SG CYBER SAFE

CYBERSECURITY TOOLKIT

FOR SME OWNERS

UPDATED: 7 OCTOBER 2021

About the Cyber Security Agency of Singapore (CSA)

Established in 2015, CSA seeks to keep Singapore's cyberspace safe and secure to underpin our National Security, power a Digital Economy and protect our Digital Way of Life. It maintains an oversight of national cybersecurity functions and works with sector leads to protect Singapore's Critical Information Infrastructure. CSA also engages with various stakeholders to heighten cybersecurity awareness, build a vibrant cybersecurity ecosystem supported by a robust workforce, pursue international partnerships and drive regional cybersecurity capacity building programmes.

For more news and information, please visit www.csa.gov.sg

Cybersecurity is a
business investment.
It will pay for itself over time.

Overview

Digitalisation has changed the way we work, learn, transact, and stay connected. Developments such as global pandemics have accelerated the scale, scope, and speed of digitalisation. SMEs have leveraged the Internet and technology for their business operations. In order to reap the benefits of going digital, many SMEs are taking business continuity measures, such as adapting to new ways of working, by bringing their services online.

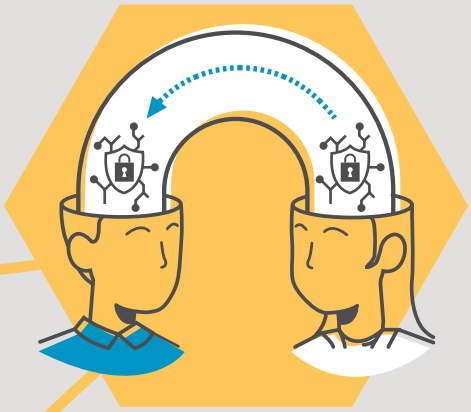
The benefits of digital transformation can be fully reaped when enterprises invest in cybersecurity. SMEs which do not invest in cybersecurity when they embrace digitalisation may render themselves as easier targets for cyber attacks. By enhancing their cybersecurity, SMEs will be in a better position to fully take advantage of digital transformation as the risks posed by cyber attackers will be significantly reduced.

The Cyber Security Agency of Singapore (CSA) has developed a series of cybersecurity toolkits for enterprises. These include the "**Cybersecurity Toolkit for Enterprise Leaders**", the "**Cybersecurity Toolkit for SME Owners**", the "**Cybersecurity Toolkit for Employees**" and the "**Cybersecurity Toolkit for Information Technology (IT) Teams**".

This cybersecurity toolkit is targeted at owners and key business leaders in Small and Medium Enterprises (SMEs). Compared to larger enterprises, SMEs tend to be constrained by resources, or face limited access to Information Technology (IT) and/or cybersecurity-trained personnel and know-how. This cybersecurity toolkit for SME owners covers five areas of focus which are fundamentals that an SME should consider in order to ensure cybersecurity is adequately addressed.

CYBERSECURITY GUIDANCE FOR SME OWNERS

Cultivate cybersecurity leadership in your organisation



Educate your employees on cybersecurity

Protect your information assets[1]

Secure your access and environment

Ensure your business is cyber resilient

[1] Refers to hardware, software and data assets.

Each area in the toolkit addresses the following questions:

What can you do to improve your cybersecurity?

This section provides actionable advice for SME owners to improve their cybersecurity and highlights why cybersecurity is important for SMEs.

What does good cybersecurity look like?

This section provides guiding statements and questions to help SME owners understand the best practices for cybersecurity. SMEs that have limited IT resources to address cybersecurity in your organisation may refer to the "**Cybersecurity Toolkit for Information Technology (IT) Teams**" for resources and implementation examples.

Cultivate Cybersecurity Leadership in Your Organisation

Why is this important?

As an SME owner, understanding the importance of cybersecurity allows you to identify the cyber threats your organisation faces so that you can take the necessary actions to protect your business. SMEs are not too small to be attacked[2]. By taking a proactive approach towards cybersecurity from the top, you are also leading by example and helping to promote a cyber safe culture for your organisation.

[2] For example, in CSA's Cyber Threat Landscape 2020 report, most of the ransomware cases reported to CSA were from SMEs.

What can you do to improve your cybersecurity?

