

CYBER SECURITY TODAY: What it means for you



ANDY PRAKASH

Co-Founder | AntiHACK.me
CEO | Privacy Ninja

Safe Data. Empowered Business.

Co-hosted By:

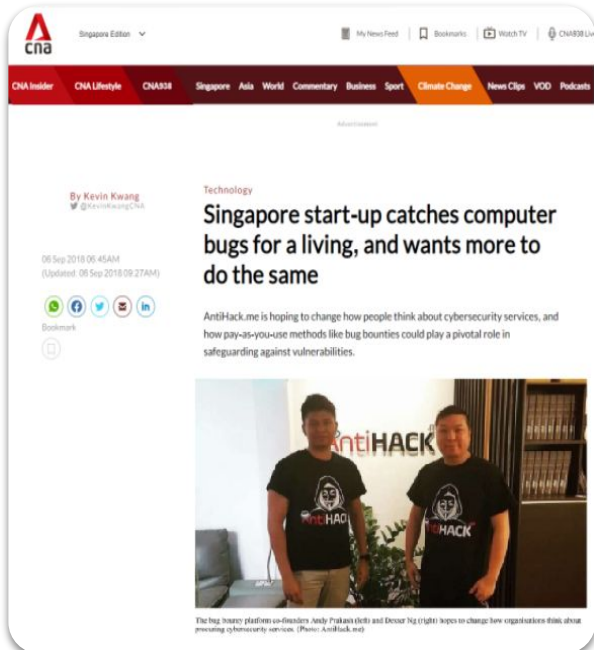


Privacy Ninja

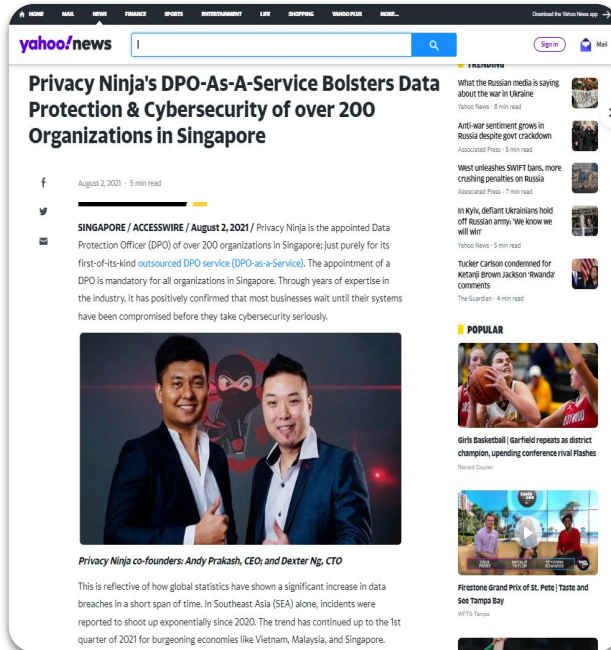
TRUSTED BY OVER 300 ORGANISATIONS IN SINGAPORE



STRENGTHENING THOUGHT LEADERSHIP | MEDIA FEATURES



Affordable Cybersecurity
Channel NewsAsia - Sep 2018



Outsourced DPO Service
Yahoo! News - Aug 2021




OCBC Bank Scam
Zaobao - Feb 2022

STRENGTHENING THOUGHT LEADERSHIP | MEDIA FEATURES

THE STRAITS TIMES SINGAPORE

More children cheated in game scams; counsellors urge peer support and parental supervision



Counsellors said they have seen an increase in the number of clients below the age of 16 seeking help after encountering scams. PHOTO BY FILE

Jessie Lim and Yeo Shu Hui

PUBLISHED MAR 6, 2022, 5:00 AM SGT


Mr Andy Prakash, co-founder of cyber-security firm Privacy Ninja, said that games which involve items that are highly rare and can only be obtained through loot boxes may incentivise children to take part in unsafe transactions.

Melody (not her real name), who was playing the game Murder Mystery on the platform, wanted to use the in-game credits to buy weapons to level-up her character.

