



JANUARY - MAY 2021, ISSUE 1

THE CYBER ALERT

THE NEWSLETTER BY CCHY CYBER WELLNESS



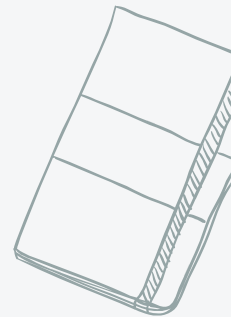


EDITOR'S NOTE

Cyber Alert is a newsletter designed to communicate and disseminate issues on cyber wellness for both adults and students. We want it to be entertaining and informative, at times reflective but above all useful.

You can take control if you take steps to protect and guard yourselves.

Enjoy reading!



WHAT'S INSIDE?

CYBER
THREATS

HOW TO
SECURE
DATA?

FEATURED
STORY





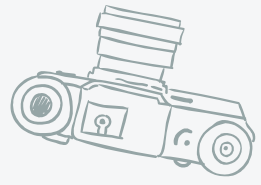
CYBER THREATS IN SINGAPORE

The Cyber Security Agency of Singapore (CSA) reported that cyber threats in Singapore grew in scale and complexity since 2019; targeting various local industries such as e-commerce, banking and finance.



“... there is no permanent fix nor absolute cybersecurity. It is a constant battle—against cunning adversaries with advanced capabilities.”

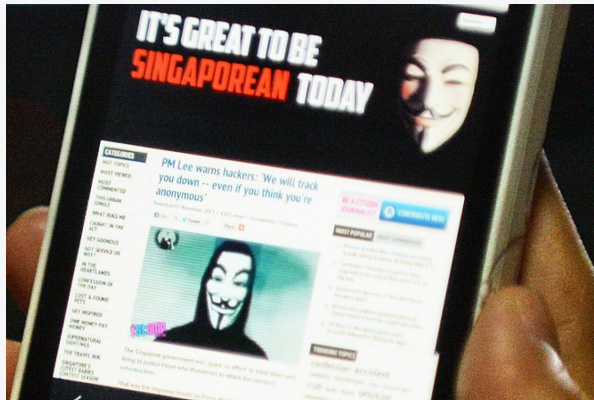
Statement by Mr S Iswaran, Minister-in-Charge of Cybersecurity during Parliamentary Sitting on 15 January 2019



LOCAL CASES

Website Defacement

An unauthorised modification of a website to change its visual appearance and/or to alter the hosted website information.



'Anonymous' website hacking on PM's Lee site in 2013

Phishing

A fraudulent attempt to obtain sensitive information or personal data such as credit card details, by disguising oneself as someone from a legitimate institution.

