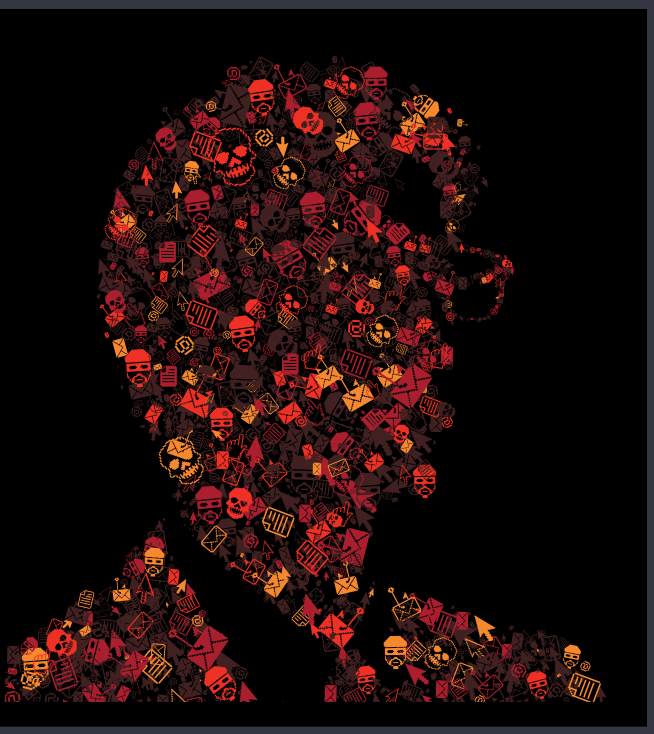

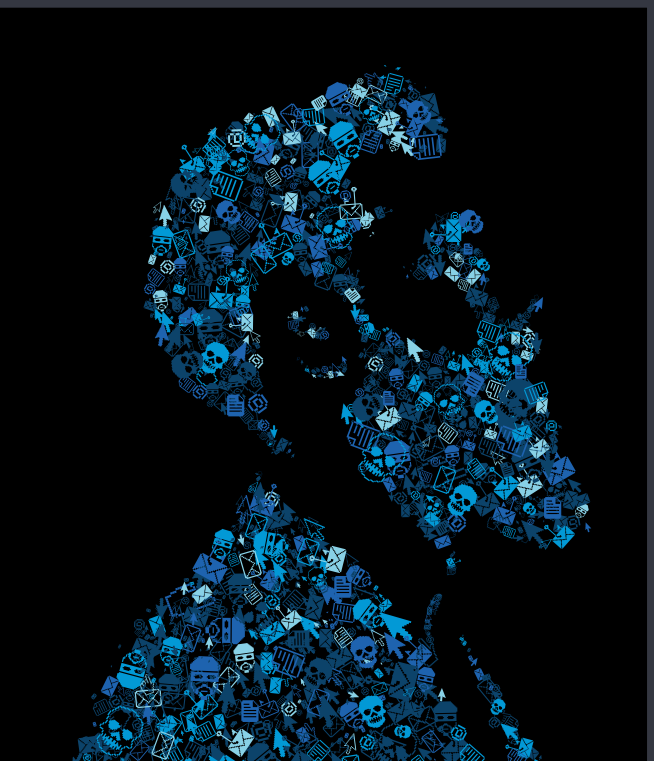

proofpoint.

REPORT

The 2022 Singapore User Risk Report

Exploring people-centric cybersecurity in the hybrid era

proofpoint.com

ABOUT THIS REPORT

The 2022 Singapore User Risk Report complements research from the **2022 Human Factor** from Proofpoint. Since its inception, the Human Factor has explored a simple premise: that people—not technology—are the most critical variable in today's cyber threats. Since then, this once-contrarian notion has become a widely acknowledged reality. Cyber attackers target people. They exploit people. Ultimately, they are people.

To effectively prevent, detect and respond to today's threats and compliance risks, information security professionals must understand the people-centric dimensions of user risk: vulnerability, attack and privilege. In practical terms, this means knowing:

- Where users are most vulnerable
- How attackers are targeting them
- The potential harm when privileged access to data, systems and other resources is compromised

Addressing those elements—the human factor of cybersecurity—is the core pillar of a modern defence.