Game Scams
Straits Times - Mar 2022

THE STRAITS TIMES SINGAPORE

Posting photos of your boarding pass could allow strangers to cancel your holiday



Mr Jason Ho created a TikTok video showing how easy it is to obtain personal details from a photo of a boarding pass. PHOTOS SCREENSHOTS FROM JASON HO'S TIKTOK

Jessie Lim

UPDATED JUN 22, 2022, 1:05 PM SGT


Mr Andy Prakash, co-founder of cyber-security firm Privacy Ninja, showed The Straits Times how by using these details, one can view someone's full name, passport number, e-mail address and mobile phone number.

It is also possible to see some details of a person's travel companions if the tickets are under the same booking.

Data Privacy
Straits Times - Jun 2022

THE STRAITS TIMES SINGAPORE

At least 93 victims lost \$56.2m to business e-mail compromise scams from Jan to March 2022: Police



Business e-mail compromise scams involve the sending of e-mails supposedly from the victim's colleagues, business partners or suppliers. PHOTO ILLUSTRATION BY FILE

Jessie Lim

PUBLISHED JUL 26, 2022, 6:03 PM SGT

Mr Andy Prakash, co-founder of cyber-security firm Privacy Ninja, noted how in such scams, recipients of these e-mails may not be able to spot any signs that the e-mail is spoofed, if they do not have phishing e-mail detection tools installed.

He said, "Using a software, scammers can send a victim an e-mail from an address which looks identical to the sender they are impersonating and unless you know how to identify the original sender found inside the metadata of the e-mail, you will not be able to spot the difference."

Business Email Compromise
Straits Times - July 2022

STRENGTHENING THOUGHT LEADERSHIP | MEDIA FEATURES



Channel NewsAsia - Bug Bounty



Interpol World - Cybersecurity



Echelon Asia Summit - Live Hacking



Channel 8 - GovWare



Channel 8 - Dark Web



Channel 8 - IoT Security



Live Hacking Demo at Echelon



Presentation at Interpol



Presentation at Chambers



Training Startups/Co-Working Spaces



Masterclass



Channel 8 - IoT Security

The Past Landscape

- Email threats were not yet as sophisticated as they are now
- Smart everything wasn't as prevalent (e.g. smartphones, smart appliances, etc.)
- The lines between personal and professional were not as blurred
- An emerging trend in cyber crime as a profitable business



The Present Landscape

- Unprecedented expansion of personal digital territory
- The lure of convenience, at the price of protection taking a back seat
- Blurred lines between personal and professional
- The rise of Ransomware-as-a-service

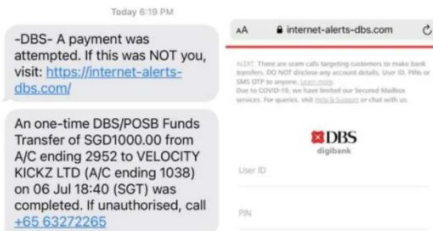




Types of Hacking & Their Impact on Individuals or Organisations

Singapore

New type of phishing scam targets bank customers with spoof SMSes: Police

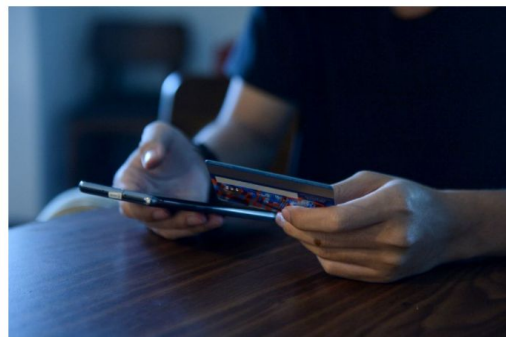


Screenshots of a spoof SMS (left) with a link directing victims to a phishing website (right). (Screenshots: SPF)

SINGAPORE: Banking-related phishing scams have re-emerged in the form of spoof SMSes that trick victims into thinking they were sent by their bank.

A total of S\$1.07 million was lost in 374 cases of such scams between January and May this year, said the Singapore Police Force (SPF) in a news release on Saturday (Jul 10).

Lured by \$2 payout, woman in S'pore lost over \$70,000 in job scam



The Singapore police advise people not to accept dubious job offers that offer lucrative returns for minimal effort. PHOTO: ST FILE

Yeo Shu Hua

PUBLISHED JUL 18, 2021, 5:00 AM SGT



SINGAPORE - All it took was a few clicks to like a few videos and comments on a social media page, and Amanda (not her real name) earned \$2.

