BEWARE OF RANSOMWARE

Did you know?

Ransomware is a type of malware (malicious software) that criminals use to prevent you from accessing files on your computer, then demand a ransom in exchange for "release" of the files.

How does ransomware affect you?

First, the ransomware encrypts files on your computer or shared network drive, preventing you from accessing these files.

Next, the ransomware notifies you of the ransom payment process (usually in Bitcoin), in exchange for a decryption key to access your files again.

How can I protect myself from ransomware attacks?

Be Cautious
If you receive a suspicious email, do not click on links, download files or open attachments. Report the suspicious email to your IT department for investigation before deleting the email.

Be Careful of Links Provided in Unsolicited Emails
If you are accessing a hyperlink, do not click on it first. Hover your cursor over links or clickable buttons to show the actual URL. If there is a mismatch between the URL and the link, it could be a phishing link. Clicking on it could lead you to a phishing site or to download malware (such as ransomware).

Watch Out for Suspicious Activity
If you spot any suspicious activity on your computer, immediately disconnect from the network.

Always Back Up Your Data
Back up the data on your computer in a separate location for recovery purposes

Block Pop-Ups on Web Browsers
If an amazing offer or deal appears in a pop-up window, it is usually too good to be true, and may be a ransomware attack. Blocking pop-ups on your web browser can prevent these attacks.

STAY CYBER SECURE

Ransomware attacks are becoming more common, and often target individuals. Prevent ransomware attacks by staying cautious and aware of potential phishing (email-based) attacks!

If you are the victim of a ransomware attack do not panic, and alert your IT department immediately!

Keep in mind that paying the ransom in the event of an attack:

- Does not guarantee that you will have access to all files
- Encourages and funds illegal activities

An initiative by: MPA SINGAPORE CSA SINGAPORE

STRENGTHENING YOUR SOCIAL MEDIA SECURITY

Why do I need to keep my social media accounts cyber secure?

Most of us use social media today, and it is important to keep our accounts secure and personal information safe.

Malicious parties can access social media accounts or profiles to retrieve personal/sensitive data through a variety of ways, such as hacking accounts, posing as a friend, or through scams and viruses. What you share online could also potentially help hackers in password-guessing or formulating an email to be used in a scam.

Use these five tips to keep your social media accounts secure.

How can I use social media safely?

Manage Your Passwords

- Use **strong and complex passwords** i.e. at least 12 characters with uppercase and lowercase letters, numbers and symbols such as @, #, &, etc
- **Do not reuse** your passwords
- **Do not use** personal information in your passwords **(e.g. name, NRIC or birthdate)**
- **Enable** Two-Factor Authentication (2FA) when available

Manage Social Media Requests

- **Be wary of strangers,** they may not be who they say they are
- Consider **setting your account to private**
- **Speak to your friend in person** if they are acting out of character, asking for money or personal/sensitive data
- **Exercise Caution when Clicking on Links**

By following these tips, you can ensure safer use of social media yourself and in turn, your family and friends as well!

Be Wary of Spam

- **Be wary of "free" offers** that ask for your credit card details or personal/sensitive data, as these offers are usually scams

Share with Caution

- Be careful of what you share and **do not reveal personal/sensitive information**
- Never share your OTP* with anyone, including family and friends.

*One-time Password

Watch Out for Impersonation Scams

- Compromised accounts are used to impersonate friends/followers
- Scammers ask victims for their personal details **e.g. mobile number, internet banking account details, and OTP** on the pretext of helping them to sign up for lucky draws or contests

An initiative by:

