CYBERSHIELD

WHERE AWARENESS UNLOCK SECURITY

CYBERSECURITY TOOLKIT

FOR EMPLOYEES

Updated march 8, 2024.
CyberShield Team, Dar es salaam- Tanzania.

About CyberShield Team Inc.

CyberShield is the Tanzania's largest integrated platform for security awareness training established in 2024. We offer a combination of simulated phishing attacks, incident response plan templates and disaster recovery plans, for crosscutting small and medium scale business industries, we provide person privacy cultural practices highlights and social engineering attack avoidance techniques.

CyberShield is your platform for new-school security awareness training, we help you keep your users on their toes with security top of mind. With this integrated platform you can gain awareness training programs free after subscription, engage in real time phishing attack simulations, create business continuity plan from our localized and industrial based techniques, use free it tools to test your security strength and defend the best achieved security posture and train your employees with us.

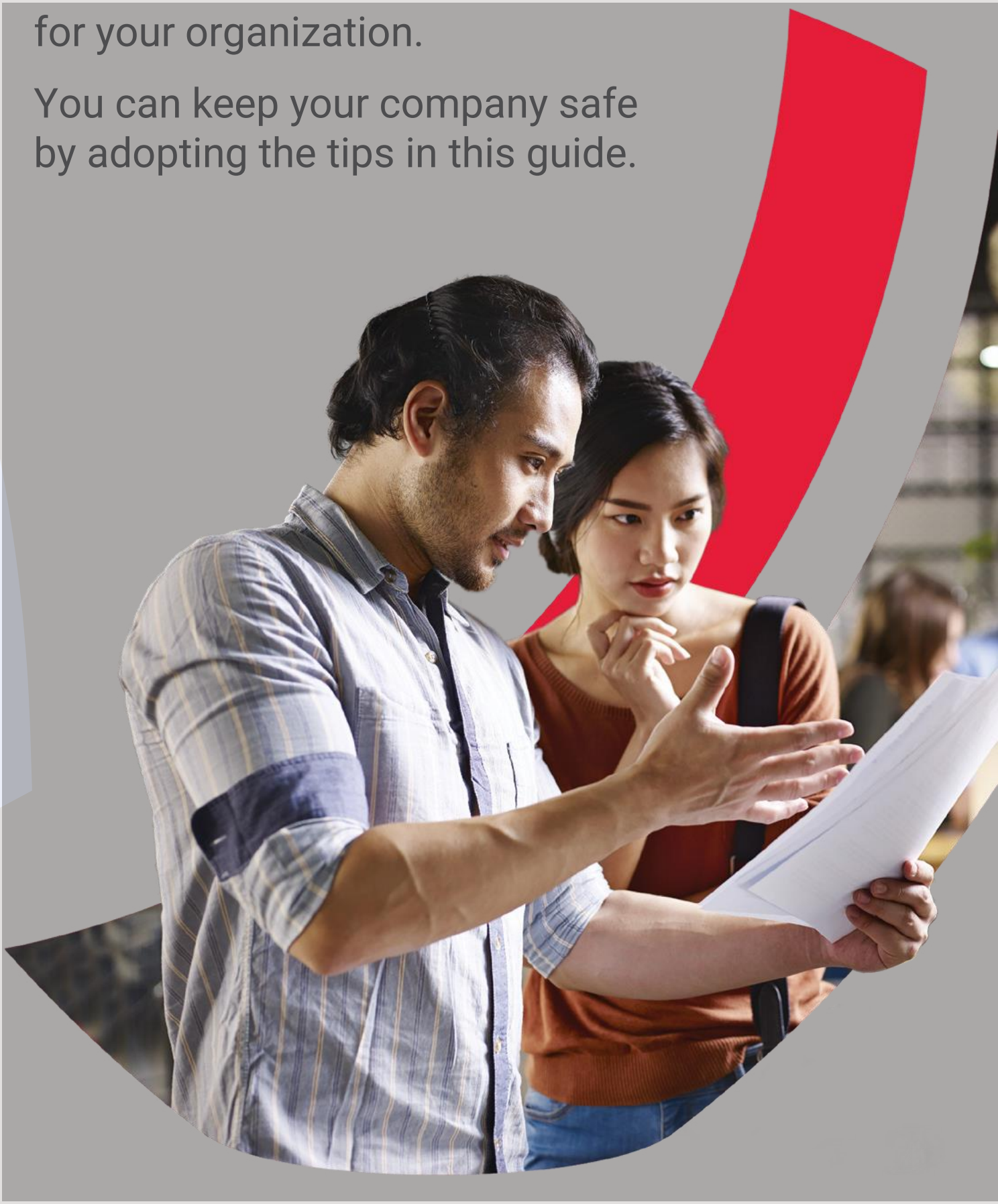
You get on-demand, interactive, engaging training through the website and on.

For more news and information, please visit https://www.cybershield.ac.tz

As employees,

You are the first line of defense for your organization.

You can keep your company safe by adopting the tips in this guide.

