Module 1: Cybersecurity

Learning Outcome

1. Have knowledge on common cybersecurity threats online (e.g. phishing, malware, scams) and tips on staying safe online
2. Able to spot signs of phishing; create strong passwords and use two-factor authentication (2FA)
3. Understand the tips for using E-payment solutions
4. **Activity: Share 1-2 tips on cybersecurity, use CSA-password checker to check if password is strong, spot signs of phishing etc.**

What is Cybersecurity?

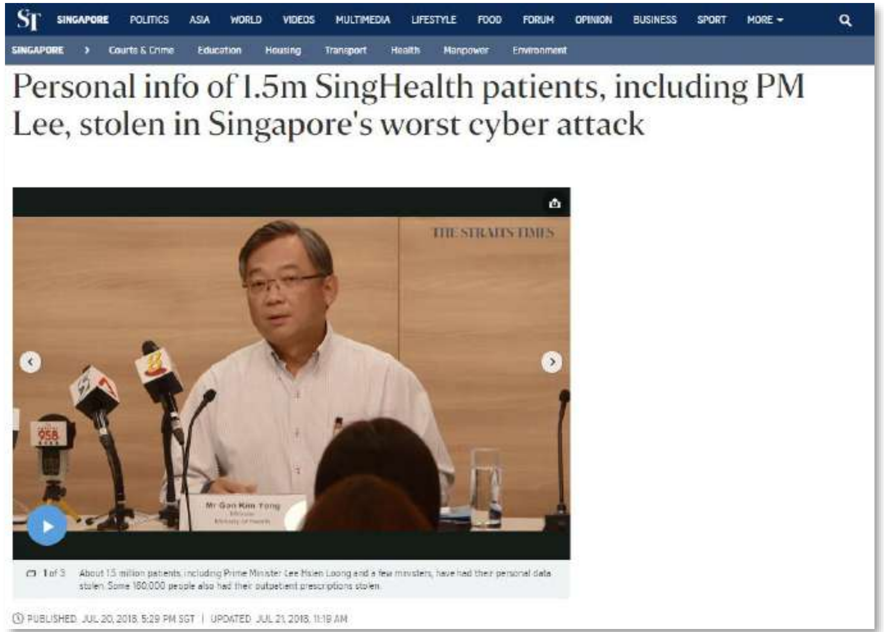
- Cybersecurity is the practice of protecting your internet-connected devices and systems from cyber incidents.
- With the increasing population owning a smart device, we are at a higher risk of being exposed to cyber incidents.

Do What's Right: Be Safe

https://tinyurl.com/dwrbs

Watch a video by scanning the QR code above to learn more about staying safe online!

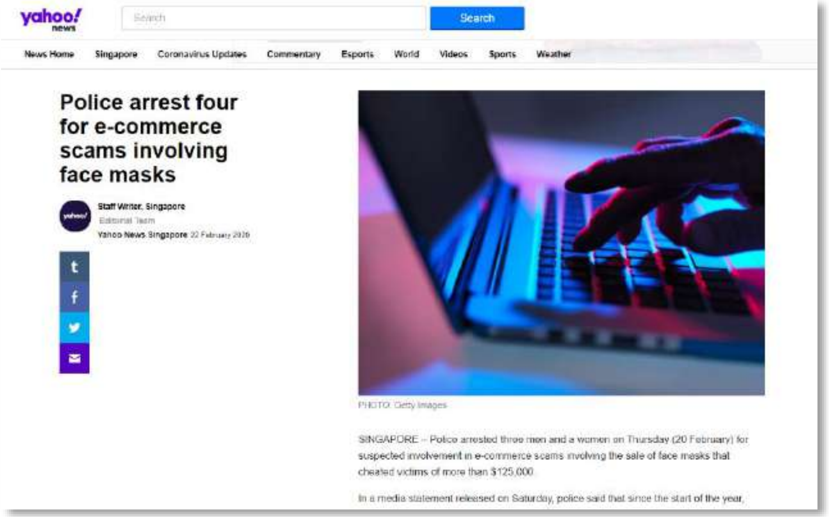
Cyber Incidents in Singapore


ST SINGAPORE POLITICS ASIA WORLD VIDEOS MULTIMEDIA LIFESTYLE FOOD FORUM OPINION BUSINESS SPORT MORE
SINGAPORE > Courts & Crime Education Housing Transport Health Manpower Environment
THE STRAITS TIMES
Mr Gan Kim Yong

Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

1 of 3 About 1.5 million patients, including Prime Minister Lee Hsien Loong and a few ministers, have had their personal data stolen. Some 160,000 people also had their outpatient prescriptions stolen.

PUBLISHED JUL 20, 2018, 5:29 PM SGT | UPDATED JUL 21, 2018, 11:19 AM


yahoo! news
Search
Search
News Home Singapore Coronavirus Updates Commentary Esports World Videos Sports Weather

Police arrest four for e-commerce scams involving face masks

Staff Writer, Singapore
Editorial Team
Yahoo News Singapore 22 February 2020

PHOTO: Getty Images

SINGAPORE – Police arrested three men and a women on Thursday (20 February) for suspected involvement in e-commerce scams involving the sale of face masks that cheated victims of more than $125,000.