Ensure employees and departments are clear on their roles and responsibilities with respect to cybersecurity

- Communicate the importance of cybersecurity to all employees in your organisation by encouraging them to take joint responsibility and accountability for cybersecurity.
- Assign role(s) for cybersecurity champion(s) within your organisation. The champion should have up-to-date knowledge on cybersecurity fundamentals. The cybersecurity champion will take charge of initiatives to promote good cybersecurity measures within your organisation by sharing tips, news, and suggestions to improve internal processes.

Establish a cybersecurity work plan

- Cyber threats are constantly growing more sophisticated and happening more frequently, and all enterprises, large or small, will need to be prepared. Having a cybersecurity work plan is crucial to protect your business against such attacks.
- The cybersecurity work plan consists of:
  - Providing training for employees to be aware of cybersecurity;
  - Taking steps to protect your information assets, which can include hardware, software, and data;
  - Taking steps to secure your access and environment to minimise unauthorised entry; and
  - Putting in place plans to help your business remain cyber resilient.

Allocate budget minimally for cyber hygiene measures

- Allocate budget to invest in cybersecurity, for example:
  - Ensure your employees are trained to be aware of cybersecurity;
  - Implement cybersecurity tools based on your cybersecurity work plan; and
  - Ensure your business devices and legacy systems (e.g. laptops, outdated applications) remain updated.

Identify potential risk and assess measures in place to address risk

- Identify “what could go wrong” in your business environment arising from cybersecurity issues.
- Assess if sufficient cybersecurity measures are in place to protect your business environment.

What does good cybersecurity look like?

Guiding Questions and Statements for SME Owners

Q1
Have you identified "what could go wrong" in your business environment arising from cyber attacks?

- Are you aware of the importance of cybersecurity to your business?
- Are your current cybersecurity solutions sufficient to protect your business environment when cyber attacks happen?

Q2
How do you encourage your employees to take joint responsibility for cybersecurity?

- Are your employees aware of their roles in contributing to cybersecurity in your organisation?
- Do you document this formally in a policy document and circulate this to employees, so that they are aware of this expectation?

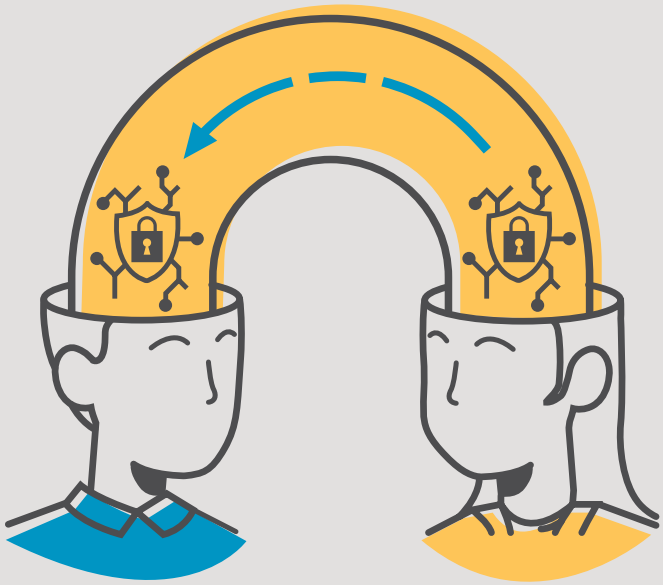
Q3
Do you have a cybersecurity work plan to protect your organisation?

- Does the work plan identify the systems and information that are essential for your business?
- Does the work plan consider the impact to your business if these systems and information were to suffer a cyber attack?
- Does the work plan include measures in place to protect these systems and information?
- Does the work plan have a defined and realistic timeline?

Q4
Do you have a budget allocated specifically to cybersecurity?