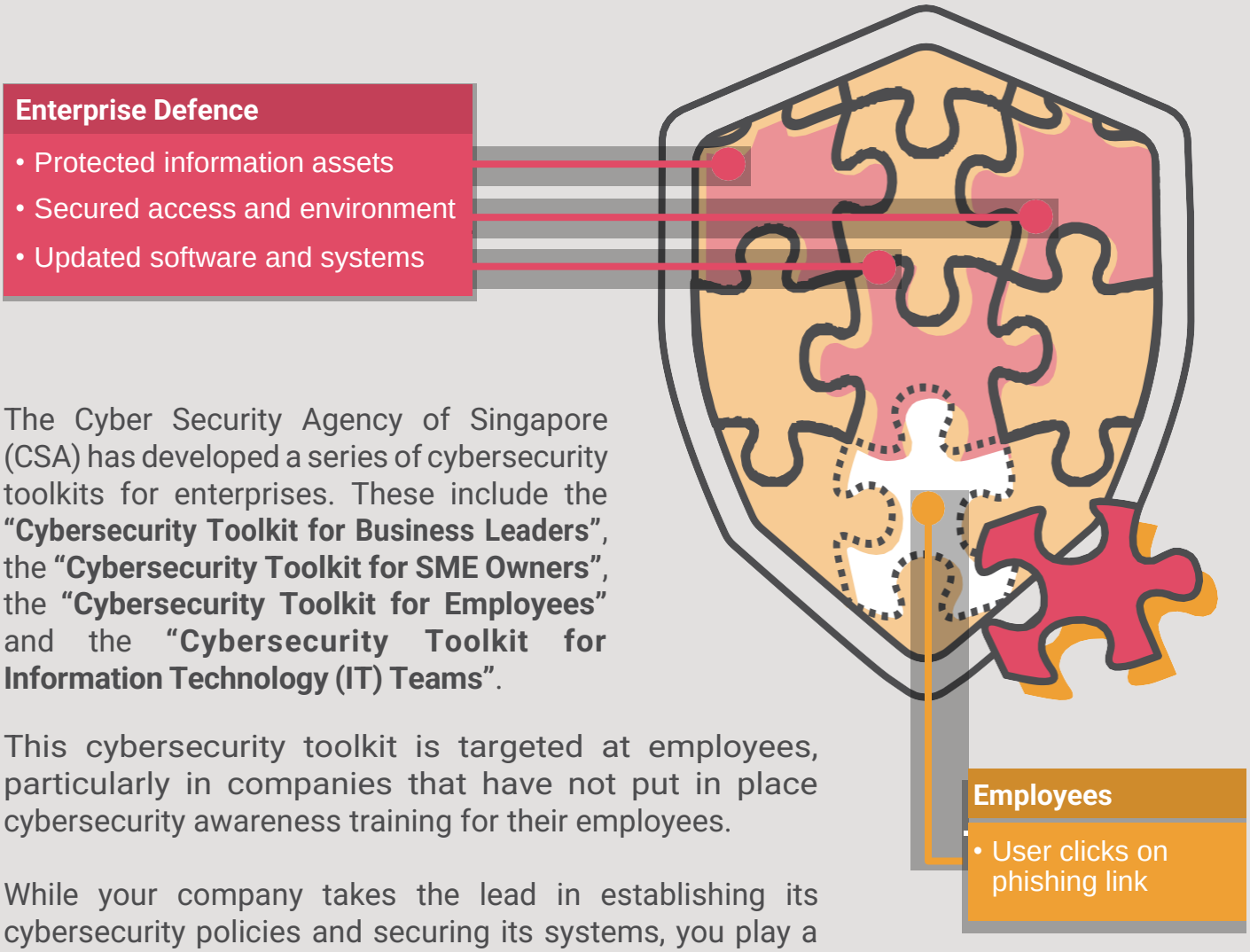


Overview

Whether your company is a large enterprise or a Small Medium Enterprise (SME), you depend on computer systems and devices to get your work done.

Should cyber attackers gain access to your devices and your company's computer network, they can create severe and long-lasting consequences that hurt you and your company. Heavy financial losses, loss of confidential corporate and/or personal information, and reputational damage are some examples.

One of the biggest threats to cybersecurity in any company comes from its employees, whose actions may inadvertently result in a cybersecurity incident.



The Cyber Security Agency of Singapore (CSA) has developed a series of cybersecurity toolkits for enterprises. These include the **"Cybersecurity Toolkit for Business 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 employees, particularly in companies that have not put in place cybersecurity awareness training for their employees.

While your company takes the lead in establishing its cybersecurity policies and securing its systems, you play a key part as your company's first line of defence.

Through this toolkit, you can learn these actionable tips to protect yourself and your company from security breaches.

CYBERSECURITY TIPS FOR EMPLOYEES

Protect yourself from phishing

Set strong passphrases and protect them

Protect your corporate and/or personal devices(used for work)

Report cyber incidents (including suspected incidents)

Handle and disclose business-critical data carefully

Work onsite and telecommute in a secure manner

Protect Yourself from Phishing

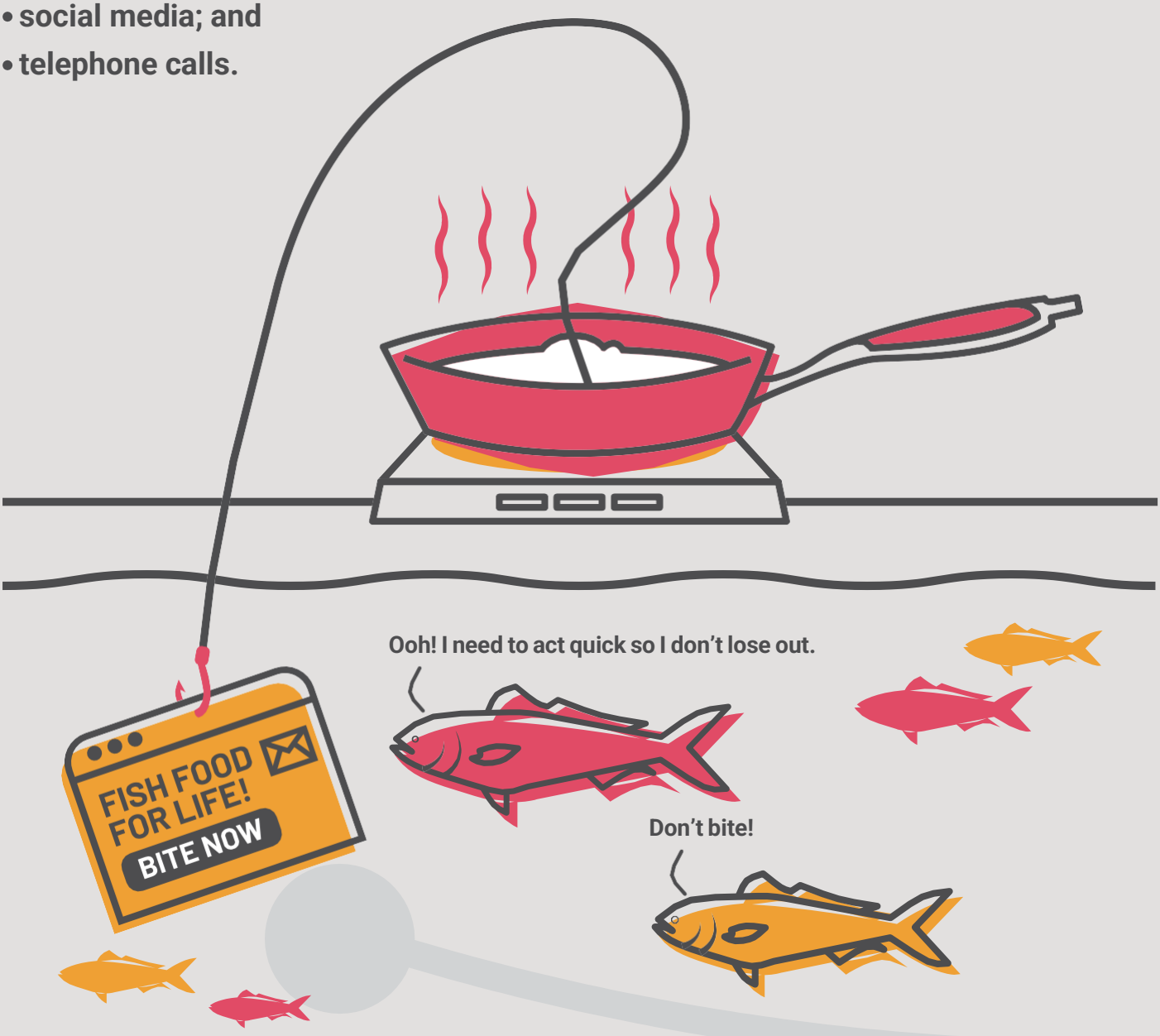
Cyber attackers may use fraudulent emails or texts to trick you into providing confidential information, and/or to open malicious links or attachments. There are several things you can do to protect yourself and your company.