In a media statement released on Saturday, police said that since the start of the year,

the new paper
NEWS SPORTS ENTERTAINMENT LIFESTYLE RACING
YOUR TIP-OFFS READ E-PAPER
POPULAR: COURT & CRIME Food & Drink
SINGAPORE
KFC JUST A CLICK AWAY

130% rise in number of e-commerce scams involving electronics: Police

Osmond Chia
Apr 22, 2020 06:00 am

The number of e-commerce scams involving electronic products, such as mobile phones and games consoles, has jumped, said the police on Tuesday.

Between January and March, at least 531 such reports were made, with total losses amounting to over $380,000.

The police said in a press release this marks a 130 per cent increase in the number of reports received compared to the same period last year and a 44 per cent increase in the total amount lost.

Mobile phones were the most common product involved, amounting to almost half of the cases.

Airpods and game consoles made up 17 per cent and 13 per cent of the cases reported respectively, while the remaining cases were related to laptops, television sets and other devices.

GRAB CREDITS, IPHONES

TOP STORIES THIS MONTH

SINGAPORE
MBS not renewing contracts of some foreign employees

SINGAPORE
Singaporeans to get up to $1k in payouts this month

S'pore woman loses S$94,000 to scammers over 3 days, only realises when police calls to tell her

The scammers identified themselves as officers from Singtel and the CSA, and sought her cooperation to catch hackers who supposedly compromised her IP address.

Nigel Chua | June 05, 2020, 08:33 PM

误坠诈骗集团圈套

帮'网安局'捉骇客 女老板反遭骗17万

3天6次转账给对方 银行助追回7万6000元

涂健强 报道
thorkk@sph.com.sg

▶警方提醒公众不要轻易听从来电指示安装"Teamviewer"或"Anydesk"等电脑程序，这些电脑程序能让骗子远程操控受害者的电脑。（档案示意图）

帮忙设圈套反中圈套，女老板无辜损失超过9万元！一名冒充新加坡网络安全局官员的骗子，请女老板联手设圈套抓骇客，要女老板三天内进行六次银行转账约17万元以便让骇客上钩。岂料两天后女老板接获反诈骗中心电话才得知自己上当，银行成功帮她取回7万6000元，但仍损失逾9万元。

在本地工作20年的芭芭拉（61岁，企业咨询公司老板）于4月15日接到自称是新电信职员打来的电话，通知她网络地址（IP）被骇客盗用来进行转账，并说会有网安局人员联络她。

芭芭拉今早受访时说："我是新电信长达20年的客户，所以接到电话时没有怀疑，过后一个自称是网安局人员的男子打给我，叫我跟他们合作设圈套抓骇客，我也答应了。"

对方先是请她安装Teamviawar电脑程序，这程序让骗子能够远程操控她的电脑，然后骗子叫她上网转账以便引骇客上钩。芭芭拉在三天内进行了六次转账，总数约17万元，有时是她亲自转账，有时则是骗子自己动手，她只提供资料和一次性密码。

她说："两天后我接到反诈骗中心的电话，告知银行职员发现我的户头有异常转账交易，我才惊觉被骗了。"

芭芭拉是通过两家银行进行转账，银行职员成功阻止四个转账，取回约7万6000元，另两个转账交易则已经过账，当中包括最大笔的转账，那是把6万5000美元（约9万1000新元）转到位于香港的中国银行户头，另一笔追不回的转账则约3000新元。

根据警方数据，冒充本地电信服务业者或政府机构人员提供技术援助是骗子常用的伎俩，今年第一季警方至少接到125起相关报案，涉及金额高达450万元。

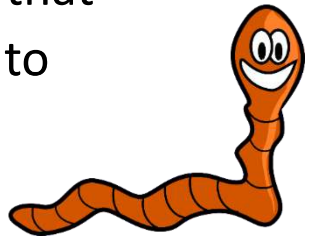
Content provided by the Cyber Security Agency of Singapore

Common Cyber Threats

Malware: Short for malicious software, these are programmes devised to compromise the security of a computer system. They can come in the form of:

- **Ransomware:** This malware locks the files in your computer, rendering your files inaccessible until a ransom is paid.
- **Virus:** A programme that can copy itself and spread quickly like real-life viruses.
- **Adware:** Devised to pop-up unwanted advertisements on the victim's computer, the pop-ups tend to behave erratically and is tedious to close them.
- **Worm:** The Worm virus is a malicious code that copies itself and makes use of the network to spread to other devices.

- **Trojan Horses:** A malicious programme hidden within a legitimate software. Once downloaded, it will install itself and run automatically.
  - **Banking Trojans** attempt to steal a victim's banking credentials once their device is infected.



Content provided by the Cyber Security Agency of Singapore

Common Cyber Threats

Common signs and symptoms of infection:

- Slowing down of your computer, programmes and internet connection
- Unanticipated frequent system or programme crashes
- Unexpected decrease in disc space
- Your screen is bombarded with pop-ups of unwanted advertisements
- Blocked access to your own system and ransom is demanded
- Friends complaining of receiving strange messages from you

Cyber Threats can also come in the form of a Phishing Attack. They are often designed to appear as though they are from familiar persons or companies, such as your bank or e-mail service provider.