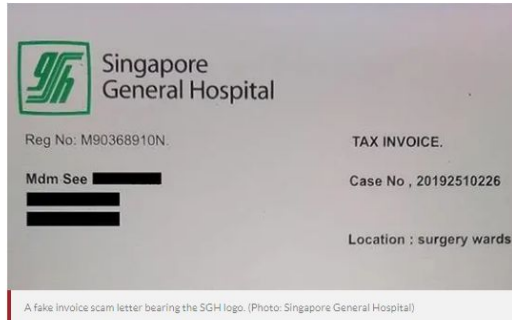
"I thought it was a pretty simple task," she said, adding that she was paid via PayNow.



Types of Hacking & Their Impact on Individuals or Organisations

Singapore

SGH files police report over fake invoice scam



SINGAPORE: The Singapore General Hospital (SGH) said on Saturday (Oct 26) that it has filed a police report over a fake invoice scam.

The hospital also cautioned members of the public against falling for such falsified documents.

Singapore

MOH warns of scammers impersonating its employees, COVID-19 contact tracing teams



SINGAPORE: The Ministry of Health (MOH) said it was aware of scammers using automated voice calls or impersonating its staff members and COVID-19 contact tracing personnel.

Fraudsters have requested personal information from people, including financial details; or have asked them to collect documents from the ministry, MOH said in an advisory on Friday (Mar 27).



Types of Hacking & Their Impact on Individuals or Organisations

Singapore

IN FOCUS: How ready is Singapore for a major ransomware attack?



FILE PHOTO: A man types on a computer keyboard in front of the displayed cyber code in this illustration picture taken on March 1, 2017. REUTERS/Kacper Pempel/illustration

SINGAPORE: Imagine being in a large, dark house - there are cameras, but you can't see in all the corners.

This is how Mr Eric Nagel, general manager for APAC at cybersecurity firm Cyberason, characterises the way the company hunted down a ransomware attack in a high-end Asian manufacturing company.

Shipping company loses \$1.8m from fraudulent payments in email scam



A shipping company has failed in an attempt to recover \$1.8m from Standard Chartered Bank that was paid fraudulently after an unknown third party accessed the client's email account in an apparent "whaling" scam.

Marcus Hand | Jan 10, 2018

THE STRAITS TIMES

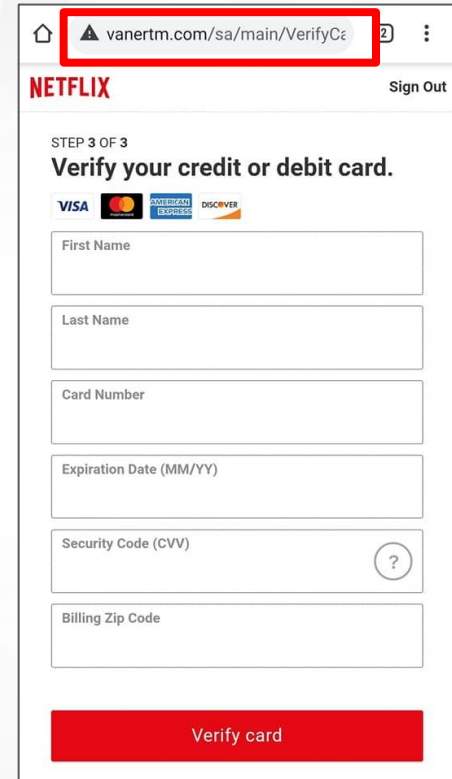
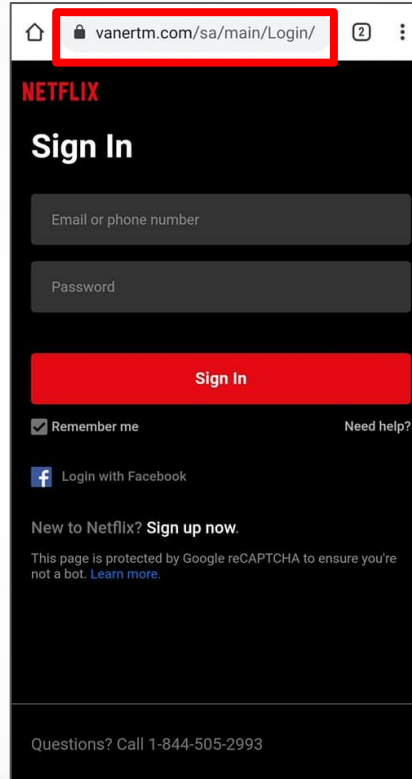
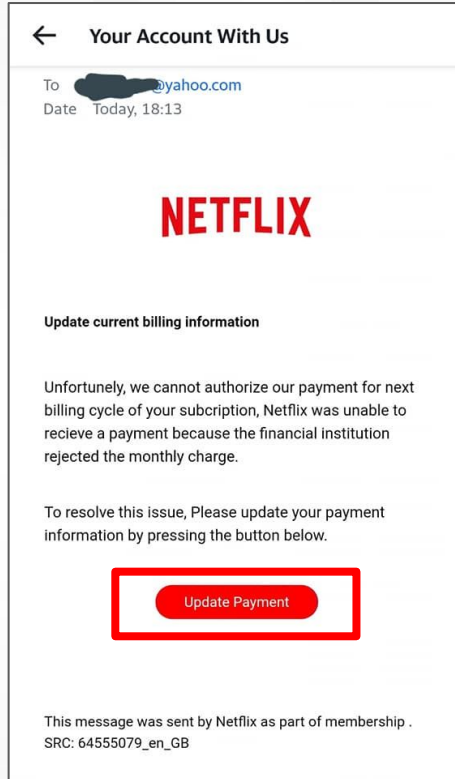
SINGAPORE