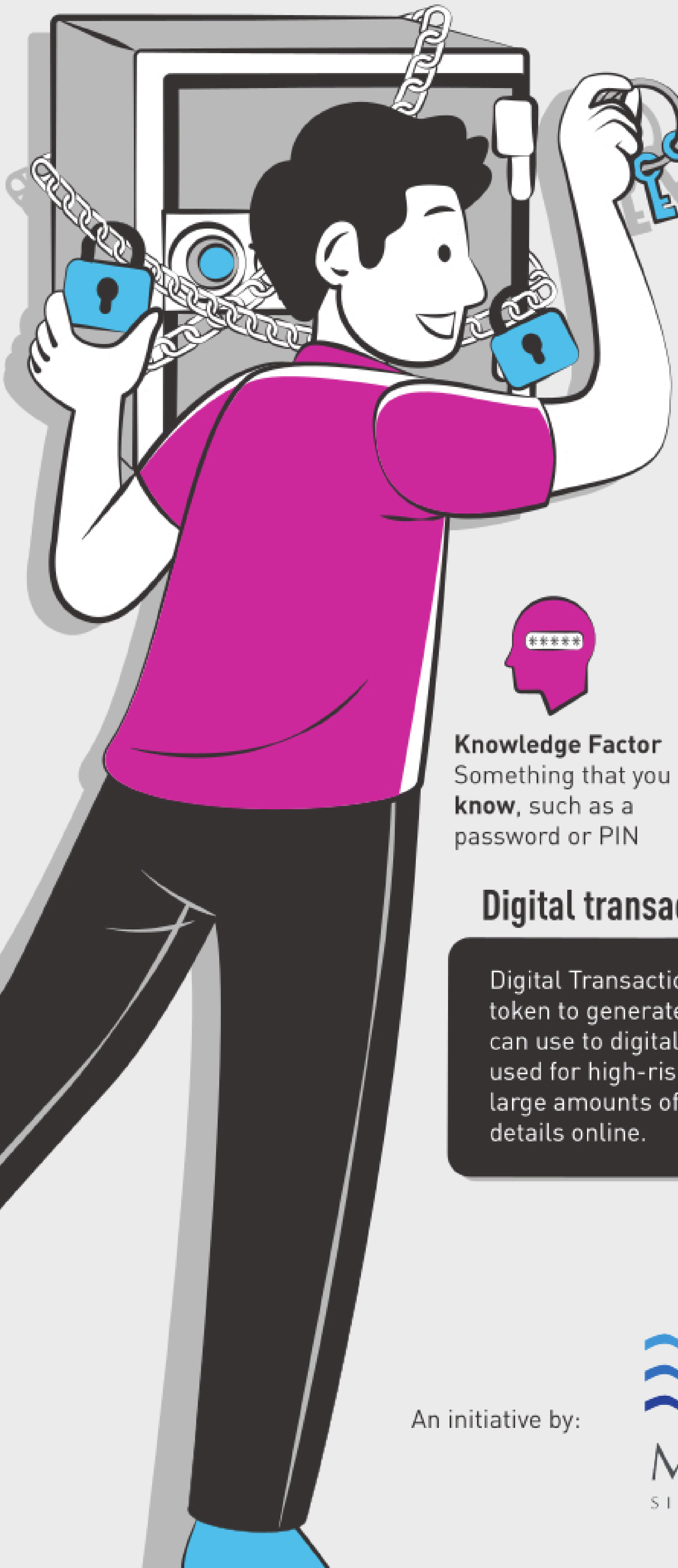
MPA SINGAPORE

CSA SINGAPORE

SAFE ACCESS WITH TWO-FACTOR AUTHENTICATION (2FA)

Did you know?

Cyber threats such as hacking and identity fraud on online systems and personal computers have become more common. Using Two-factor authentication (2FA) will help increase the security of your online accounts. Enable 2FA on your online accounts when available.



How does 2FA work?

Authentication is the process of verifying the identity of a person, and authenticating that the person is who they claim to be. When you are asked to provide 2FA authentication for a system or website, your identity is verified using two or more of the factors below:

Knowledge Factor
Something that you **know**, such as a password or PIN

Possession Factor
Something that you **have**, such as a security token

Inherence Factor
Something that you **"are"**, such as your fingerprint

Digital transaction signing

Digital Transaction Signing is when you use a 2FA security token to generate a One-time Password (OTP), which you can use to digitally "sign" your transaction. This is often used for high-risk transactions, such as when transferring large amounts of money or changing your personal details online.