What is phishing?

Phishing is a method used by cyber attackers to trick you into acting on their instructions, such as providing confidential information relating to your company or yourself, and/or opening an attachment with a virus.

Cyber attackers use different digital communications to send phishing messages to you, they include:

- **emails;**
- **instant messaging;**
- **social media; and**
- **telephone calls.**

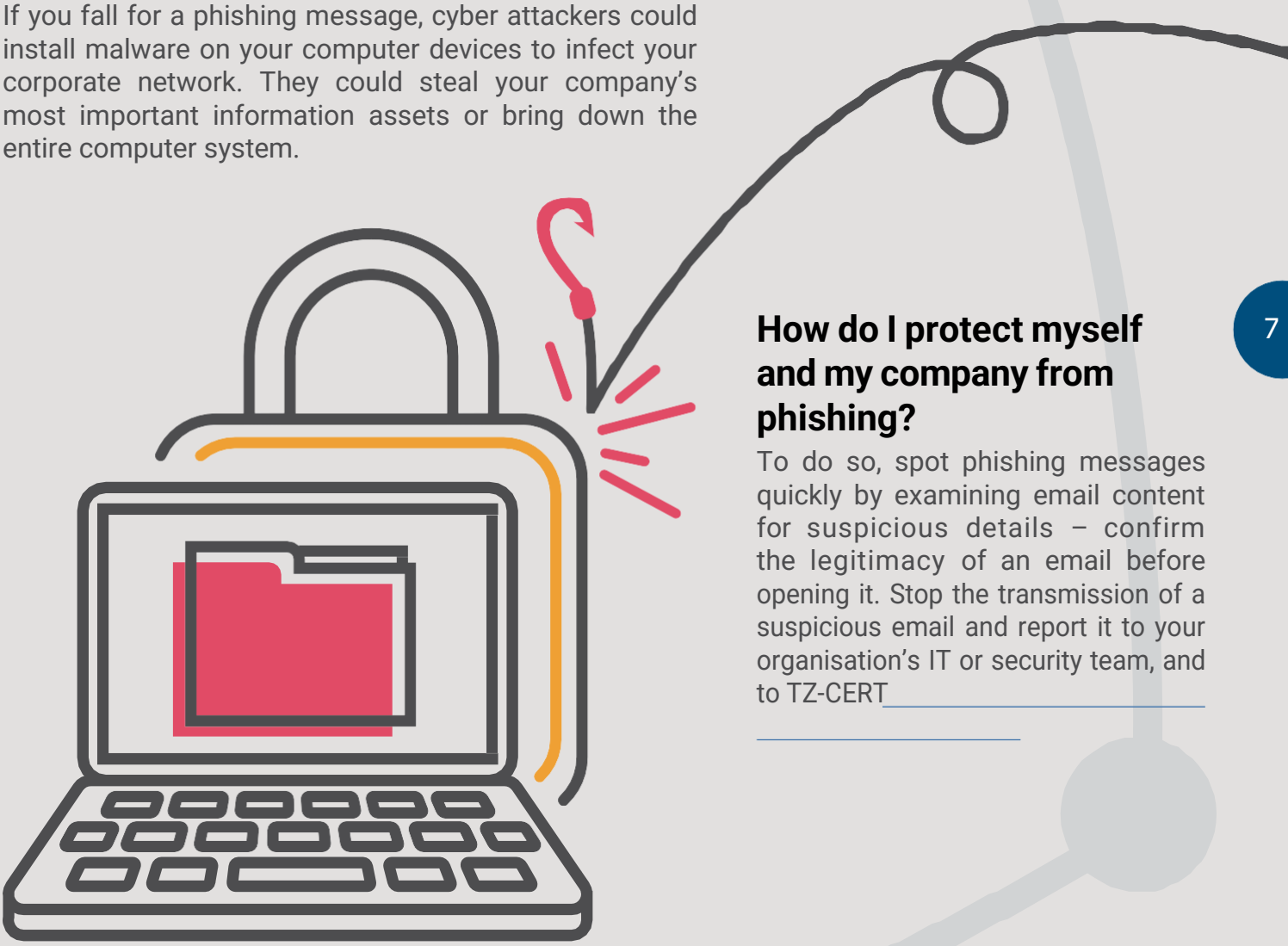


Social Engineering and Phishing

Social engineering refers to the "psychological manipulation of people into performing actions or divulging confidential information[1]." 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.

Why is this important?

If you fall for a phishing message, cyber attackers could install malware on your computer devices to infect your corporate network. They could steal your company's most important information assets or bring down the entire computer system.



How do I protect myself and my company from phishing?

To do so, spot phishing messages quickly by examining email content for suspicious details – confirm the legitimacy of an email before opening it. Stop the transmission of a suspicious email and report it to your organisation's IT or security team, and to TZ-CERT

Step 1

Spot phishing messages[2]

Two broad categories of questions that can help you identify phishing messages are:

Category A	Category B
Does the **sender-related information** (such as email addresses, domain names) seem legitimate?	Does the **content** of the message seem legitimate?

