From: Richard Neo
To: MCI DataRegulation (MCI)
Subject: Re: Feedback on draft PDP (Amendment) Bill

Dear Sir/Madam,

Here attached are the following:

1) Comments on the draft PDP (Amendment) Bill ;

2) Annex which contains the supporting materials.

Thank you very much.

With Regards,

[Document subtitle]

Summary of major points

1) Having a whitelist of types of crucial personal data that could result in significant harm to individuals will be helpful but the list may not be exhaustive and will need to evolve along with technology like facial recognition technology which are increasingly being used to capture important and confidential biometric data.

2) Inclusion of non-government organisations acting on behalf of government organisations in the application of the DP Provisions of the PDPA will bring fairer treatment of non-government organisations handling data from public or private sector in terms of enforcement and penalty imposition.

3) Increased financial cap may have the effect of reminding organisations handling personal data but it may not be effective if the there is any organisation situated outside Singapore in a jurisdiction which does not have equivalent or reasonable personal data protection legislations or compliance culture.

4) Statutory undertakings may need additional safeguards by including clauses stating personal liability of director or signatory who represent the organisation to engage the service of foreign organisations or companies in the provision of goods and/or services to the government or non-government organisation(s) with/without informing the government or non-government organisations.

5) The suggested improvement in control over unsolicited marketing messages sent to IM platforms is in encouraging move but companies should ensure there are options available in the IM platforms for users to select to receive or reject all or some marketing messages. Also, companies using those foreign apps for work purposes should be made aware of the privacy risks that come with their uses.

Statement of Interest

I am a member of the public who has gone through the **Practitioner Certificate in PDP Preparatory Course** and passed the examination for **The Practitioner Certificate in Personal Data Protection (Singapore).** Personal data protection is one area that I have an interest in in addition to the current data analytics course I am taking. Furthermore, I have real life experience of how my own personal data can be potentially compromised (e.g. My personal data is leaked during Singhealth hacking incident).

In addition, from the news, I have learnt about the real-life incidents where personal data is hacked, misused and even put on sale on the Dark Web. Such incidents are relevant to everyone, including me. As such, I do hope to contribute my part in enhancing the protection of personal data of many and exploring the possibility of increasing the accountability and responsibilities of service providers who handled personal data directly or indirectly especially in Government or Government-linked projects.

I think paying special attention to the presence of foreign service providers or sub-contractors who work along with the local ones is necessary as equivalent data protection and reciprocal arrangements may not exist in foreign jurisdictions. The local laws may not have arms long enough to reach these in foreign jurisdictions and hence I do wish to contribute my own ideas for your considerations.

Note: The text highlighted in orange are my comments while the parts I will be commenting on will be in black italic format. The part(s) highlighted in red are those that I wish to request to not be published.

1) With reference to the following:

18. MCI/PDPC also intends to prescribe in Regulations categories of personal data which, if compromised in a data breach, will be considered likely to result in significant harm to the individuals. This makes clear the types of data breaches that organisations will be required to notify affected individuals. Several jurisdictions have adopted a similar "whitelist" approach for data breach notification to affected individuals and/or the authorities11. Examples of data categories prescribed by other jurisdictions include social security numbers, drivers' licence numbers, state identification numbers, credit/debit card numbers, health insurance information and medical history information.

Comments: With increasing use of facial recognition technology in payment, unlocking devices and doors, the whitelist should also include biometric data like facial images and thumbprints, both of which appear on NRIC too. The facial image of a particular individual can be used to identify the real person directly, fabricate fake news, enable authorised entry for another person (intruder), effect e-payments via mobile apps for expenses incurred by someone else etc. If the collection, storage, transfer and use of biometric data are not adequately regulated, I believe more may appear in the Dark Web for sale. Identity thefts, deepfake creation and financial loss will then be increasingly common. (Please refer to Annex: Picture A & Picture B)

In addition, I noted the use of facial recognition devices in some shopping centres and other places like the Parliament. Are the contractors who supply such devices compliant with the current PDPA and willing to sign any written undertaking to take on greater accountability and possible liabilities should there be any data breach, hacking incident or data theft? Are there adequate safeguards and data protection procedures in place before the installation of such devices? If these are absent, will a major data breach incident happen that could taint Singapore's reputation as a safe location for data centres to be located in? (Please refer to Annex: Picture C)

My suggestion to enhance the accountability of such suppliers and sellers is to make it mandatory for the suppliers and sellers of those facial recognition devices to apply for and obtain license to sell those devices in Singapore so that the government can regulate the increasing use of such devices which can capture and store a lot of biometric data that could directly identify many

individuals. By using a licensing framework, the firmware and designs of such devices can be inspected for any security loophole. Nevertheless, I do acknowledge that this is not within the purview of PDPC but ensuring personal data security is a multifaceted issue and it may require the collaboration of various government departments to achieve the objective of better personal data security effectively and efficiently.