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

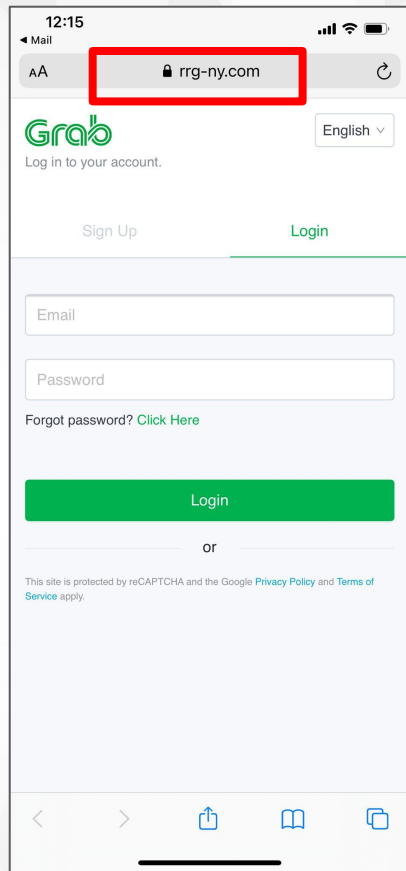
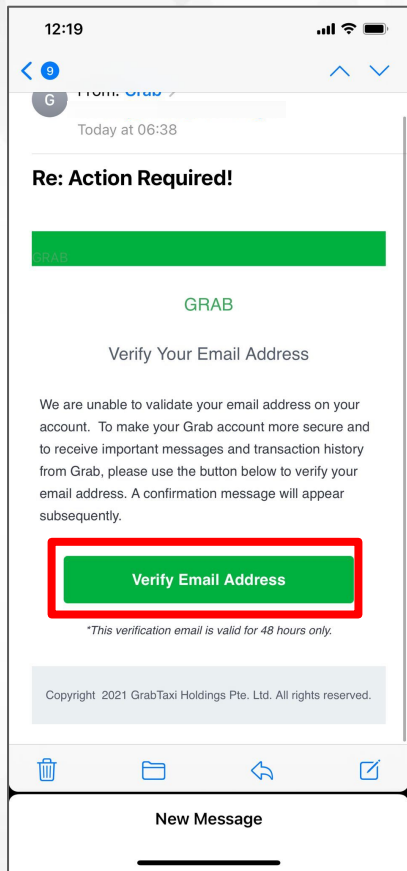


1 of 3 About 1.5 million patients, including Prime Minister Lee Hsien Loong and a few ministers, have had their personal data stolen. Some 150,000 people also had their outpatient prescriptions stolen.