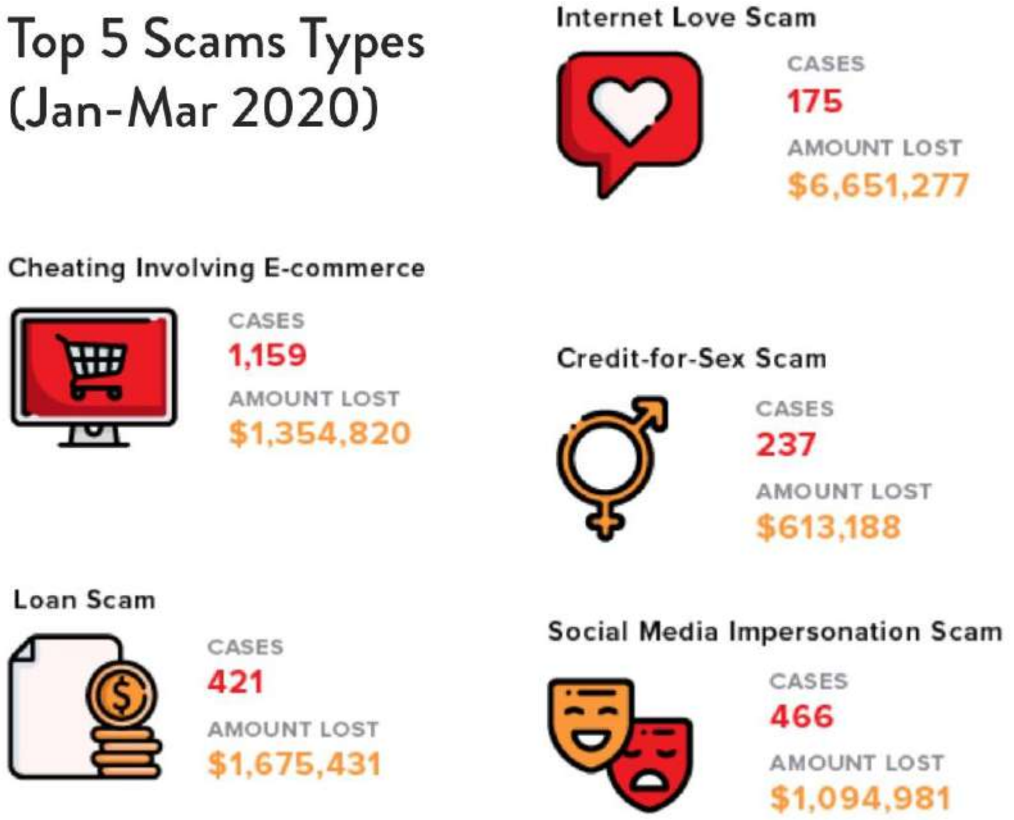
Webmail
Duplics
Yahoo
Tigerair
Dropbox
Match.com
Facebook
AOL
SeniorPeopleMeet
Canada Revenue Agency
AT&T
Verizon
Amazon
Microsoft
Netflix
Capitalone
Etisalat
LinkedIn
USAA
PayPal
Ebay
Internal Revenue Service
Google
Groupon
Expedia
Santander
Norton
DHL
Apple
Alibaba
Immigration & Checkpoints Authority of Singapore (ICA)
Inland Revenue Authority of Singapore (IRAS)
Ministry of Manpower (MOM)
Singapore Police Force (SPF)
@

Commonly-spoofed websites

Content provided by the Cyber Security Agency of Singapore

Online Scams on the Rise

www.scamalert.sg was launched by the police and the National Crime Prevention Council (NCPC), as part of an anti-scam public education campaign.



Top 5 Scams Types (Jan-Mar 2020)

Cheating Involving E-commerce
CASES
1,159
AMOUNT LOST
$1,354,820

Loan Scam
CASES
421
AMOUNT LOST
$1,675,431

Internet Love Scam
CASES
175
AMOUNT LOST
$6,651,277

Credit-for-Sex Scam
CASES
237
AMOUNT LOST
$613,188

Social Media Impersonation Scam
CASES
466
AMOUNT LOST
$1,094,981

Visit www.scamalert.sg to learn more about:

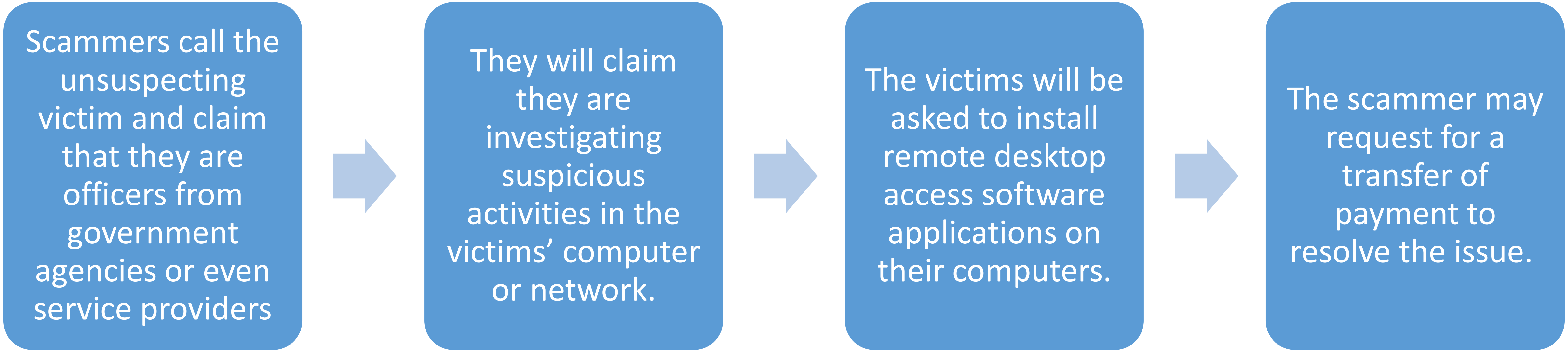
- What is a scam?
- Different types of scams.
- Stories shared by others of their experiences.
- News of scams.
- Helpline and resources (blog/posters/videos).