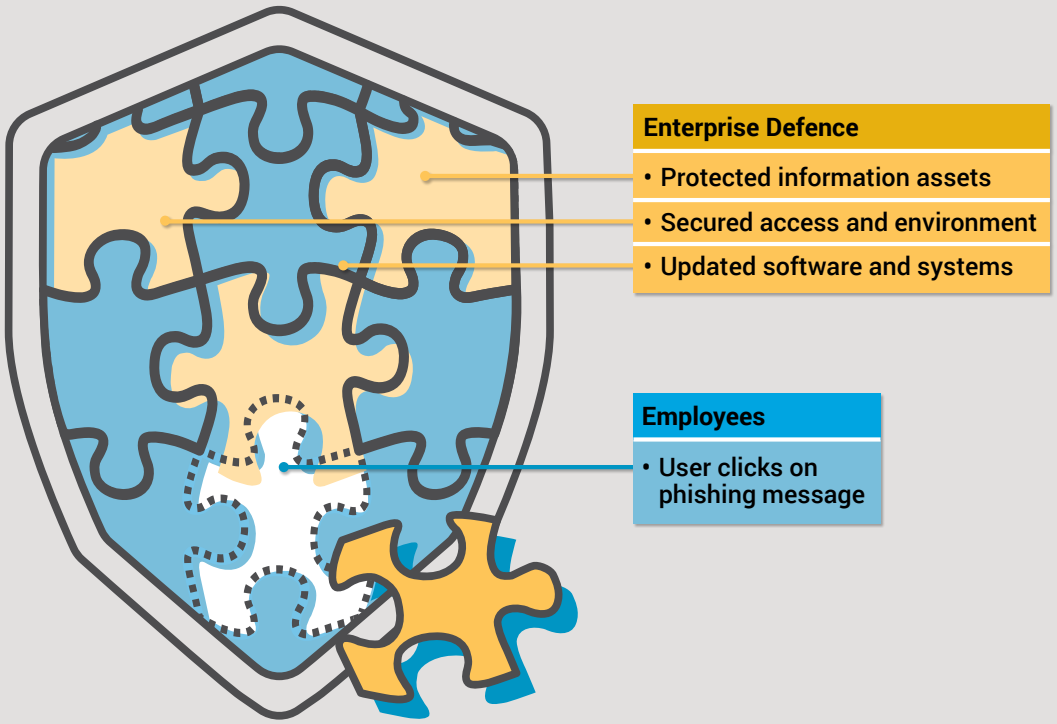
- This can be used to implement your cybersecurity work plan, e.g. provide cybersecurity training for your employees, deploying cybersecurity tools, or to support the activities driven by the cybersecurity champions in your organisation.

Educate Your Employees on Cybersecurity



Why is this important?

One of the biggest threats to cybersecurity in any organisation comes from its employees, whose actions may inadvertently result in a cybersecurity incident in your organisation. Cyber attackers often take advantage of this weakness and use social engineering[3] tactics to trick your employees into giving up sensitive information like login credentials, or to download malicious software that could infect the rest of your organisation. If you ensure your employees are trained to be aware of cybersecurity, this helps your employees to become your first line of defence.



[3] Social engineering refers to the "psychological manipulation of people into performing actions or divulging confidential information". Social engineering attacks often exploit human behaviour and are not always technological in nature. This can be done through either digital or non-digital means. Phishing is one of the most common forms of social engineering.

What can you do to improve your cybersecurity?

Ensure cybersecurity starts from the top and instil security mindset

- Communication on cybersecurity is the most effective when it comes from you, the SME owner:
  - Lead by example – Ensure you remain up-to-date on cybersecurity developments and openly support cybersecurity initiatives; and
  - Provide clear and specific rules and guidelines related to cybersecurity, so that your employees know what to do, or not do.
- Ensure that your employees understand how important they are to the cybersecurity of your organisation, and that they are your organisation's first line of defence against cyber attacks.

Ensure that you and your employees minimally have basic knowledge and awareness of cybersecurity

- Put in place a cybersecurity training programme for all your employees, so that they know how to recognise and handle the various types of cybersecurity incidents.
- Ideally, the training and awareness programme should not take a "one size fits all" approach. Consider customising the programme for your business environment and for the different roles in your organisation, especially for those roles that have access to sensitive data and systems.

What does good cybersecurity look like?

Guiding Questions and Statements for SME Owners

Q1
How have you reinforced the message that cybersecurity is the responsibility of everyone in your organisation?

- Do you clearly and openly communicate the importance of cybersecurity across your organisation to ensure that all employees have a part to play in cybersecurity?
- Do you document your cybersecurity policies or guidelines, i.e. the practices for ensuring good cybersecurity within your organisation, so that employees are aware this is the expectation of them?
  - Are the policies or guidelines written clearly and are easy for all employees to understand and follow?
  - Are these policies or guidelines made freely available to all employees within your organisation so that they are aware of the expectation of them?
  - How do you make sure your employees are aware of these expectations, and know where to access the policies and guidelines to ensure that they follow good cybersecurity practices?

Q2
Have all your employees been trained to be aware about cybersecurity?