Online Fraud

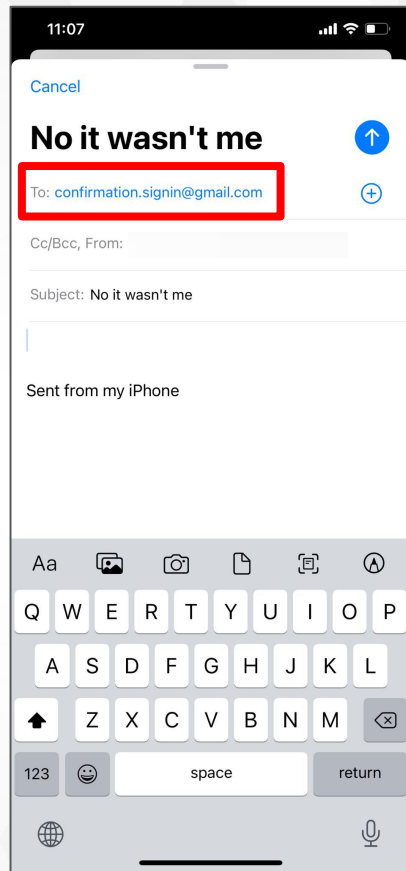
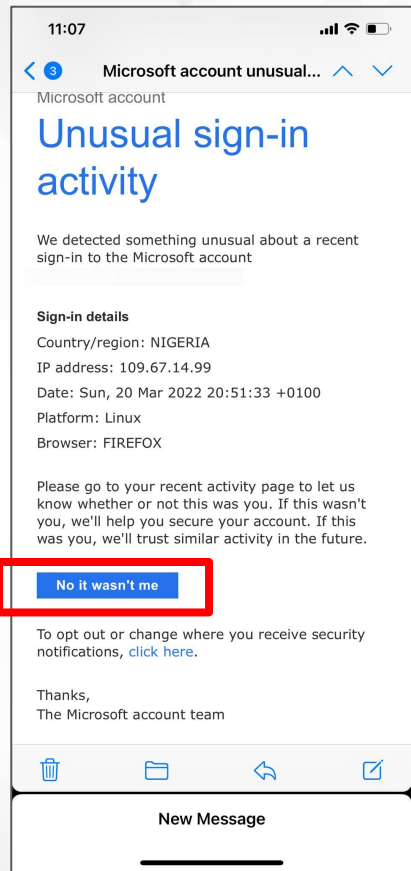


Online Fraud

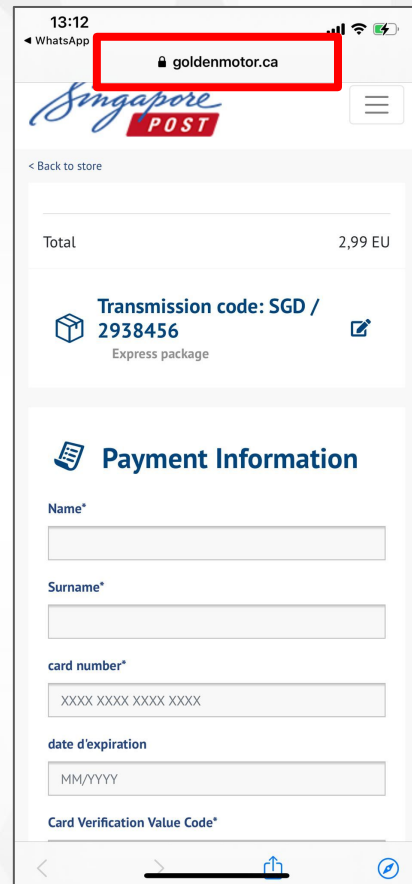
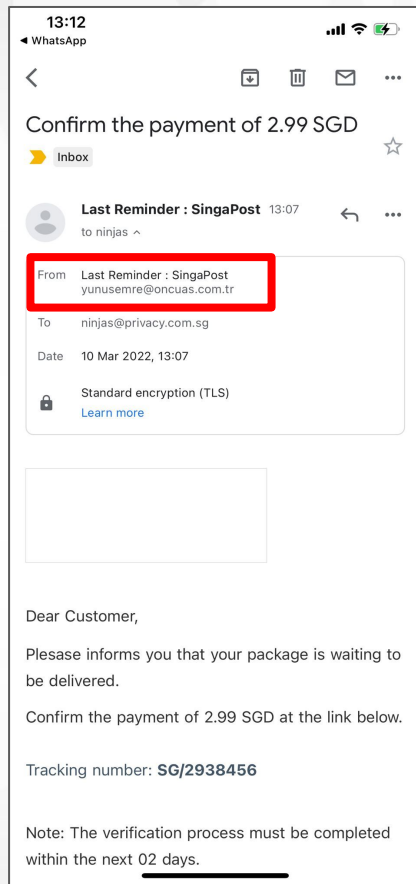