Each suspicious indicator may not conclusively confirm if it is a phishing message and should be considered holistically.

[2] "Categorizing human phishing difficulty: a Phish Scale", Adapted from Journal of Cybersecurity, 2020.

Category A: Examine sender-related information

Check if the sender is who he/she claims to be. The following questions will guide you on this:

Questions	Legitimate **Emails and/or Website Domain Names**	Suspicious **Emails and/or Website Domain Names**
Does the name of the sender match the email address?	Use corporate accounts Tend to have email addresses that match the sender's name	Be wary that cyber attackers could create personal email addresses (such as Gmail, Yahoo mail) with the sender's name
Does the domain name for email and/or website seem legitimate? **Domain names** For emails: Found after the @ sign within the email address and can be found when you hover your mouse cursor over the sender's display name. For websites: Found before the .com in the address bar of your web browser.	Correspond to the company's name or its initials, and/or use specific domain names The Singapore government uses the domain name ".gov.sg" for all its email addresses and websites while certain government educational institutions use ".edu.sg"	Common tricks cyber attackers use to create domain names that look similar to the legitimate ones by: ● Replacing letters in the email address (including domain names) with similar-looking letters, numbers, or symbols, such as: ○ Replacing the lower case "L" with the number "1" (e.g. Paypal.com and Paypa1.com) ○ Substituting the letter "m" with the letters "rn" ○ Using the cyrillic "a" instead of "a" Do pay attention to such minor differences, because this could trick you into thinking that it is a sender from a legitimate source.
Do the attachments or links in the message seem legitimate? **Real web address embedded in links:** Found when you hover your mouse cursor over the link.	Legitimate links should: ● Correspond to its real web address	Suspicious attachments tendto be: ● Unsolicited ● Use file types such as .zip, .scr, .exe files Legitimate attachments, such as popular office software for documents and spreadsheets, may come with macros that run malware ● Disable these software macros by default, and only run them when required

Category B: Examine message content

Confirm whether it is from a legitimate source. The following questions will guide you on this:

Questions	Legitimate Messages	Suspicious Messages
Is the message relevant to my context?	Written for a specific person and purpose in mind With technological advancements in artificial intelligence, it is becoming easier to generate highly targeted and tailored messages (which tend to be more effective in tricking victims)[3].	Messages that are not specifically addressed to you (but says "Dear customer") and are not relevant to your context could be phishing messages ● For instance, phishing messages may ask you to update software that you do not have or give you an invoice for an item you did not purchase
Does the message/ website look professional?	Look professional ● Reputable companies tend to maintain a professional and consistent branding, and use error-free spelling and grammar in their communications ● However, do also be aware that reputable companies may also be commonly spoofed, e.g. Amazon, Paypal, Facebook[4]	
Does the message use the following common tactics to manipulate you into acting on their requests, especially requests for confidential information?		Cyber attackers tend to use a convincing pretext or scenario for you to act on their instruction, and/ or use threatening language that causes a sense of urgency Common scenarios include: ● Mimicking work emails from your company colleagues asking you to act on their instruction ● Pretending to be the government, bank, or technology providers asking you to update, verify, or supplement your confidential data ● Pretending to be legitimate companies asking you to complete an email survey with a reward, enter lucky draws, or apply for limited time offers

[3] "AI wrote better phishing emails than humans in a recent test", Wired, July 2021.
[4] "Singapore Cyber Landscape 2020", CSA.