An initiative by:

MPA SINGAPORE

CSA SINGAPORE

PRACTISING
GOOD CYBER HYGIENE

Did you know?

Cyber hygiene refers to good practices we can all adopt to improve cybersecurity of our devices and online accounts. We are responsible for our own cybersecurity. Prevention is key in the fight against cyber threats. Practising good cyber hygiene will ensure that we keep our devices and our information safe.

Here are some practices you can follow to stay cyber secure!

1. Use Strong Passwords and 2FA

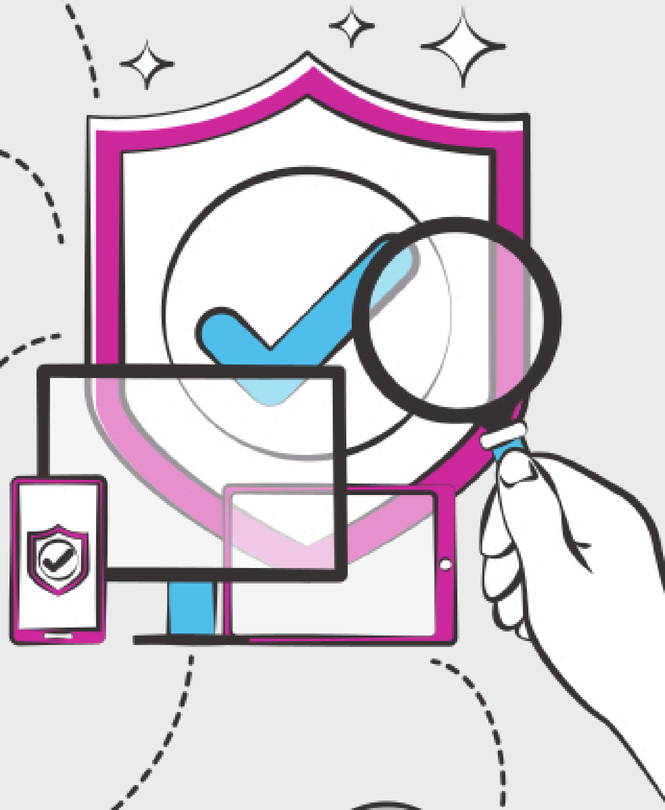
- Create passwords, using phrases, of at least 12 characters with uppercase and lowercase letters, numbers and symbols e.g. LearnttoRIDEabikeat5!
- Enable 2FA (Two-factor authentication) for your accounts where possible

2. Keep Personal Information to Yourself

- Don't share your personal information online, or use them in your passwords
- Don't reveal your actual location, or upcoming plans online as scammers could use this information for malicious purposes

3. If Uncertain, Don't Click On Links And Attachments

- Even known senders may unknowingly send you malicious links, so exercise caution before opening attachments or links on emails, social networking sites or messaging apps
- Links and email attachments may contain viruses, worms and Trojan horses that hackers can use for cyber attacks



4. Keep Your Security Software Updated

- Protect your device from latest malware with up-to-date security software
- Enable your computer's firewall to protect it from unauthorised access over the internet

5. Be Smart When Accessing Information Online

- Always check reliability and trustworthiness of information sources
- Do a fact check against other reliable sources

6. Watch Out for Online Scams

- Beware of online advertisements that sound too good to be true
- Check credibility of sellers before making payments
- Whenever possible, pay only upon delivery of items

An initiative by:

MPA SINGAPORE

CSA SINGAPORE

KEEPING YOUR SMART PHONE SAFE

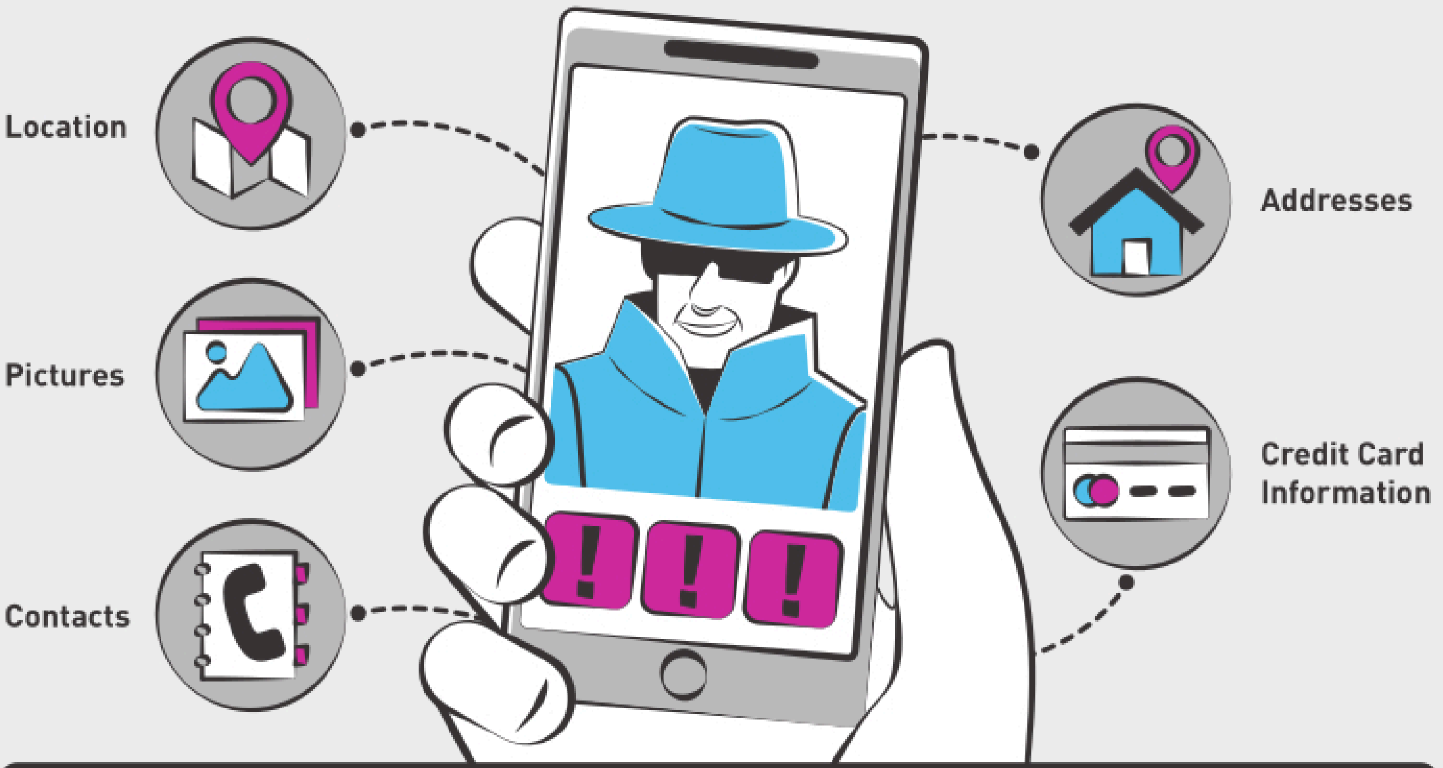
Mobile phones today have evolved beyond just a calling and messaging device. They are now mini computers we carry in our pockets which allow us to perform tasks such as access our email, browse the web and perform online transactions.

Is your phone safe?

Many think that their smartphones are relatively safe and not prone to cyber attacks. However, as the use of smartphones continues to grow, malicious apps have become more common.

What are malicious apps?

Malicious apps collect sensitive and private data from your phone. If you install a malicious app on your phone, hackers will be able to gain control of information on you such as your:



Here are some tips on how you can keep your phone safe from malicious apps!