ABOUT THE HUMAN FACTOR

The global Human Factor report offers detailed insights into vulnerabilities, attacks and privilege, drawing on data collected from Proofpoint deployments around the globe.

EACH DAY, WE ANALYSE MORE THAN:

2.6B
email messages

49B
URLs

1.9B
attachments

25M
cloud accounts,

1.7B
suspicious mobile messages

Together, this amounts to trillions of data points across the digital channels that matter.

The 2022 Human Factor can be downloaded **here**.

What this report covers

Organisations in Singapore have invested hundreds of millions of dollars in cybersecurity, and they work hard to keep up with changing regulations. Despite these efforts, some of the best-known brands have succumbed to phishing attacks. In one of countless recent examples, the customers of a leading bank lost SG$13.7 million in an SMS phishing scam where the attacker impersonated the bank.

Driven by the global pandemic, organisations have increased remote working and accelerated adoption of cloud platforms. These shifts, while beneficial and even necessary, have massively expanded attack surfaces. At the same time, greater digital engagement has given attackers new avenues for phishing.

This report focuses on social engineering, the common thread in modern cyber attacks. Social engineering exploits human nature rather than technical vulnerabilities, making it fiendishly difficult to defend against.

In Singapore, phishing attacks that use email, voice and SMS most often impersonate health authorities, banks, telecommunications and logistics and delivery companies. These forms of fraud reflect the changing nature of work and life. People are often working from home. They are anxious about their health. They're also banking online and making online purchases much more often than before. For attackers, it's a windfall of new opportunities.

Methodology

The 2022 Singapore User Risk Report uses survey data collected on the Ipsos DIY digital platform between September 5–9, 2022. The survey was conducted amongst 600 working adults based in Singapore to explore how people expose their organisations to cyber threats. It focuses the facets of user risk for Singaporean users and organisations, with comparative global context. Ipsos complies with the ESOMAR code of conduct and associated guidelines. Ipsos is in no way responsible for or affiliated with the findings and conclusions laid out in the report; Proofpoint used the Ipsos DIY digital platform for data collection only.

DEFINING CYBERSECURITY RISK

In cybersecurity, risk is defined as:

THREATS VULNERABILITY IMPACT SECURITY CONTROLS

In other words, a people-centric risk model takes into account:

- The probability of someone being attacked (attacks)
- The likelihood that they will interact with a piece of malicious content sent to them (vulnerability)
- How severe the impact could be if their credentials are compromised (privilege)

This report focuses on each of these elements through the lens of our people-centric model of user risk—vulnerability, attacks and privilege—with recommendations on ways to mitigate each.

49%

of Singaporean employees work remotely, blurring the lines between personal and professional life and expanding attack surfaces massively.

According to the Proofpoint 2022 State of the Phish Report:

54%

of employees globally use their personal phones for work purposes.

SECTION 1

Singaporean Organisations at Risk in Hybrid Work Environments

Nearly half of Singaporean employees (49%) work remotely, blurring the lines between personal and professional life and expanding attack surfaces massively. According to the Proofpoint 2022 State of the Phish Report, 54% of employees globally use their personal phones for work purposes. This means that, for many, the smartphone contains the keys to both personal and professional data.

And as hybrid working becomes the norm, cyber criminals are using a combination of tactics and communications tools to reach their intended targets, regardless of where they connect from. Our report shows that Singaporean organisations are at an alarmingly high risk of receiving fraudulent communications.

Worse, many of these phishing attacks have been phenomenally successful for attackers. Highly publicised phishing attacks on the customers of major Singaporean banks made headline news and greatly distressed many people. Our research reveals that 76% of Singaporeans receive scam calls, text and emails at least once a week, and 14% receive them more than five times a week.