- Do your employees know how to identify a phishing email[4] and know what to do when they receive one, such as immediately reporting the phishing incident to the relevant parties in your organisation?
- Do your employees know how to come up with strong passphrases[5], and have good habits on passphrases, e.g. not to write them down and leave them in open areas, not to share passphrases with others, not to use the same passphrase for different accounts, etc?
- Do your employees know their responsibilities in protecting their corporate devices and personal devices (used for work)? Are employees aware of best practices when accessing the company's data and information from their personal devices?
- If your employees encounter a suspected cybersecurity incident, do they know what to do, e.g. to report to the relevant parties in your organisation? Do you provide a sufficiently "safe" environment to encourage your employees to report suspected cybersecurity incidents?

[4] Signs of phishing include use of urgent/threatening language, suspicious attachments in the message, and grammatical mistakes.
[5] Passphrases are similar to passwords, but they use a sequence of random words, rather than characters, e.g. putting five random words together. Strong passphrases should be at least twelve characters long, include upper case, lower case, numbers and/or special characters.

CASE STUDY #1:

Impact:

In 2020, an education institution fell victim to a successful phishing scam. This led to an estimated loss of $2.3 million.

Issue:

Phishing emails were sent to the institution in November 2020. Due to the lack of cybersecurity awareness of its employees, the employee had not recognised the phishing emails and was deceived into altering bank account details to a known vendor, resulting in three separate transactions being sent to a fraudulent bank account created by the attackers. Another employee uncovered the scheme a month later after realising the funds were missing, leading to the involvement of law enforcement and authorities.

Lesson Learnt:

Business Email Compromise (BEC) scams usually begin with phishing, in which malicious and fraudulent emails are sent in the hopes of duping an employee into paying invoices or revealing sensitive information. Without the proper training to identify these, it can become easy for the attackers to succeed. These type of attacks could have been mitigated by having a cybersecurity awareness programme to ensure employees have the skills, knowledge, and capabilities to prevent, detect, and respond effectively to cyber incidents.

Protect Your Information Assets

Why is this important?

Information assets refer to hardware, software, and data which provide value and support the day-to-day operations of your business. Protecting your information assets against cyber attacks will allow your business to prevent and minimise the damage and loss caused by these attacks.

What can you do to improve your cybersecurity?

Keep track of your hardware, software, and data

- You should keep track of all the hardware, software, and data in your organisation and ensure this list is kept updated. It is only possible to plan for the protection of the hardware, software, and data in your organisation if their existence is known.

Know what are the hardware, software, and data that are important to your organisation

- You are likely to have a wide range of hardware, software, and data – identify the ones that are critical to your organisation's existence and crucial for your day-to-day operations.
- Additional effort would be needed to protect and secure the hardware, software, and data that are critical and crucial to your organisation.

Ensure hardware, software, and data are well-protected

- For hardware devices such as computers and mobile phones that are connected to your organisation's network, ensure that they are protected with anti-virus and anti-malware solutions.
- For software and operating systems, ensure information about their patching and update status is documented.

What can you do to improve your cybersecurity?

Ensure regular system/software updates and avoid using outdated systems and software

- Systems and software may see new vulnerabilities being discovered, and their vendors typically provide patches to address these vulnerabilities. Therefore, it is important to constantly keep your systems and software patched and up to date, so that the security "holes" can be closed as soon as possible. You should also consider the following:
  - Regularly update all of your systems and software;
  - Turn on automatic download and installation of updates whenever possible;
  - Identify all systems and software that require manual updates; and
  - Take into account any mobile devices in your environment.

Ensure backups are conducted regularly

- Ensure that business-critical systems and data are identified and backed up offline, i.e. in a separate location from your systems and data.
- Backups should be conducted on a regular basis – you can determine the frequency of the backup by deciding how much data loss you can accept between backups.

Consider appointing an IT vendor

- Appoint an IT vendor to look into your organisation's cybersecurity needs, such as developing cybersecurity policies and procedures to protect information assets, as well as implementing and managing cybersecurity controls.

What does good cybersecurity look like?

Guiding Questions and Statements for SME Owners

Q1
Are you fully aware of what information assets such as hardware, software, and data assets are used in your organisation?

- Have you created an asset inventory listing to keep track of your hardware, software, and data assets in your organisation? Do you know what all the business-critical hardware, software, and data that need to be protected are?

Q2
What are the cybersecurity measures that have been put in place to protect your hardware, software, and data?