Content provided by the Cyber Security Agency of Singapore

What is a Scam?

Scam: Scheme or swindle to cheat a person of their money and valuable possessions. Perpetrators may also use phishing tactics to scam victims.

Scammers often lie to the victims in order to trick them into handing over their personal and bank account details. e.g. Tech support impersonation scam



Scammers call the unsuspecting victim and claim that they are officers from government agencies or even service providers

They will claim they are investigating suspicious activities in the victims' computer or network.

The victims will be asked to install remote desktop access software applications on their computers.

The scammer may request for a transfer of payment to resolve the issue.

For more information, please visit https://scamalert.sg/types-of-scams/

Content provided by the Cyber Security Agency of Singapore

Tips To Protect Yourself From Scams

- Scammers will use topics of interest to lure victims (e.g. COVID-19, low-interest loans, free gifts/vouchers).

- Watch out for calls from an unknown number and prefixed with a plus (+) sign, indicating that it is likely an overseas call.

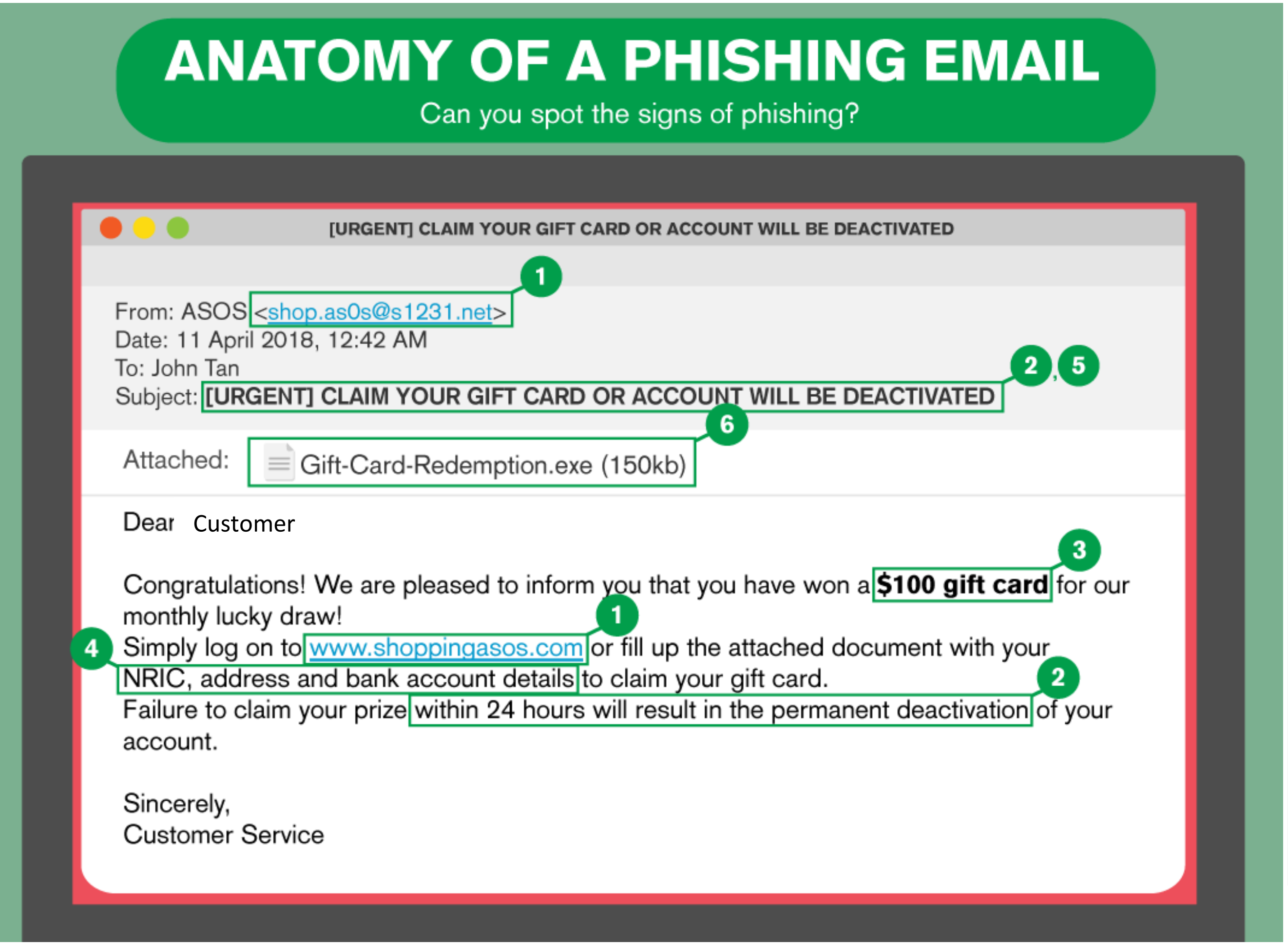
- Do not follow any instructions to install any software or applications on your device.