Step 2

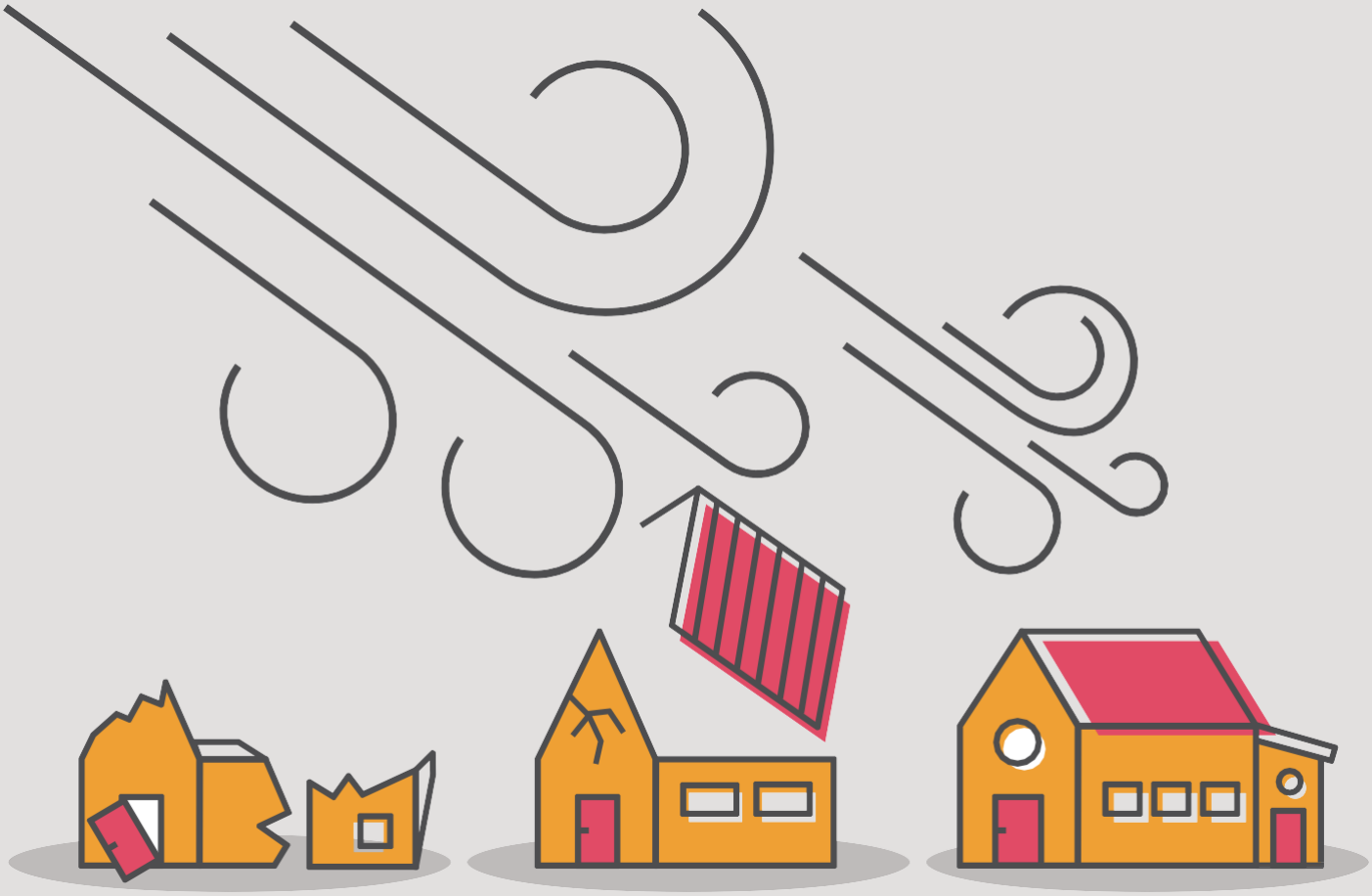
Act on your doubt

If you suspect that you may have received a phishing message (after step 1):

- Do not open the attachment, and do not delete or forward the message.
- Where possible, contact the company or person that the email claims it is from via contact information found from a reliable independent source (e.g. company website) to verify.
    - Do not reply to the message or use the web addresses given within the message for this verification.
- Contact your organisation's information technology help desk or security team as soon as you can and seek advice on how to proceed, especially if you have downloaded attachments or clicked on the link.
- Change your passphrase immediately for this account and other accounts that may use the same passphrase[5].
- Run a full system scan with your anti-virus software, especially if you had clicked on a link or opened an attachment within the phishing message.

[5] You are not advised to use the same passphrase across different accounts.

Set Strong Passphrases and Protect Them



What are passphrases?

Passphrases play the role of digital keys that help you to access your online accounts, devices, and computer systems. They are similar to passwords, but typically longer, because they use a sequence of random words, rather than characters.

Passphrases tend to be more secure because of the longer length, which makes them harder for machines to crack. At the same time, multiple random words put together encourages a range of passwords that have not been previously considered. It is also more usable to enter a passphrase made of random words, compared to one that contains a complex range of characters.

Why is this important?

Passphrases help us protect our online accounts, devices, and computer systems.

The stronger your passphrases, the betterour defences are against cyber attackers hacking into them.

How do I protect myself and my company from passphrase compromise?

To do so, set strong passphrases and protect them. If you suspect that your passphrases may have been stolen, change your passphrases immediately and report unauthorised activity to your organisation's IT or security team.

Step 1

Set strong passphrases

The following questions will guide you on whether you have set a strong passphrase:

Questions	Strong Passphrases	Weak Passphrases
Does your passphrase have at least twelve characters and include various character categories?	Long passphrases that are at least twelve characters long Include upper case, lower case, numbers, and/or special characters Can be made up of five random words that you can remember ● E.g. "Ilovesundayroast@12noon", "LEARNtoRIDEabike@5", "IhadKAYAtoastKOPI@8am"	
Is your passphrase unpredictable?	Unpredictable and cannot be easily figured out by cyber attackers	Use publicly available information about yourself ● E.g. your or your family member's name or birthday Common phrases ● E.g. "May the force be with you" Common patterns such as: ● Capitalising the first letter of the passphrase, e.g. "Livelongandprosper" ● Adding a number at the end, e.g. "qwerty1" ● Replacing a letter with a number or symbol, e.g. "p@ssw0rd"
Is your passphrase unique for different accounts?		Use the same passphrase across different accounts

Put simply, a strong passphrase should have the following elements:

1. At least TWELVE characters long
2. MIX IT UP with upper case, lower case, numbers, and/or special characters
3. Use around FIVE RANDOM WORDS only you can remember
4. Make it UNPREDICTABLE
5. Make it UNIQUE

Password Length or Complexity[6]

Increasingly, the thinking on passwords is shifting towards a longer password, rather than a complex one. This is because computing systems are getting more powerful and it has become a lot easier to use brute-force attacks – where cyber attackers try various combinations of usernames and passwords in order to find the right ones.

Complex Passwords

Because complex passwords are harder to remember, when we are required to use them we tend to choose predictable sequences for our passwords, write down our passwords, or use them across different accounts, and these increase our risks.

Longer passwords

Longer passwords are stronger because there is more uncertainty in the combinations they can take and makes them harder to crack. Using lengthy passphrases made out of words achieve similar outcomes, but are easier to remember.

[6] "Password security: Complexity vs Length", Adapted from Infosec Institute.

Step 2

Protect your passphrases

The following questions will guide you on whether your passphrasesare well protected.

Questions	Strong Protection	Weak Protection
Do you share your passphrases with others or write them down?	Only you should have your passphrases Use software that helps you to manage your passphrases ● Such software should be from trusted sources and support Multi-Factor Authentication (MFA) ● This protects the software from getting hacked, which could lead to having all your passphrases stolen	Passphrases are left lying around, whether it is with someone else or in your notebook
Do you use multiple keys or MFA?	MFA should be used ● The use of multiple keys helps to strengthen security o One key is typically your passphrase o The other key could be an authorisation from an application on your mobile device or through biometrics (like fingerprint and face recognition)	Passphrases, including OTPs, are shared with others

Step 3

Act on your doubt

If you suspect that your passphrases may have been stolen:

- Verify if your passphrases have indeed been compromised using a software to manage your passphrases or web browsers (such as Google) that may come with such features.
- Change your passphrases immediately for this account and other accounts that may use the same passphrase[7].
    - Check for signs of unauthorised activity.
    - Should you find any unauthorised activity, such as monies transfers from your company account, access into a restricted database, or unauthorised email rules (e.g. auto-forwarding rules), immediately notify your IT and security teams.

[7] You are not advised to use the same passphrase across different accounts.

Protect Your Corporate and/or Personal Devices (Used for Work)

What are corporate and personal devices?

Corporate and personal devices are computing devices, such as desktop computers, laptops, mobile phones, and storage media (like hard disks or thumb drives) that are owned by your company and you respectively. We often use a mix of corporate and personal devices for work. For example, you may have a corporate laptop, but use your own mobile phone for work-related communications.

While your company is responsible for your corporate device's cybersecurity, such as installing anti-virus software, you will still need to upkeep its security – like update its software. If your personal devices include confidential corporate information, you are solely responsible for its security and you must make the effort to protect them as well.