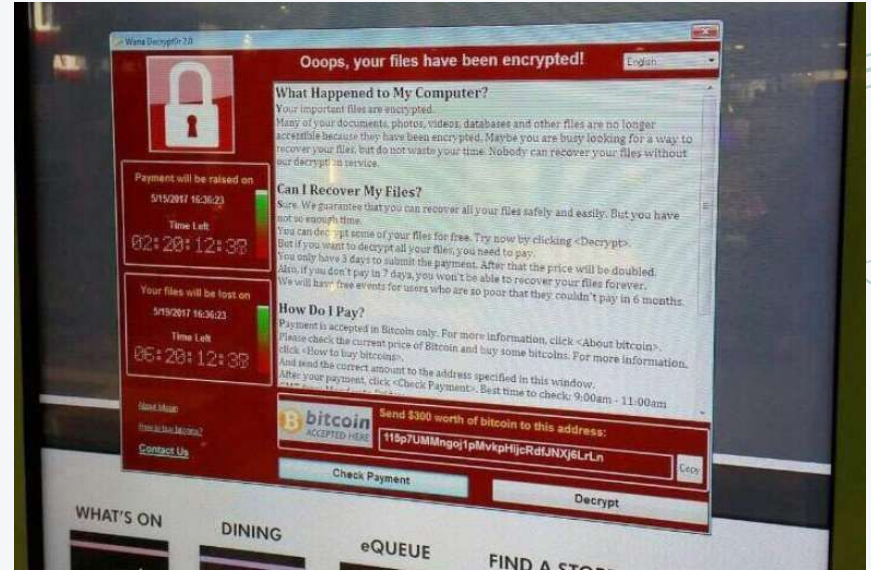


Screengrab of phishing SMS from SingPost, Image: SPF

LOCAL CASES

Malware Infections- Ransomware

A malicious software designed to block access to a computer system unless a ransom is paid.



A digital display at Tiong Bahru Plaza shows a ransomware message.
Image: Straits Time, 2017



HOW TO SECURE OUR DATA?

Some practical tips...





Do you use strong passwords for your accounts?

If you need to safely store passwords, look into a secure password manager.



Is your Wi-Fi connections encrypted?

Some public Wi-Fi connections are not encrypted which means you are at risk of people monitoring your online activities. Remember to turn on your firewall and have up-to-date malware protection.





Do you use **Two-Step Verification** synched to your mobile number for your account settings?

It provides extra protection by preventing unauthorised access to your mobile number and your linked accounts.



Is your **data backed up** to the cloud or a physical hard drive?

Backing up data is often overlooked but it remains a very important aspect of data protection.



DID YOU KNOW

on 12 June 2018

40,000

attacks were reported during

TRUMP-KIM SUMMIT

which made Singapore the top cyber attack target in a day!



Singapore's data privacy watchdog investigating customer data breach at ShopBack

Published Sep 26, 2020, The Straits Time



FEATURED STORY

SINGAPORE - Local authorities are investigating a data breach at homegrown e-commerce cashback platform ShopBack, after the firm made public an incident involving unauthorised access to customers' personal data.

A spokesman at privacy watchdog the Personal Data Protection Commission said it has been notified of the incident. "Investigations are ongoing," he added.

In an email to customers on Friday (Sept 25) evening seen by The Straits Times, ShopBack said that it became aware of unauthorised access to its systems which contained customers' personal data "a few days ago". It was still investigating what data had been compromised.



FEATURED STORY

"To date, we have no reason to believe that any of your personal data has been misused, however the possibility still exists," said the firm, apologising for the incident.

"What we can assure you is that your cashback is safe... Your credit cards are safe, as we do not store your 16-digit card number or CVV on any of our systems."

ShopBack said that it had immediately initiated an investigation after the incident came to light, and engaged leading cybersecurity specialists to assess the extent of the breach and also to further enhance its safety measures.

It added that it is currently working together with the authorities to investigate the extent of the damage.

FEATURED STORY

ShopBack said that customers' account passwords are encrypted, but suggested that they change them as an "added precautionary measure".

"We also suggest that you do not use the same password on other digital platforms," it said, while committing to taking steps to minimise the risk of a similar incident occurring again in future.

ShopBack accounts can still be used, as the platform's business operations have not been affected by the incident.

Customers can contact Shopback at care@shopback.sg if they have questions related to the incident.

FEATURED STORY

ShopBack user Cordelia Lee, 24, said she finds it unsettling at the lack of confirmation over what data was breached on the platform.

While she will be changing her account password, the design firm executive said: "I'm actually more concerned about how this happened, and am looking forward to the company sharing future steps in ensuring better securing their customer's data."

USEFUL LINKS



Cyber Security Agency of
Singapore @

<https://www.csa.gov.sg/>



Fact Sheet: Digital Defence

@

<https://www.mindef.gov.sg/>



101 Data Protection Tips @

[https://digitalguardian.com/
blog/101-data-protection-tip
s-how-keep-your-passwor
d-s-financial-personal-inform
ation-safe](https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe)



THANKS!

Any questions?

You can find me at:

nur_marlinda_aziz@moe.edu.sg