- Do not disclose personal or financial details over the phone.

- Do not make any transfers or payment. Government agencies will not ask for your details or request any payment for services rendered over the phone. If unsure, please hang up and contact the agencies directly for verification.

Content provided by the Cyber Security Agency of Singapore

How to Spot Signs of Phishing



ANATOMY OF A PHISHING EMAIL

Can you spot the signs of phishing?

[URGENT] CLAIM YOUR GIFT CARD OR ACCOUNT WILL BE DEACTIVATED

From: ASOS <shop.as0s@s1231.net>
Date: 11 April 2018, 12:42 AM
To: John Tan
Subject: [URGENT] CLAIM YOUR GIFT CARD OR ACCOUNT WILL BE DEACTIVATED

Attached: Gift-Card-Redemption.exe (150kb)

Dear Customer

Congratulations! We are pleased to inform you that you have won a **$100 gift card** for our monthly lucky draw!
Simply log on to www.shoppingasos.com or fill up the attached document with your NRIC, address and bank account details to claim your gift card.
Failure to claim your prize within 24 hours will result in the permanent deactivation of your account.

Sincerely,
Customer Service

1
2, 5
6
3
1
4
2

1
www.onlinebanking.com
http://www.wq31.data.net
2
[URGENT]
CLICK NOW!!!
SIGN UP NOW!
3
$50 VOUCHER
$
4
5
6

1 Mismatched and misleading information

2 Use of urgent or threatening language

3 Promises of attractive rewards

4 Requests for confidential information

5 Unexpected emails

6 Suspicious attachments

Content provided by the Cyber Security Agency of Singapore

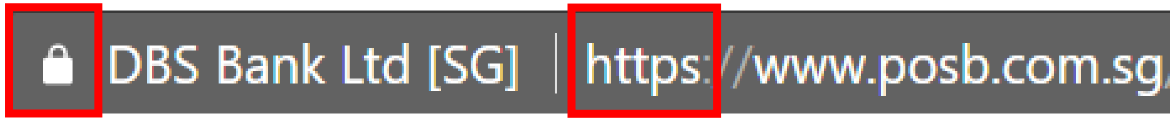
Tips To Protect You Against Fake/Phishing Websites

1 Check that the URL is correct before login

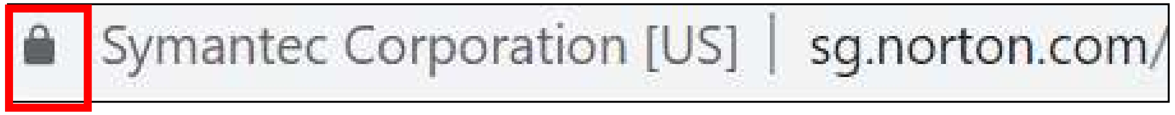
2 Secure website - “**https**” rather than “**http**”

“**https**” - Provides an additional layer of encryption often used for online payment transactions.

ⓘ Secure websites usually have a padlock icon.



DBS Bank Ltd [SG] | https://www.posb.com.sg/



Symantec Corporation [US] | sg.norton.com/

3 Purchase or download Apps from official or reliable websites.

ⓘ Visit below link or scan QR code to learn more about phishing.

How to protect yourself against spam and phishing

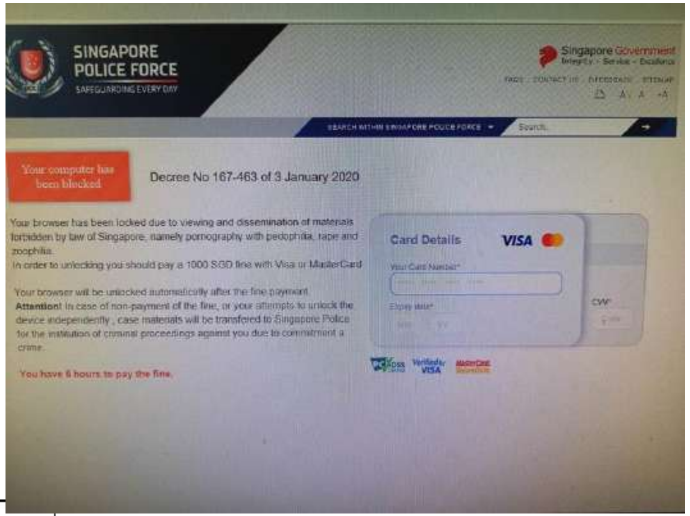
https://tinyurl.com/phishingtips

Content provided by the Cyber Security Agency of Singapore

Tips To Protect You Against Fake/Phishing Website

- Cyber criminals may also attempt to impersonate Government agencies to request for personal information

- Verify the legitimacy of these emails or websites by contacting the government agency directly.



Your computer has been blocked

Decree No 167-463 of 3 January 2020

Your browser has been locked due to viewing and dissemination of materials forbidden by law of Singapore, namely pornography with pedophilia, rape and zoophilia.
In order to unlocking you should pay a 1000 SGD fine with Visa or MasterCard

Your browser will be unlocked automatically after the fine payment.
Attention! In case of non-payment of the fine, or your attempts to unlock the device independently , case materials will be transfered to Singapore Police for the institution of criminal proceedings against you due to commitment a crime.