Why is this important?

We live our digital lives across a variety of devices. It is important to ensure that these devices are well protected. This reduces the risk of cyber attackers hacking into your devices and/or infecting them with malware, which could lead to your company network being infected in turn.

There are severe and long-lasting consequences for such security breaches. For instance, a malware infection could allow cyber attackers to gain access to our devices and the corporate network to steal confidential corporate and/or personal information. This could result in financial and reputational damage in the long run.

How do I protect my personal and corporate devices from becoming compromised?

For your corporate devices, consult your IT teams first if you are unsure whether you have enabled the right settings on these devices or if you would like to install any software.

Step 1

Protect your device from loss/theft and unauthorised access

The following questions will guide you on whether you have protected your device from loss/theft and unauthorised access.

Questions	Good Practice
Do you always know where your devices are?	Always know where your devices are and never leave them unattended ● Their portability makes it easier for them to be stolen or misplaced Use appropriate physical locks, such as laptop locks, to secure them If available, activate your devices' "find your device" function
Have you secured your device's system?	Secure your device with digital keys such as passphrases, PINs, or biometric locks Encrypt your data and switch on your device's ability to remotely delete company data, if available These security measures will prevent cyber attackers or anyone from accessing your device's systems in the event your device gets stolen or goes missing.
Have you turned on your device's security settings? Do you disable automatic Wi-Fi network connections by default?	Ensure that your devices have the necessary security settings enabled Some of your devices may come with such software or hardware installed, and you will only need to enable these settings ● Such settings include the firewall that protects your devices and the networkby monitoring the network to only allow legitimate traffic Ensure that anti-virus software is installed to prevent your devices from being infected by viruses Only turn on network features when they are needed ● Prevent your devices from connecting to unsecured networks, such as public Wi-Fi networks
Do you regularly back up your device's data, especially important data?	Regularly back up and maintain an updated backup of your device's data in an external storage device or online storage service Ensure that these storage devices are kept offline to prevent cyber attackers from accessing these storage mediums to delete these backups If using external storage devices, ensure that they are kept properly If using online storage services, use a reputable service and act on the passphrase guidance featured in this toolkit Having backups will help you to retrieve/restore your data should your device get stolen or go missing. These backups will also be useful in cases where your device malfunctions.

Step 2

Protect yourself when using public Wi-Fi networks

The following questions will guide you on whether you have protected yourself when using wireless access:

Questions	Good Practice	Poor Practice
When accessing company data and work emails on your devices, do you use public Wi-Fi networks that may be insecure?	Only use trusted networks, such as your corporate or personal Wi-Fi and mobile networks, and/or with a Virtual Private Network (VPN), if it is available ● If trusted Wi-Fi networks are not available because you are working at a public place, use your mobile phone's hotspot Disable the automatic connection to Wi-Fi hotspots Ensure your firewalls are turned on	Use public Wi-Fi networks which may not be secure ● May expose your activities and data to cyber attackers

Step 3

Keep your device updated

The following questions will guide you on whether you have kept your device updated:

Questions	Good Practice
Have you enabled automatic software updates for your device and its applications, if available?	Update your software because it: ● Includes additional security features that resolve security issues of earlier software versions ● Enhances the software's performance and usability which improves user experience Enable automatic software updates (if available onyour devices) ● Your device will regularly check if software updates are available and download them Reboot your device at the earliest opportunity to allow updates to take effect Remember that software updates do not replace anti-virus software and firewalls, which still need to be installed on your devices.
Do you only use devices and software from authorised sources?	Use devices and software either provided by your company or purchased from authorised vendors ● These include your mobile phone apps which should only be downloaded from the official app stores

Step 4

Act on your doubt

If you suspect that you may have lost your corporate and/or personal device used for work:

- Immediately try to locate it.
- If it cannot be found, report this loss to your IT or security teams,and to the police.

Report cyber incidents (including suspected incidents) using either phone call or any other available successful means to the authority.

Report Cyber Incidents (Including Suspected Incidents)

What are cyber incidents?

Cyber incidents are events that can threaten digital information and/or information systems. These range from serious organised cyber crime to basic malware attacks and even the loss of your corporate devices. When cyber incidents happen, it does not always mean that your company or you will be harmed. But there is a potential risk that such harm could happen. For example, the loss of your corporate laptop does not mean that confidential corporate data will be stolen, if you manage to locate it much later in your house.

Why is this important?

As there is a risk that harm could happen when a cyber incident occurs, it is crucial that you learn to spot cyber incidents (even suspected ones) and report them quickly so that you can prevent these potential harms from actually happening. For instance, the potential risk of data theft could happen if your corporate laptop was intentionally stolen by someone.

This means that no matter how small the issue may seem to you, it is important to report these cyber incidents to your IT or security teams to investigate further.

How do I prevent cyber incidents (including suspected incidents) from becoming more serious?

Your IT or security teams cannot be present everywhere all the time – you can be their eyes and ears to let them know if something does not look right.

Step 1

Spot cyber incidents

The following questions will guide you on possible common cyber incidents that you should report:

Questions	Possible Cyber Incident	Details
Are you unable to access your company files and did you receive any messagesabout having to pay a ransom to get them unlocked?	Likely a ransomware attack	• Ransomware is a form of malware that locks up your files • To unlock these files, cyber attackers will demand a ransom from you to do this • Some ransomware variants may spread to other machines on the network, e.g. WannaCry
Do you notice your corporate device or web browser acting oddly, such as slowing down, unknown files appearing, or your anti-virus program sending alerts?	Likely a malware (or malicious software) attack	• Malware is designed to disrupt or deny normal information system operations, steal information, and gain unauthorised access • Different types of malware are designed to perform different tasks and include viruses, trojans, and spyware
Do you notice that your company's confidential data has been accessed or modified without your knowledge?	Likely a data breach	Data breaches are incidents that expose confidential data to unauthorised access, modification, or similar risks