- Always password-protect your phone so that your information is not easily accessed
- Update your phone's Operating System and apps regularly so that it contains the latest security and bug fixes
- Enable encryption on your phone to protect your data from unauthorised disclosure
- Turn your Wi-Fi and Bluetooth off when not in use so that hackers do not access your devices without your knowledge
- Back up the data on your phone for recovery purposes

An initiative by: MPA SINGAPORE CSA SINGAPORE

STRONG PASSWORDS

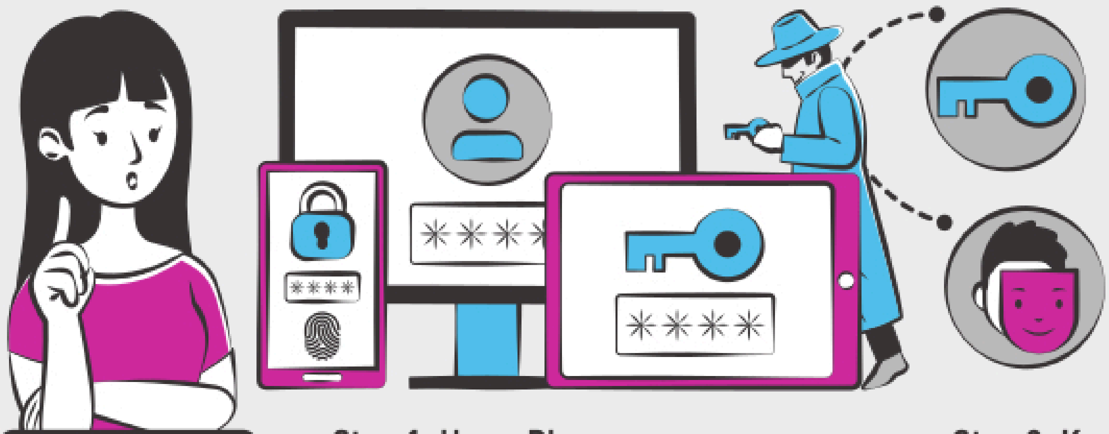
FOR SECURE ACCOUNTS

Passwords are the key to your digital life. As the first line of defence against cyber criminals attempting to gain access to your online accounts, your passwords should be secret and known only to you.

Why do you need a strong password?

Weak passwords, while easy for us to remember, can be easily guessed by cyber criminals. You may lose your online accounts, important personal information and even your finances, especially if you use the same password across many accounts.

For example, if cyber criminals gain access to your email account, they can use it to:



Access your other online accounts

Impersonate you and carry out scam-related crimes on people you know

How can you create a strong password?

Step 1: Use a Phrase

- Think of a phrase relating to a memory that is unique to you and at least 12 characters **e.g. learnttorideabikeatfive**
- Do not use personal information such as your name, NRIC or birthdate, or other information that can be obtained easily, for instance by doing a search online

Step 2: Keep it Random

- Use uppercase and lowercase letters, numbers and symbols to make your password even more difficult to crack e.g. LearnttoRIDEabikeat5!
- Keep it random by ensuring that your password does not have a pattern and is unpredictable

Maintaining good password hygiene

Here are some tips on how to protect your passwords:

Use different passwords for different accounts

Keep your passwords secret — do not share them with anyone or write them down

Do not log in to online services over unsecured or public Wi-Fi networks

Do not provide your passwords or OTP in response to a phone call, email or suspicious website as it could be a phishing scam

(OTP: One-time Password)

If you believe that your password has been compromised, change it immediately and check for signs of unauthorised activity

Don't wait till it is too late. Start using strong passwords and enabling 2FA (Two-factor authentication) for your online accounts today!

An initiative by:

MPA SINGAPORE

CSA SINGAPORE

KEEP YOUR ACCOUNTS SAFE WHEN BANKING ONLINE

Did you know?