Cyber Security Today: What it Means For You

Online Fraud

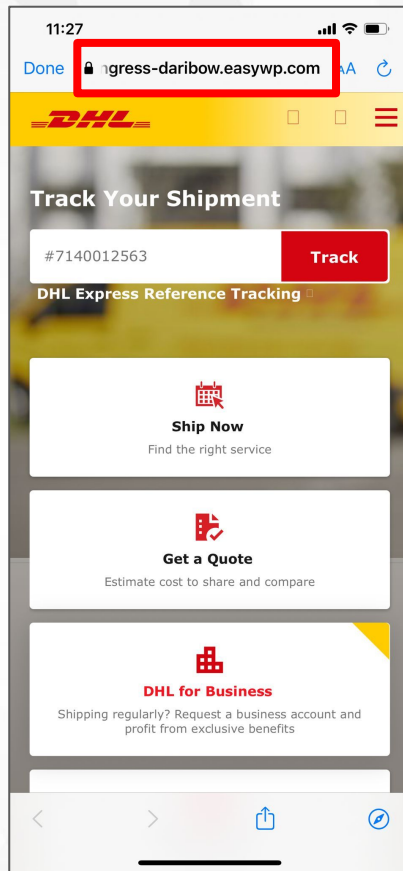
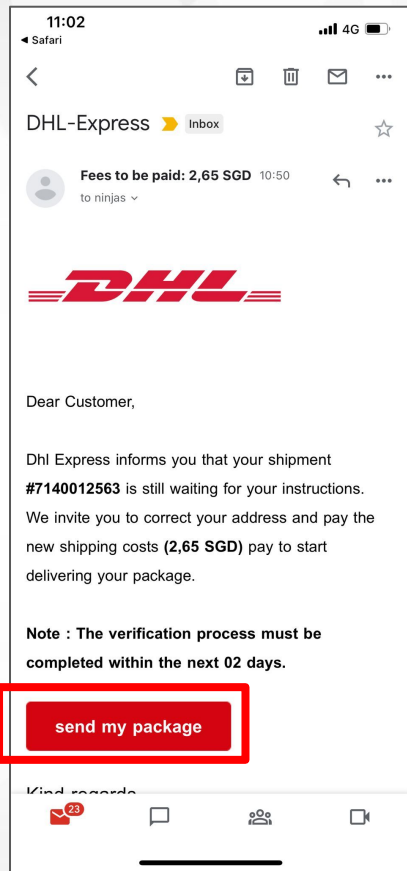


Online Fraud



Cyber Security Today: What it Means For You

Online Fraud



Cyber Security Today: What it Means For You



Recent Hacking Incidents



Singapore Home Cams Hacked And Stolen Footage Sold On Pornographic Sites

SINGAPORE (THE NEW PAPER) – Security cameras in Singapore homes have been hacked, and the footage shared online. Clips from the hacked footage were uploaded

Data of some 129,000 Singtel customers, including NRIC details, stolen in hack of third-party system



Some of the stolen information may have been put up on the dark web. PHOTO: ST FILE