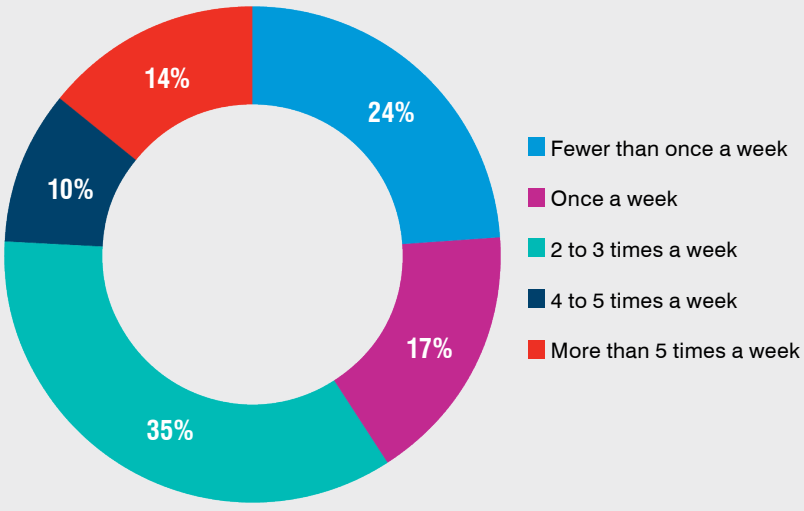

Figure 1: How many times a week do you receive scam calls, texts or emails?

Our data shows that more than

100K

attempts to initiate a telephone-oriented attack are made every day.

SECTION 2

More than Half of Working Singaporeans Cannot Recognise Scam Calls

One of the most unexpected findings in our Human Factor global report was the **sharp increase in telephone-oriented attack delivery (TOAD)**. Our data shows that more than 100,000 attempts to initiate a telephone-oriented attack are made every day. These attacks require a high level of direct interaction—the emailed lures do not always contain malware or malicious URLs. Instead, the goal is to persuade the victim to call a fake customer service number. Once the victim calls, the attacker guides them into giving remote access to their computer or manually downloading malware.

This type of phishing attack is a toxic blend of voice, email and SMS engagement. Calls designed to dupe victims are becoming more sophisticated. And to many recipients, they seem genuine.

For example, a call purporting to be from a government health agency when changes are being made to COVID-19 regulations can easily lure a victim into divulging personal credentials. A call from a bank warning of a security breach and asking for passwords to be reset can seem very convincing—an ironic effect of heightened concerns about cybersecurity.

Unfortunately, less than half (44%) of working Singaporeans can definitely determine whether a call from an unknown caller is a scam. This uncertainty makes the use of voice communications much more attractive to cyber criminals.

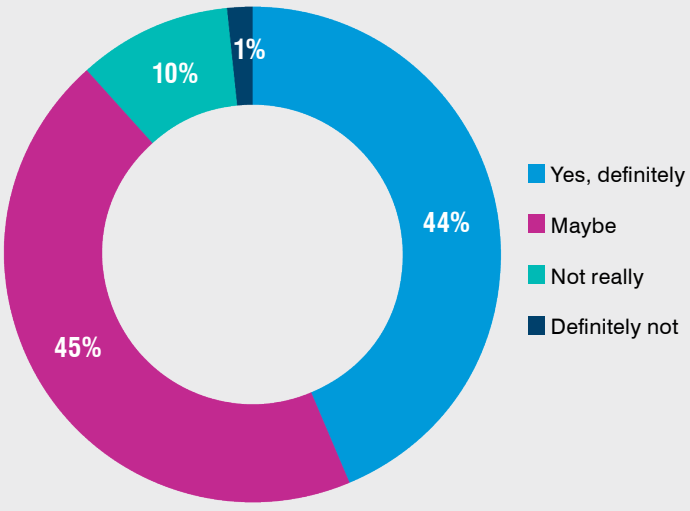

Figure 2 - Do you think you are able to determine whether a call from an unknown caller is a scam?

Our global data for 2021 shows that over

90%

of monitored cloud tenants were targeted every month.

24%

of cloud tenants fell victim to a successful attack.