- Have you deployed anti-virus and anti-malware solutions on all your organisation's computers to prevent your data from being corrupted or stolen?
- Does the software you use still receive support and security updates from the supplier?
  - Are the security updates automatically downloaded and installed to ensure that your systems are protected against the latest security "holes"?
- Do you use any products which are no longer supported by the supplier?
  - Are you aware of the risks of using such products in your organisation? Suppliers will no longer offer patches, bug fixes, and security upgrades for these products, and this will compromise your security.
  - Can you minimise these risks by using alternative products?

Q3
Are your business-critical systems and data backed up to ensure operations are able to continue in the event of a cyber incident?

- Are business-critical systems and data backed up offline, so that the data is still available in the event of a cyber incident?
- Have you tested your backup and restore process to ensure it will work in the event of a cyber incident?

CASE STUDY #2:

Impact:

In August 2020, a food and beverage outlet fell victim to a ransomware attack, rendering key business-critical servers and devices inoperable.

Issue:

The business was unable to recover the data lost to the ransomware as all backups were stored on infected servers and could not be restored. As a result, the business had to totally rebuild its IT system from scratch.

Lesson Learnt:

Organisations with important data are often key targets for ransomware attacks. Prevention is key to avoid falling victim to an attack. Organisations should take appropriate measures to secure their infrastructure and systems, and to ensure that their networks are properly segmented (e.g. external and internal networks, guest and wireless networks) to minimise the impact of an attack. In addition, they should perform regular backups and keep these backups offline.

In the event of a ransomware attack, it is not recommended to pay the ransom as the payment does not guarantee the decryption and confidentiality of your data. It also encourages the hackers to continue their criminal activities and target more victims. The hackers may also see your organisation as a soft target and may strike again in the future.

Organisations may also refer to SingCERT's advisory on ransomware for more information.

CASE STUDY #2

Secure Your Access and Environment

Why is this important?

Securing access to your organisation's environment prevents unwelcome and malicious parties from accessing and using your systems and data. Such unauthorised access could lead to the loss and disclosure of sensitive information.

By managing and controlling the access of every account and individual within your environment, including third parties, this would reduce the risks of such incidents. Strong passphrases and Multi-Factor Authentication (MFA)[6] are also used to secure your organisation's environment.

What can you do to improve your cybersecurity?

Know who has access to critical systems and data

- It is important to control access to critical systems and data, based on the user's needs. A user should only have access to the systems, applications, and data based on their roles and needs.

Manage the cyber risks when engaging external vendors

- Ensure that all vendors, particularly those with access to sensitive systems and data, are actively managed and meet the agreed levels of security.
- Measures, e.g. contractual agreements, should be in place to ensure that your vendors meet the security requirements of your organisation to prevent disclosure of sensitive information.
- Drive the importance of using strong passphrases and MFA mechanisms.
- Understand what your vendor is doing, and whether there are any risks that may need to be managed.

[6] MFA is the use of multiple keys to strengthen security. One key is typically your passphrase, and the other key could be an authorisation from an application on your mobile device or through biometrics (like fingerprints and face recognition).

What can you do to improve your cybersecurity?

Use strong passphrases and MFA to secure access

- Encourage everyone to use a strong passphrase – this is a sequence of random words combined into a phrase, and this provides a good combination of memorability and security.
- Adhere to these best practices for strong passphrases:
  - Do not reuse them elsewhere;
  - Do not share them with colleagues; and
  - Enable MFA, particularly for high-value accounts.

What does good cybersecurity look like?

Guiding Questions and Statements for SME Owners

Q1
Are employees' access to devices and assets limited based on their role in your organisation?

- Is access to business-critical assets restricted by default to ensure that it is only granted to employees on an as-needed basis?
- Are the access rights for all employees reviewed and kept up to date? Are access rights revoked when an employee changes their role or leaves your organisation?

Q2
How do you manage third party access to confidential and/or commercially sensitive systems and data?

- Have you established cybersecurity requirements in your third-party contracts to prevent the disclosure and misuse of your organisation assets by third party vendors?

Q3
Have you implemented strong user authentication mechanisms to secure user login?

- Have you established and defined user authentication requirements including the use of strong passphrases? Have you outlined the best practices to follow for strong passphrases in training and awareness activities to your employees and in documented policies?
- Have you implemented MFA where possible to ensure that access to sensitive or critical systems and data is protected with an additional layer of protection?