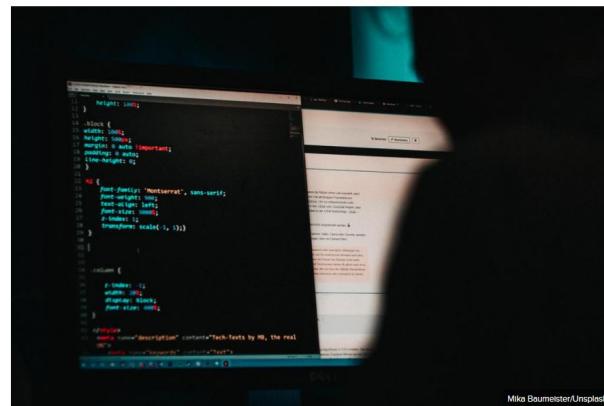
2 firms fined S\$43,000 in total over personal data breaches affecting Mindef, SAF personnel



By LOUISA TANG

Published JUNE 13, 2021

Updated JUNE 13, 2021



Mika Baumeister/Unsplash

Recent Hacking Incidents

Breach of the Protection Obligation by Audio

Breach of the Protection Obligation by Vhive

Breach of the Protection Obligation by

Breach of the Protection Obligation by Trinity

Breach of the Protection Obligation by Tanah Merah Country Club

18 Feb 2022

A financial penalty of \$4,000 was imposed on Tanah Merah Country Club for failing to put in place reasonable security to protect personal data in its possession. The incident resulted in personal data being accessed.

Cyber Hygiene

**May we have two volunteers
Please share your business email with us.**

Cyber Hygiene

Demonstration Exercise

Email spoofing from Person A
to Person B.

Cyber Hygiene

Malicious downloads can be masked as an innocent looking attachment until they are opened. To ensure that you will never fall victim to these attachment shams, always practice these 3 rules:

1

Link (Any Website Link)

- Always make it a habit to inspect a link / copy and paste in a new tab

2

Document (Excel, MS Word File or PDF)

- Double check the document if you're not expecting to receive the file

3

Image (.exe file masked as a file – E.g Virus, Trojan, Keylogger, Ransomware)

- Double check the document if you're not expecting to receive the file

Cyber Hygiene

1

Verify the authenticity of requests from companies or individuals by contacting them directly

- Paying of invoices to suppliers, claims or urgent payment

2

Be suspicious of unknown links or requests sent through email or text message

- Avoid opening Software or Files if you're not expecting it
- Turn off the option to automatically download attachments

Cyber Hygiene

3

Do not give out personal information

- Do not reveal personal or client's particulars over electronic means
- Avoid sending any form of logins online

4

Set secure passwords and don't share them with anyone

- Avoid using common words, phrases, or personal information and update regularly
- Use minimum 8 to 12 characters with complexity (Xyyyyyy123!)

Cyber Hygiene

5

Multi-Factor Authentication

- Enable Two-Factor Authentication (2FA) when available

6

Keep your operating system, browser, anti-virus and other critical software up to date

- Security updates and patches are available for free from major companies
- Schedule Full Scans as often as possible, have the “Kiasu” mentality

Cyber Hygiene

7

Pay close attention to website URLs & File Extensions

- Malicious websites use a variation in common spelling or a different domain (.com instead of .net)
- Enable viewing of full file extensions for windows machines

8

“Sound Off”, not Brush Off

- Report any improper cyber hygiene being practiced at the workplace
- Alert the IT administrator/CISO of any suspicious email, better safe than sorry

Cyber Hygiene

9

Social Media Presence

- Keep your personal information off the internet
- Change your account settings from public to private, and change privacy and security settings to prevent search engines from indexing your profile page.

10


Connecting to Unknown Networks

- Ensure the integrity of any access point you connect to
- If you have to access the internet thru public wifi, connect using a VPN

Cyber Hygiene

<https://www.brightcloud.com/tools/url-ip-lookup.php>

Look up URL or IP:

☐ I'm not a robot 
reCAPTCHA
Privacy - Terms

LOOK UP

If you have a mutually executed agreement with Webroot, those terms apply to your use of the BrightCloud Service. If you do not have a mutually executed agreement with Webroot, by clicking "LOOK UP", you agree to the terms and conditions of the BrightCloud Threat Intelligence Service for Enterprise Agreement.