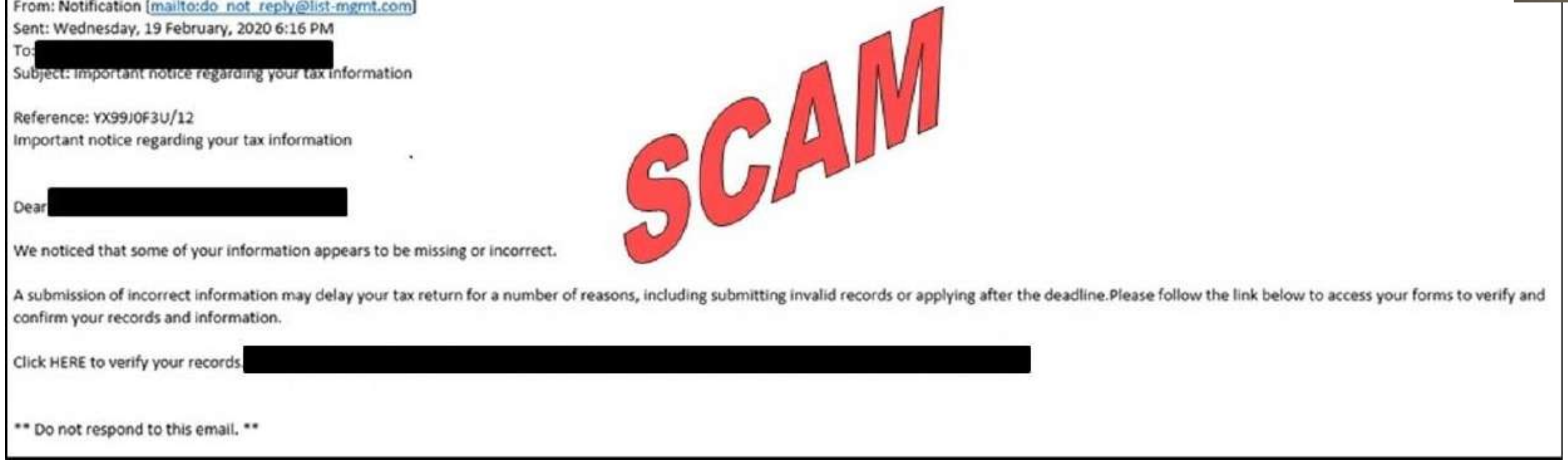
You have 6 hours to pay the fine.

Card Details

Your Card Number*

Expiry date*

CVV*



From: Notification [mailto:do_not_reply@list-mgmt.com]
Sent: Wednesday, 19 February, 2020 6:16 PM
To: [redacted]
Subject: Important notice regarding your tax information

Reference: YX99J0F3U/12
Important notice regarding your tax information

Dear [redacted]

We noticed that some of your information appears to be missing or incorrect.

A submission of incorrect information may delay your tax return for a number of reasons, including submitting invalid records or applying after the deadline.Please follow the link below to access your forms to verify and confirm your records and information.

Click HERE to verify your records [redacted]

** Do not respond to this email. **

Content provided by the Cyber Security Agency of Singapore

Tips To Protect You Against Malware

Dos

- Use Anti-Virus Software.
- Update your software regularly.
- If you suspect your account has been compromised, reset your password immediately and check for unauthorised transactions.

Don’ts

- Do not open unknown attachments.
- Do not trust pop-up windows that ask you to download software.
- Do not click on suspicious links or access suspicious websites.

Content provided by the Cyber Security Agency of Singapore

Installing An Anti-Virus App

- Search for anti-virus apps for your mobile phone, i.e. Apple App Store or Google Play.

  - ❑ At the minimum, your anti-virus app for your mobile phone should be able to scan and detect malware.

  - ❑ Some anti-virus options can only detect and quarantine malware, but may not remove viruses in your device. When searching for a suitable anti-virus app, look out for one which offers malware removal capabilities.

- Some internet service providers (ISPs) offer the service for a small monthly fee. Check with your ISP for details.

- Enable automatic software updates if the option is available so that you have the most up-to-date software to protect against the latest threats.

Content provided by the Cyber Security Agency of Singapore

How To Create A Strong Password

How to create long and random passwords that you can remember easily:

Step 1: Use five different words that relate to a memory that is unique to you (at least 12 characters) e.g. Ihadkayatoastat8am

Be sure not to use personal information such as your name, NRIC or birthdate, or other information that can be obtained easily by doing a search online

Step 2: Use uppercase and lowercase letters, numbers and symbols to make it even harder to crack. e.g.IhadKAYAtoastAT8am!

Remember to keep it random by ensuring that your password does not have a pattern and is unpredictable. It should be difficult for others to guess.

What to avoid:

- Using commonly used phrases e.g. Password1234
- Obvious patterns such as capitalising the first letter of the password e.g. Limfamily123
- Replacing a letter with an obvious number or symbol e.g. p@ssw0rd

Think you're ready to set a strong password?