CASE STUDY #3

CASE STUDY #3:

Impact:

From 2016 to 2018, a technology company's employee managed to defraud the company of more than 10 million USD in digital currency.

Issue:

It is believed that the attacker was a member of company's testing team working on e-commerce solutions, and he was able to create fictitious store accounts to simulate customer purchases. While the company store system blocked the delivery of real physical goods ordered from these accounts, it did not block the delivery of digital gift cards. The attacker used not only his own account but also several test accounts related to his colleagues. He then resold some of the stolen gift cards through online resellers.

Lesson Learnt:

There are different ways for organisations to successfully prevent their employees from misusing privileged accounts. Examples include securing such accounts with Multi-Factor Authentication (MFA), one-time passwords, and manual approval of access requests. Many organisations also have privileged accounts used by multiple users, like admin or service management accounts. In this case, the organisation can use secondary authentication tools to distinguish actions of individual users performed under such accounts. Another way of preventing such events from happening is to ensure that privileged users (except for administrators) do not have the ability to create new accounts, and also ensure that regular users are given only the minimum level of access and permissions needed to perform their work.

Ensure Your Business is Cyber Resilient

Why is this important?

As cyber attacks increase in frequency, scale, and sophistication, it is no longer a matter of "if", but "when". All enterprises, large or small, will need to be prepared. Correspondingly, SME owners should establish plans to minimise the adverse impact of an incident or disruption. For your organisation to be cyber resilient, SME owners need to put in the necessary measures so that your business can recover from a cyber attack with minimal business disruption.

What can you do to improve your cybersecurity?

Drive and plan for disruption to business operations caused by cybersecurity/IT incidents

- Develop a formal Incident Response Plan, which contains clear guidelines, roles, and responsibilities documented to ensure that all security incidents are responded to and addressed in a timely and appropriate manner.

Drive the importance of integrating cybersecurity into your Business Continuity Plan (BCP)

- Ensure that you have included cybersecurity in your BCP, so that you can resume your business operations in the event of a disruption.
- Ensure various plausible scenarios have been considered while planning for business continuity including cyber attacks, data loss, and breaches.

What does good cybersecurity look like?

Guiding Questions and Statements for SME Owners

Q1
Do you have a cybersecurity Incident Response Plan and how do you ensure it is effective in the event of a cyber incident?

- Does your cybersecurity Incident Response Plan include clearly defined roles and responsibilities to ensure your organisation can respond to cybersecurity incidents such as a virus attack or ransomware?

Q2
Do you have a Business Continuity Plan (BCP) and how do you ensure it is effective in the event of a business disruption?

- Is cybersecurity integrated into your overall BCP to ensure your organisation is able to operate in the event of a cyber incident?
- A basic BCP should minimally include the following:
  - Clear roles and responsibilities for escalation and reporting;
  - Recovery plan for the recovery of operations; and
  - Various business disruption scenarios to stay prepared.

CASE STUDY #4:

Impact:

In September 2020, a medical clinic was hit with a ransomware attack causing the shut down of its entire network. While the medical clinic facilities were still able to continue outpatient care and services for emergencies, other services had to be postponed for a week.

Issue:

The company first noticed technical disruptions and took its computer systems offline. However, these systems remained offline for at least three weeks while investigations were carried out. After investigations, the technical disruptions seemed to be the result of a ransomware attack. Even though there was no information on how the ransomware attack happened, it is believed that one of the most common attacks is through emails.

Lesson Learnt:

Healthcare institutions are vulnerable to such attacks due to the nature of their operations. However, this medical clinic had an emergency plan in place which allowed it to shut down its network and avoid the compromise of important data. With the rise of cyber attacks happening, it is crucial to have plans such as a BCP or Incident Response Plan in place for such attacks.

CASE STUDY #4

Contact Details

If you wish to find out more about Singapore's efforts in cybersecurity, please visit the following website or contact us:

Cyber Security Agency of Singapore

www.csa.gov.sg

contact@csa.gov.sg
for general enquiries/feedback

If you have any feedback on this publication, or wish to find out more about the SG Cyber Safe Programme, please visit the following programme page or contact us:

SG Cyber Safe Programme

www.csa.gov.sg/sgcybersafe

sgcybersafe@csa.gov.sg
for general enquiries/feedback

If you wish to report a cybersecurity incident, please contact:

SingCERT

www.csa.gov.sg/singcert


CSA
SINGAPORE


SG
CYBER
SAFE