ANTIHACK.ME

Web Reputation:



- Low Risk (74 of 100)

[Request a reputation change](#)

Web Category:

- Computer and Internet Security

[Request a category change](#)

Web Reputation Influences:

- No infections past 12 months
- Medium popularity
- 17 months old (established)

Impact:



Cyber Hygiene

<https://haveibeenpwned.com/>

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

pwned?

Cyber Hygiene

Password Managers

LastPass...

1Password

dashlane

Privacy Guidelines

- As long as personal data / sensitive information is to be collected, perform a Data Protection Impact Assessment (DPIA) before commencement.
- Always leverage on latest security standards and best practices to access/secure data (in-transit or storage), example encryption and authentication.
- Adhere to the retention policy and dispose personal data / sensitive information properly.
- Perform due diligence (PDPA Compliance & Cyber Security) on third parties whom you may be disclosing personal data / sensitive information to.

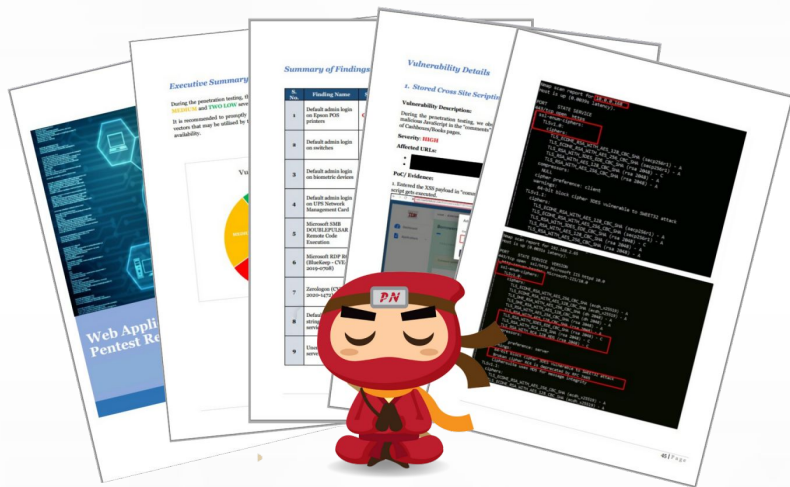


PDPA & Data Protection Officers (Requirements & Penalties)



- Appointing a DPO is mandatory for all organisations in Singapore
- Failure to do so risks a fine of up to 10% of annual gross turnover / \$1 Million
- Develop internal capabilities
 - PDPA Fundamentals
 - DPO Practitioner Certification
 - Certified Information Privacy Manager (CIPM)
- Outsourced DPO Service

PDPA & Data Protection Officers (Requirements & Penalties)



- Implement email authentication protocols to prevent Business Email Compromise (“Email Spoofing”) on your domain
- Don’t underestimate what an anti-virus software installation can detect & prevent
- Conduct periodic/annual Vulnerability Assessment & Penetration Tests (VAPT) on systems and network
- Conduct regular PDPA / Cyber Hygiene trainings for employees

Breach of the Protection Obligation by North London Collegiate School (Singapore)

18 Feb 2022

A financial penalty of \$10,000 was imposed on North London Collegiate School (Singapore) for failing to put in place reasonable security arrangements to prevent the unauthorised access of its student applicants' personal data residing in a website directory folder.

CASE STUDIES | EDUCATION INSTITUTIONS

From December 2019 to July 2021, parents of prospective students could submit documents for admission applications via the Organisation's website (<https://nlcssingapore.sg/>).

However, the website directory/folder was not adequately secured from automatic indexing by web crawlers. As a result, the submitted documents were indexed by search engines and could show up in online search results.

S/N	Type of Document (Scanned or Electronic Copies)	Number of Individuals Affected
1	Passport	1,742
2	Identity cards (i.e NRICs)	1,714
3	Digital Photographs of applicants	720
4	Birth Certificates	709
5	Academic Reports	676
6	Immunization Records	670

Follow us for your daily dose of cybersecurity news and cyber hygiene tips



PrivacyNinjaSG



ninjas@privacy.com.sg



Privacy-Ninja-Singapore



privacy.com.sg



@PrivacyNinjaSG

THANK YOU FOR HAVING US!



ANDY PRAKASH

<https://www.linkedin.com/in/andy-prakash/>

Cyber Security Today: What it Means For You

Co-hosted By:



Q&A