Step 2

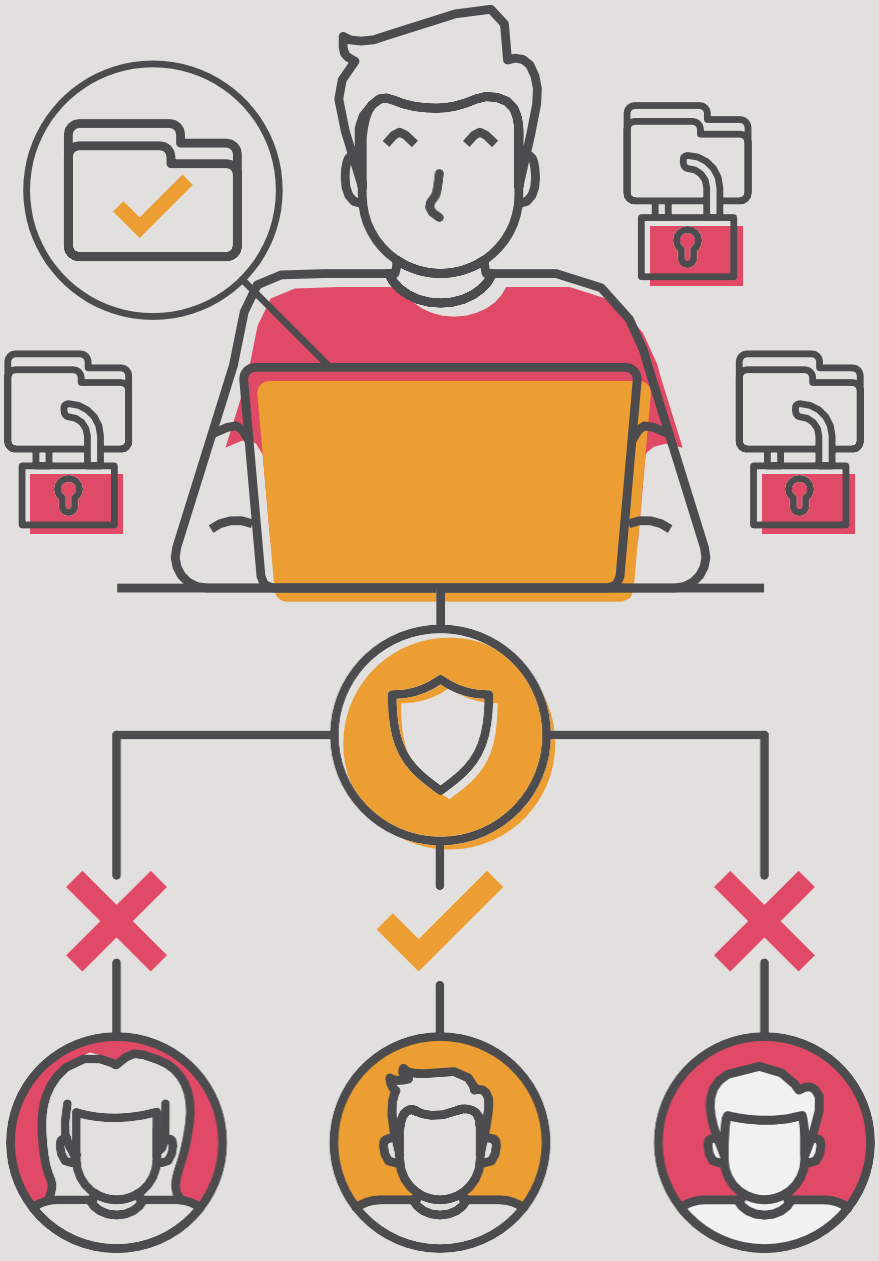
Act on your doubt

If you suspect that you have encountered a cyber incident:

- Immediately report the incident to your IT or security teams to investigate further.
- Refrain from taking action on your own as it may alert the cyber attackersthat their activity has been spotted.

- Your IT or security teams are in a better position to take remedial action.

Handle and Disclose Business-critical Data Carefully



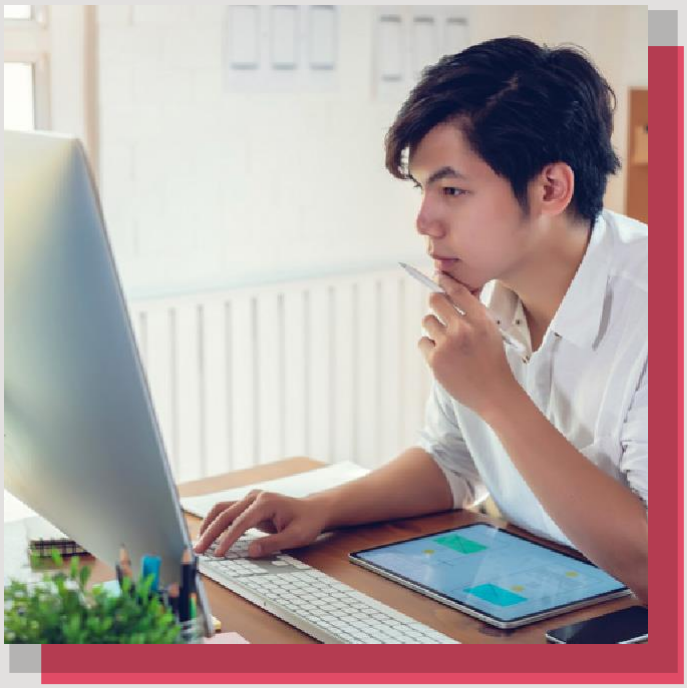
What is business-critical data?

This refers to any type of data within an enterprise that is vital and confidential to the operations of the enterprise, including personal data. They are usually classified and labelled based on their confidentiality and/or sensitivity level so that staff are aware of their confidentiality and/or sensitivity, where they are located, and the need to be careful in protecting such data in terms of data handling and/or disclosure.

Why is this important?

If business-critical data were to be exposed to unauthorised parties or personnel, it could lead to a detrimental impact.

Such data could be targeted by attackers to gain unauthorised knowledge and access to the organisation's system. Potentially, the data could also be held for ransom and/or be leaked publicly. These scenarios could disrupt business operations, cause loss of revenue for the organisation, and have an impact on its reputation or customer trust. There could also be legal and/or regulatory penalties, e.g. data breaches involving personal data.



How do I handle and disclose confidential and/or sensitive data carefully?

Confidential and/or sensitive data should be identified, classified, and protected with sufficient measures to prevent any unauthorised disclosure.

It is recommended to establish and maintain a data inventory to identify and classify the risk level of the data throughout their life cycle from collection to disposal.