And the total percentage of tenants compromised during the course of the year reached a whopping

63%

SECTION 3

About Half of Working Singaporeans Know How to Verify Links from Cloud Providers

Cloud infrastructure is now an essential component of most technology stacks. As cloud technology has become ubiquitous, so have attacks on cloud accounts. Our global data for 2021 shows that over 90% of monitored cloud tenants were targeted every month. Nearly a quarter (24%) of cloud tenants fell victim to a successful attack. And the total percentage of tenants compromised during the course of the year reached a whopping 63%. (Note: not all tenants with configured alerts have automatic remediation or protection.) Like email-based phishing and malware delivery, attempted cloud account compromise has grown into a substantial and permanent feature of the threat landscape.

Today, documents are commonly accessed via links to public cloud storage services such as Google Drive, Microsoft OneDrive and Dropbox. Links from these platforms and other legitimate cloud providers are often used by cyber criminals to lure victims into downloading malware stored on or sharing sensitive data. (These services can be used to host a wide range of content—including unsafe documents and other files.) People tend to implicitly trust these links, so attackers' have a good chance of succeeding.

The good news is that security awareness training is making an impact. Some 53% of working Singaporeans know how to verify links from cloud service providers. But that leaves 47% who do not know how to (or are unaware that they can). Companies can mitigate this people-centric vulnerability with more regular security awareness training.

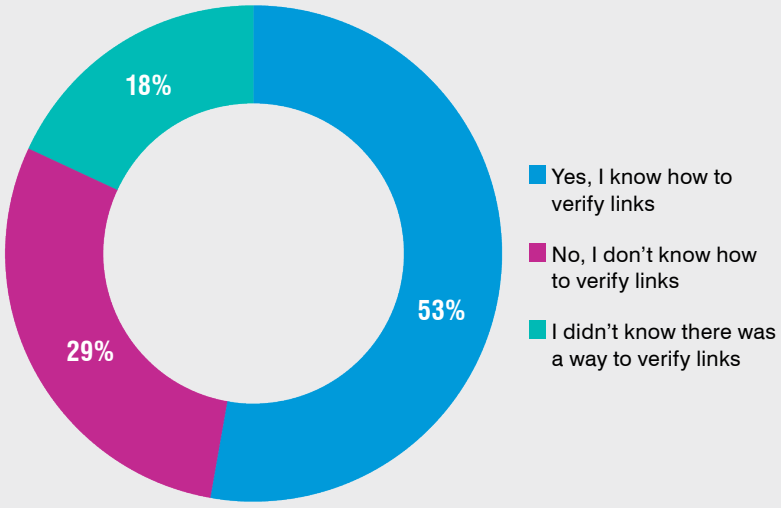

Figure 3 - When you open a document from a site like Google Drive, OneDrive, or Dropbox, do you know how to verify that the links are legitimate?

More than

1 in 4

of working Singaporeans are likely or very likely to share their OTP with a friend or acquaintance. That figure rises to

2 in 3

among managing directors and

3 in 4

among regional leaders.

SECTION 4

Senior-Level Singaporean Employees Are Far Too Likely to Share Passwords

Trust is an essential component of social engineering. To persuade someone to interact with a piece of malicious content, an attacker has to convince them to trust the source—or at least to suspend distrust long enough to succumb. Over the past year, we've seen a growing trend of cyber criminals going to surprising lengths to develop rapport with victims before attempting to initiate an attack. The most common form of conversational threat involves task-oriented lures, a form of business email compromise (BEC). These attacks typically start with a benign message asking if the recipient is available to perform a simple task. If the victim engages, the attacker asks for money, gift cards or a change to an invoice.

Singaporean employees demonstrate healthy scepticism about sharing OTPs; 55% say the chances of sharing their one- time passwords (OTPs) is very unlikely. That said, 28% of working Singaporeans are likely or very likely to share their OTP with a friend or acquaintance over an email or messaging platform, if requested. In other words, messages that appear to come from friends can expect to obtain an OTP—and possibly bypass multifactor authentication—more than once in every four tries. This finding is concerning, because the actions of just a few individuals can put an entire company at risk.