In late 2015, mobile banking users in Singapore lost thousands of dollars after falling victim to malicious software (malware) that targeted Android phones. Cyber criminals made use of malware to gain access to users' banking credentials to make fraudulent financial transactions.

Bank Phishing Scam

- Scammers would call victims via mobile chat apps, claiming to be bank staff.
- In some cases, victims respond to SMSes that claim that their ATM card has been suspended or locked, and for them to call a specific number for activation.
- In all cases, scammers asked for victims' personal information and One-time Passwords (OTP) and victims subsequently discovered unauthorised transactions in their bank accounts.

Here are some simple tips to stay safe while banking online:

One-Time Password

- One-time Passwords (OTP) are used by banks as part of Two-factor authentication (2FA) to access your accounts
- **Use a separate device**, that only you can access, to receive your OTP so that even if a cyber criminal has access to your main device, they will not be able to access the OTP to complete the transaction
- **Never give out** your OTP to anyone, including family and friends

Secured Wi-Fi

- Cyber criminals can capture information passing through unsecured Wi-Fi networks, including your bank credentials
- **Use your own home network or mobile data network** to avoid using unsecured Wi-Fi networks when performing mobile and online banking, or other financial transactions

Bank Notifications

- Set up email or SMS notification alerts for your online banking transactions, so that you can be alerted to any suspicious activity
- **When in doubt regarding requests** that you received from banks through SMSes, emails or phone calls, always contact the banks through their official hotline for verification

An initiative by: MPA SINGAPORE CSA SINGAPORE

PROTECT YOURSELF WHEN
SHOPPING ONLINE

As online shopping becomes increasingly popular, especially amongst those who wish to save time and money, cyber criminals are also doing their own "online shopping" – exploiting consumers who do not practise good cyber hygiene.

It is therefore important to take the necessary precautions to stay safe when shopping online. Here are some tips on how to protect yourself and avoid scams and frauds:

	Payment Methods	Offers that are Too Good to be True	Unsecured or Public Wi-Fi
Look Out For	• **Credit cards** offer greater fraud prevention and protection, as banks can withhold payment to the merchant in the case of fraudulent transactions • Debit card purchases, on the other hand, withdraw money straight from your account • **Escrow payment** services only release the payment to the seller upon delivery of the item	• Online shopping sites tend to offer attractive deals during festive occasions or promotions • Cyber criminals can take advantage of this to carry out scams as consumers may let their guard down	• Cyber criminals can capture information, such as your bank credentials, passing through unsecured or public Wi-Fi networks
What should I do?	• Pay with a credit card instead or opt to use the escrow payment (when available)!	• Be wary of offers that sound too good to be true. Check that they come from legitimate companies!	• Use your home network or mobile data to perform financial transactions instead of unsecured public Wi-Fi networks!

	Two-Factor Authentication	Credit Card Information	Phishing or Bogus Sites
Look Out For	• Two-factor Authentication (2FA) provides extra protection for account logins and online transactions • 2FA can also alert you to fraudulent transactions or unauthorised login attempts	• Online shops and your browser may offer to store your credit card details for future transactions • Your stored credit card information may be stolen if there is a data breach	• Cyber criminals can create websites that mimic legitimate websites, to trick people into revealing personal information • Look carefully for subtle differences in website addresses e.g. www.amazon.com instead of www.amaz0n.com
What should I do?	• Enable 2FA for online transactions when available!	• Do not store your credit card information online or provide such details over email or the phone!	• Be vigilant against phishing or bogus sites! Do not click on URL links provided in unsolicited text messages and always verify with the official website or sources.