Step 1

Identify and classify confidential and/or sensitive data

Be aware of and adhere to the organisation's data management policy. This could potentially include:

- Policies to identify and manage confidential and/or sensitive data.
- Risk classification of confidential and/or sensitive data either digitallyor physically on the accompanying medium.
- Maintaining the organisation's data inventory which may include confidential and/or sensitive data, with information such as the description, data confidentiality and/or sensitivity level, location, and retention period.
- Inclusion of confidentiality disclaimers in emails to indicate that the content of the email should be read only by the original recipient, and that there shouldnot be any sharing of content with unauthorised personnels.

Step 2

Prevent unauthorised disclosure of confidential and/or sensitive data

You can handle and disclose confidential and/or sensitive data carefully by:

- Ensuring the recipient of the confidential and/or sensitive data is authorised to access the data.
- Maintaining a data flow diagram to have visibility of confidential and/or sensitive data flow between various processes, related systems, and users. For sample Personal Data Inventory Map templates, refer to PDPC's Guide on Developing a Data Protection Management Programme
- Accessing the confidential and/or sensitive data on a trustednetwork connection.
- Ensuring documents, spreadsheets and other repositories containing confidential and/or sensitive data are protected digitally (e.g. password protection) or physically (e.g. under lock and key).
- Ensuring secure disposal or anonymisation of confidential and/or sensitive dataonce they are no longer required or past their retention period.

Step 3

Act on your doubt

If you suspect any unauthorised or accidental disclosure of confidential and/or sensitive data:

- Immediately inform the recipient to delete the confidential and/or sensitive data.
- Report to your organisation's IT or security team on details of the disclosure such as what confidential and/or sensitive data could have been disclosed andto whom.
- If personal data is involved, refer to PDPC's Guide on Managing and Notifying Data Breaches

Work Onsite and Telecommute in a Secure Manner

How is working onsite and telecommuting different?

Working onsite is the traditional way of being physically present and working at the office location. On the other hand, telecommuting takes place beyond the traditional office space, where employees work at remote locations (e.g. from home or another country). Telecommuting is becoming more prevalent as companies strive to increase flexibility for employees. Both types of working models have their own set of advantages and disadvantages. For telecommuting, one of the biggest challenges is the increase in exposure to cybersecurity risks and threats.

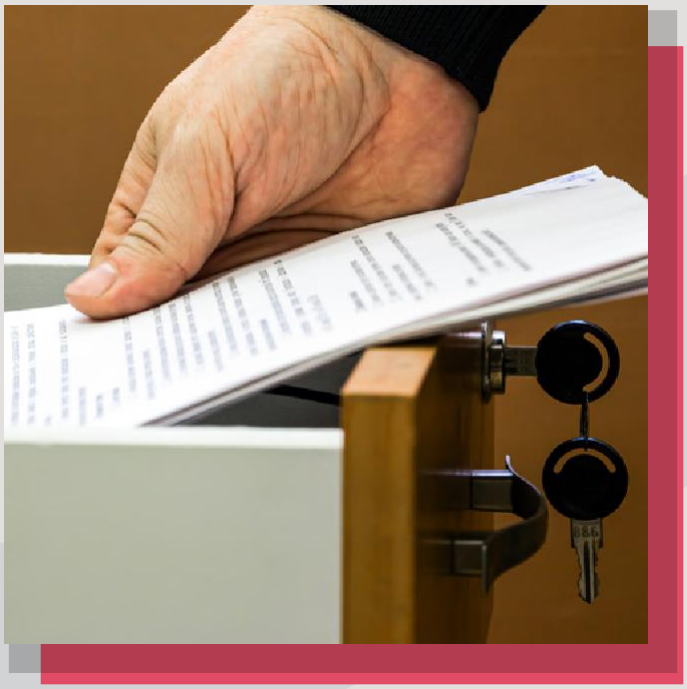
Why is this important?

Working onsite and telecommuting can each expose the enterprise to different types of cybersecurity risks. For example, working onsite could result in unintended data breaches when unauthorised personnel are within the premises of the organisation, whereas telecommuting can result in unauthorised access to business-critical data when employees connect to open and unsecured networks from the remote location.

The increasing trend towards telecommuting highlights the importance of cyber hygiene and cybersecurity awareness as opportunistic cyber threat actors may capitalise on the trend to conduct malicious cyber activities.

How do I work securely, whether onsite or at a remote location?

You can play your part to work onsite or telecommute in a secure manner by adopting good cyber hygiene practices. When working onsite, your organisation would manage the physical and cybersecurity of your work environment. When telecommuting, you would need to be aware of and take responsibility for your environment, such as the physical space or network connectivity. You should also understand the different types of cyber risks for both environments, especially when transitioning between the two working models.



Dos and don'ts of working onsite

The following will guide you on whether you have established good cyber hygiene practices when working onsite:

Good Practice

Adhere to clear desk and clear screen policy:

- Documents containing confidential and/or sensitive data are locked in the cabinet and not left unattended
- System/devices containing confidential and/or sensitive data are locked/displayed with a password-protected screen saver whenleft unattended

Look out for and report any suspicious visitorsin the work premises

Use a privacy screen to deter against shoulder surfing

Poor Practice

Work with/discuss confidential and/or sensitive data openly in publicly-accessible places in the office

Allow tailgating:

- Holding the door for or allowing unauthenticated personnel into the work premise

Dos and don'ts of telecommuting

The following will guide you on whether you have established good cyber hygiene practices when telecommuting:

Good Practice

Connect to a Virtual Private Network (VPN) when accessing your organisation's resources remotely:

- If a VPN is not available, connect only to secured networks, such as your personal Wi-Fi hotspot secured with a passphrase

When teleconferencing, use software that supports encryption and private meeting functions

For virtual meetings, generate a unique meeting room ID with password access:

- Require all participants to register themselves prior to the meeting
- Share the meeting ID and password with registered participants only
- Enable the waiting room feature and disable the option for attendees to join the meeting before the host

Poor Practice

Use of unsecured personal devices to access the corporate network:

- Personal devices typically are not as secured as corporate devices e.g. lack of anti-malware solution

Discuss confidential and/or sensitive topics openly in the presence of unauthorised third parties, e.g. your family members, during video conferencing

Contact Details

If you wish to find out more about CYBERSHIELD TEAM INC. ’s efforts in cybersecurity,please visit the following website or contact us:

info@Cybershieldteam.ac.tz

box 2958, dar es salaam

TANZANIA

CYBERSHIELD

WHERE AWARENESS UNLOCK SECURITY