Even more alarming: a staggering 66% of managing directors and 75% of regional leaders are likely or very likely to share OTPs that they believe have been wrongly delivered. High-privilege users are disproportionately targeted in attacks across organisations. Our global report shows that while 10% of users are classified as being managers, directors or executives, this group represents almost 50% of the most severe risk or attack.

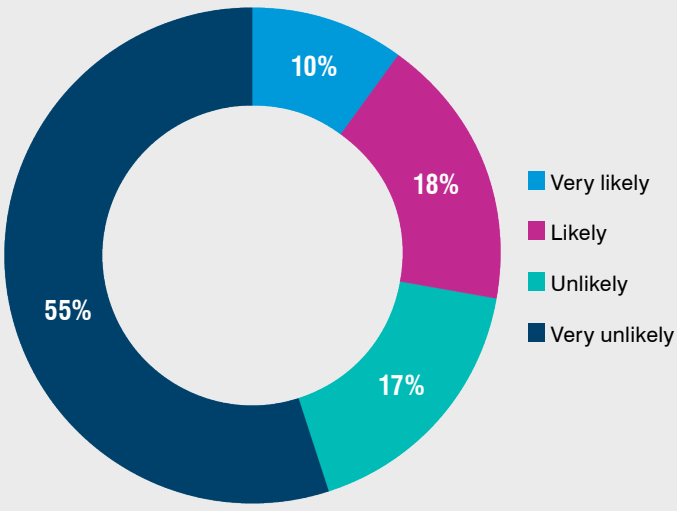

Figure 4 - When you receive a message over a messaging or email platform from a friend/acquaintance asking you to share an OTP (one-time password) because it was wrongly delivered, how likely are you to do so?

SECTION 5

Most Popular Phishing Themes in Singapore

Phishing thrives on anxiety and lack of awareness among victims. With the pandemic continuing to surge and recede throughout the year, COVID-19 lures remained a go-to theme. The first spike coincided with the widening availability of vaccines in the early part of 2021. Campaign volumes declined as more of the population became vaccinated. But that July, a surge in infections caused by the Delta variant led to a further spike in activity.

The pandemic sped up adoption of digital engagement for banking and shopping and the use of digital channels for health-related purposes. Our research reveals that 76% of fraudulent email in Singapore use health-related lures, exploiting anxiety about COVID-19. Some 75% of fraudulent communications appear to be from banking institutions, and 45% profess to be from logistics and delivery companies.

Figure 5: Top Five Themes Used by Fraudsters to Dupe Singaporean Employees

Conclusion

Our research shows that working Singaporeans continue to face high volumes of phishing and other cyber attacks that exploit the tools they use every day. The recent spate of phishing attacks on customers of major banks has been in the headlines — and most Singaporeans have first-hand experience with them. This cyber crime wave has increased awareness of phishing attacks. Still, there's room to improve their ability to detect these attacks and stop them.

More than three quarters of working Singaporeans receive fraudulent calls, texts or emails at least once a week. Our research shows only 44% of the workforce can tell whether a call from an unknown source is fraudulent. And 53% know how to verify links from well-known cloud providers. But despite warnings never to share OTPs, too many Singaporeans are willing to do so if they think the person asking for it is a friend, acquaintance or colleague. Attackers are repeatedly using tried-and-tested methods of pretending to represent banks, health authorities and delivery companies. These findings have huge implications for businesses.

Implications

So what does this mean for Singaporean companies? It highlights that in most cases, human factors matter more than the technical specifics of an attack. Cyber criminals are looking for relationships that can be leveraged, trust that can be abused and access that can be exploited.

Traditional cybersecurity controls are designed to protecting technology. Not enough focus is placed on risk-based controls that focus on people and their role in enabling cyber attacks. Companies should consider a people-centric approach that gives them visibility into:

- Which employees are being attacked
- How they are being attacked
- What data they have access to
- How susceptible they are

Cyber attacks, like the ones that targeted banking customers in Singapore, are inevitable. But with the right mindset, tools and policies, they can be a manageable risk.

LEARN MORE

To learn more about how Proofpoint provides insight into user risks and helps you mitigate them with a people-centric cybersecurity strategy, visit **proofpoint.com.**.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organisations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0401-004-01-01 11/22