Test your skills at:

https://go.gov.sg/csa-pwchecker

Content provided by the Cyber Security Agency of Singapore

Enabling Two-Factor Authentication (2FA)

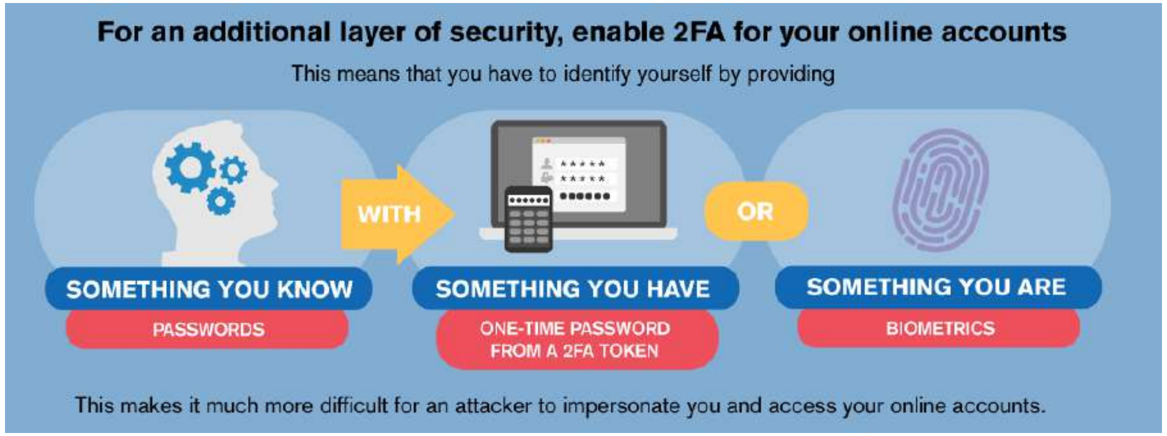
What is 2FA?

- 2FA uses more than one type of information to identify who you are in order to grant you access to your online account.
- 1st factor - usually something that you know, such as a password
- 2nd factor - something you have, such as a one-time password (OTP) from a physical OTP token
- Another factor involves biometrics (e.g. fingerprints and face recognition)

➡ A second layer of security ensures that even if a hacker obtains your password, your account is still protected if he is unable to get hold of a second factor

How do I enable 2FA?

- 2FA is readily available for many of your online accounts
- For step-by-step instructions on enabling 2FA for your online accounts, you can refer to TurnOn2FA


For an additional layer of security, enable 2FA for your online accounts
This means that you have to identify yourself by providing
WITH
OR
SOMETHING YOU KNOW
PASSWORDS
SOMETHING YOU HAVE
ONE-TIME PASSWORD FROM A 2FA TOKEN
SOMETHING YOU ARE
BIOMETRICS
This makes it much more difficult for an attacker to impersonate you and access your online accounts.

Content provided by the Cyber Security Agency of Singapore

Tips for Using E-Payment Solutions

- Use only official apps (e.g. mobile banking app).

- Set up bank transaction notification alerts; by setting up email or SMS notification alerts for your transaction so that you will be notified of any suspicious activity on your accounts.

- After scanning the QR code to make payment,
  - check if the correct apps/websites are launched. The apps/websites should be from the payment vendors.
  - check and confirm that the payment is made to the correct person/business you are buying goods or services from i.e. if the shop name is “ABC Pte Ltd”, the app should also show that you are making payment to “ABC Pte Ltd”.

More information on SGQR:
https://www.mas.gov.sg/development/e-payments/sgqr

Content provided by the Cyber Security Agency of Singapore

Tips for Using E-Payment Solutions

- **Keep your devices updated and clean -** Ensure that all the internet connected devices (including PCs, smartphones and tablets) are running on the most current version of operating systems (i.e. OS/iOS/Android), and installed anti-virus is also updated.

- **Use Strong Password and also Enable 2FA** – Enabling 2FA is especially important for any online transaction and account log-ins. This will prevent any fraudulent transactions from taking place.

- **Keep banking details to yourself** – Do not save your banking and personal details in your devices and websites. Type the information whenever you are making a transaction. Do not forget to log out every time after using the e-payment.

- **Beware when using Wi-Fi networks** – Wi-Fi networks are vulnerable to Wi-Fi spoofing by hackers. Do not make transactions involving personal or confidential information on unsecured Wi-Fi networks.

Content provided by the Cyber Security Agency of Singapore

Other Useful Tips

- **Be smart when assessing information online**
  Always check the source of your information, whether it is reliable or trustworthy and cross-check against other reliable sources to verify whether it is indeed a fact and not just an opinion.

- **Keep personal information to yourself**
  Don’t share your address, phone number or other personal information online. Don’t reveal your actual location or when you plan to be somewhere.