An initiative by:

MPA
SINGAPORE

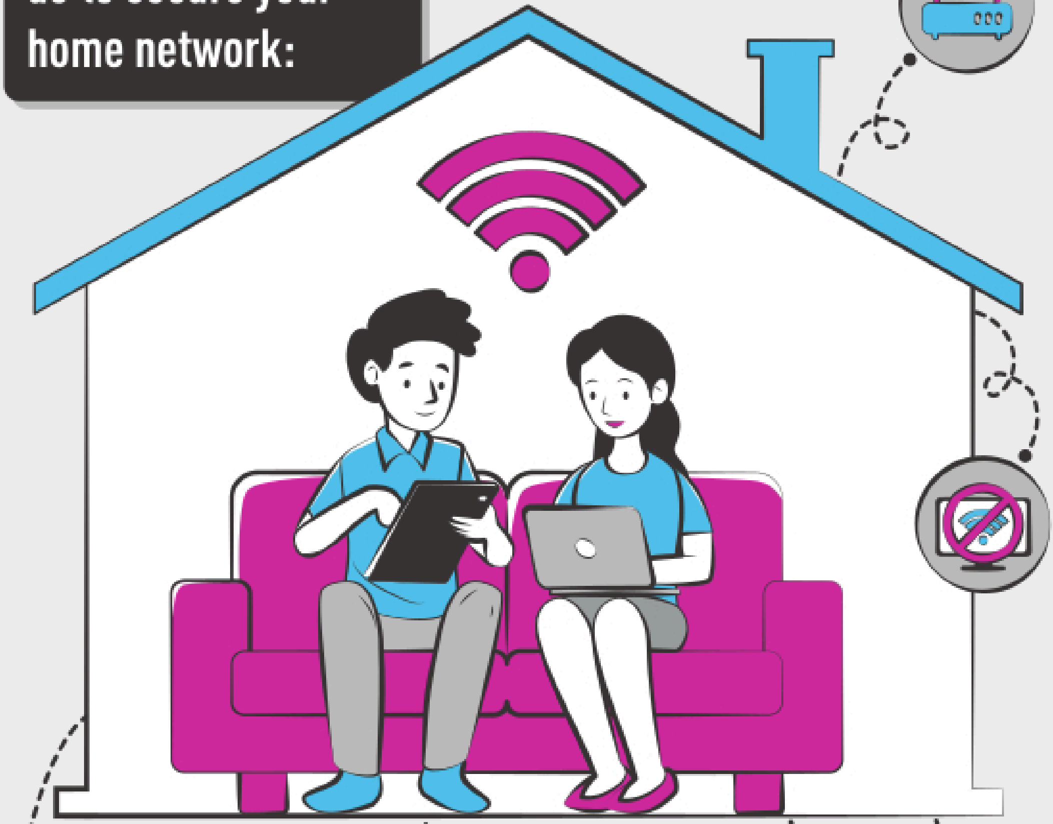
CSA
SINGAPORE

KEEP YOUR HOME CYBER SECURE

Our home wireless networks form the base of every single digital connection — from surfing the internet on our computers or mobile phones, to using smart appliances in our homes. Therefore, if our wireless network is poorly secured, this puts all our connected devices at risk to malicious cyber attacks.

Let's find out how we can improve cybersecurity at home!

Here's what you can do to secure your home network:



Change the default network name — SSID (Service Set Identifier) — on your router

The SSID provides information on the type of router you are using, which allows cyber criminals to exploit known vulnerabilities of your router's model

Disable Remote Access on your router

Leaving Remote Access enabled could potentially allow malicious attackers to access the router's settings, if they can guess the network administrator's password. This opens up opportunities for malicious attackers to launch further attacks

Use strong passwords to secure both your network and the network administrator account

Passwords should be random, at least 20 characters long, and include uppercase and lowercase letters, numbers and symbols e.g. LearnttoRIDEabikeat5!

Keep software up-to-date on your device

As far as possible, select Wi-Fi devices with in-built automatic updating features

Place the wireless router as close as possible to the centre of your house

Placing the wireless router in a central location minimises access and exposure outside your home

Activate Network Encryption to increase your Wi-Fi security

Use the latest encryption languages on your devices such as WPA2 or WPA3 when available

An initiative by: MPA SINGAPORE CSA SINGAPORE