For More Information…

- To find out more about essential cybersecurity practices for individuals and organisations,
- visit **https://www.csa.gov.sg/gosafeonline**

- To subscribe to SingCERT alerts, please visit **https://csa.gov.sg/singcert/subscribe**

- Keep up with the latest cyber trends and tips by following us at:

facebook.com/CSAsingapore
facebook.com/gosafeonline

@gosafeonline

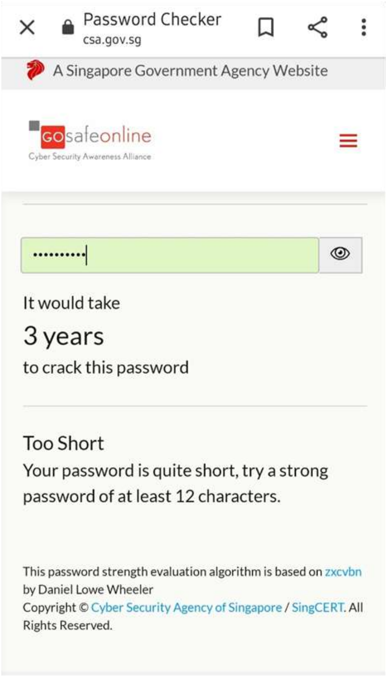
If you wish to provide any information related to scams, or if you have followed through to make payment, please call the Police hotline at 1800-2550-000 or submit it online at www.police.gov.sg/iwitness.

Content provided by the Cyber Security Agency of Singapore

Check your password

1 Let’s check if your password is secured!

- Visit https://go.gov.sg/csa-pwchecker
- Type in your password to check if it is strong.


Password Checker
csa.gov.sg
A Singapore Government Agency Website
GOsafeonline
Cyber Security Awareness Alliance

••••••••••

It would take

3 years

to crack this password

Too Short

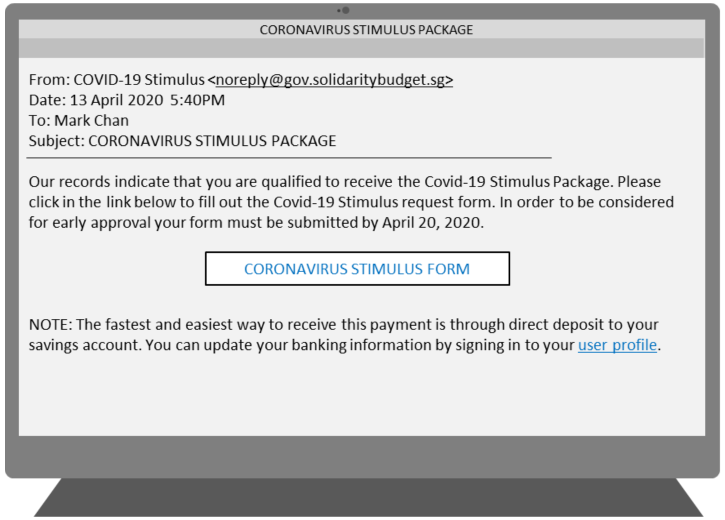
Your password is quite short, try a strong password of at least 12 characters.

This password strength evaluation algorithm is based on zxcvbn by Daniel Lowe Wheeler

Copyright © Cyber Security Agency of Singapore / SingCERT. All Rights Reserved.

Spot Signs of phishing

2 Can you spot signs of phishing?



CORONAVIRUS STIMULUS PACKAGE

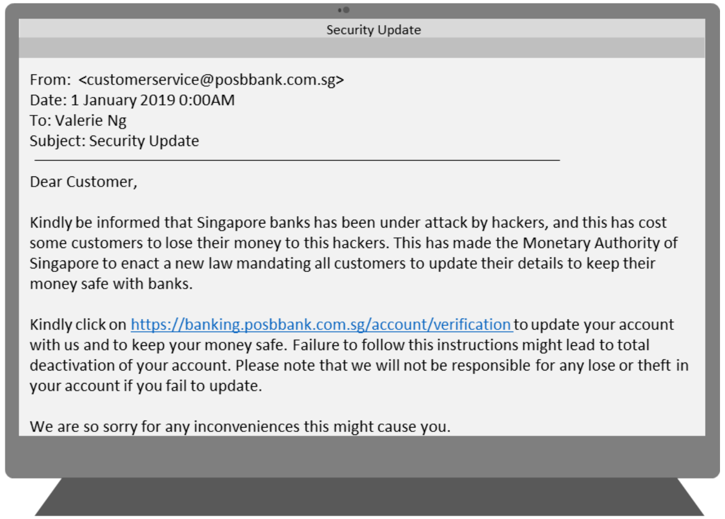
From: COVID-19 Stimulus <noreply@gov.solidaritybudget.sg>
Date: 13 April 2020 5:40PM
To: Mark Chan
Subject: CORONAVIRUS STIMULUS PACKAGE

Our records indicate that you are qualified to receive the Covid-19 Stimulus Package. Please click in the link below to fill out the Covid-19 Stimulus request form. In order to be considered for early approval your form must be submitted by April 20, 2020.

CORONAVIRUS STIMULUS FORM

NOTE: The fastest and easiest way to receive this payment is through direct deposit to your savings account. You can update your banking information by signing in to your user profile.

Example 1



Security Update

From: <customerservice@posbbank.com.sg>
Date: 1 January 2019 0:00AM
To: Valerie Ng
Subject: Security Update

Dear Customer,

Kindly be informed that Singapore banks has been under attack by hackers, and this has cost some customers to lose their money to this hackers. This has made the Monetary Authority of Singapore to enact a new law mandating all customers to update their details to keep their money safe with banks.

Kindly click on https://banking.posbbank.com.sg/account/verification to update your account with us and to keep your money safe. Failure to follow this instructions might lead to total deactivation of your account. Please note that we will not be responsible for any lose or theft in your account if you fail to update.

We are so sorry for any inconveniences this might cause you.

Example 2