2) With reference to the following:

Removal of exclusion for organisations acting on behalf of public agencies

27. Currently, under section 4(1)(c) of the PDPA, an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data is excluded from the application of the DP Provisions of the PDPA.
28. In line with the PSDSRC recommendations, the PDPA will be amended to remove the exclusion for organisations that act on behalf of a public agency in relation to the collection, use or disclosure of personal data. This will close the legislative gap where non-Government entities acting as agents of Government are not covered under the PDPA or the Public Sector (Governance) Act 2018 ("PSGA"), and ensure the accountability of third-parties handling Government data according to the PSDSRC recommendations. It will also provide clarity and consistency in the enforcement of data breaches involving non-Government entities.
29. Please refer to clause 3(a) of the draft PDP (Amendment) Bill.

Comments: This could make third parties (main contractors and sub-contractors handling Government data more accountable without prejudice or suspected protection as compared to those handling non-Government data. Moreover, the Government data may include a larger proportion of the Singapore population than those in the private sector and hence, the accountability of the third parties involved in such a case should be aligned to the magnitude of the data volume that is at risk of being leaked and thereby affecting more people.

3) With reference to the following:

Increased financial penalty cap

58. Under section 29(2)(d) of the PDPA, PDPC may impose a financial penalty of up to S$1 million for data breaches under the PDPA. The amendments will increase the maximum financial penalty to (i) up to 10% of an organisation's annual gross turnover in Singapore; or (ii) S$1 million, whichever is higher.

59. The higher cap will serve as a stronger deterrent, and provide PDPC with more flexibility in meting out financial penalties based on the circumstances and seriousness of a breach. The higher cap will also be closer to that of other jurisdictions, such as EU and Australia. For example, the EU GDPR provides for a revenue-based maximum financial penalty (€20 million or 4% of the entity's global annual turnover of the previous financial year, whichever is higher). The higher cap is also aligned with other relevant Acts 21.

Comments: The higher financial penalty cap could likely attract more attention of many non-government organisations which handle large amount of personal data

and lack rigour in its data protection policies and procedures. Some may even think it is unimportant to protect personal data as they deem penalties under PDPA as less severe than those under other Acts like Penal Code on Illegally obtained personal information and Criminal Breach of Trust or the PDPA is not as conspicuous as other Acts since it only took effect in phases since 01 January 2013. So, raising the cap on the financial penalty under the amended PDP will have the desired effect of raising eye brows and attracting more attention from all organisations and individuals so that the importance of being compliant with PDPA will be better emphasized.

4) With reference to the following:

Statutory undertakings

64. Statutory undertakings allow a regulator to apply more flexible and individually tailored approaches to enforcement. From PDPC's experience, organisations that have in place a data protection management plan will have an effective system for monitoring, internal reporting, and management of data breaches. The implementation of the data breach management plan can be the subject of a statutory undertaking. When coupled with mandatory breach notification, statutory undertakings will further encourage organisations to adopt accountable practices.

65. Several jurisdictions, such as Australia, Canada and the UK, offer undertakings as part of their enforcement regime. Presently, PDPC accepts undertakings under its Active Enforcement Framework22. The amendments will enhance the effectiveness of undertakings as an enforcement mechanism. The statutory undertaking scheme will expand the range of options for enforcing breaches of undertakings.

66. PDPC may investigate the underlying breach if the organisation fails to comply with the statutory undertaking. Alternatively, a breach of a statutory undertaking will be enforceable by PDPC directly through the issuance of directions. If the organisation fails to comply with these directions, PDPC may apply for the directions to be registered by the District Court under section 30 of the PDPA.

Comments: The statutory undertakings may not be adequately comprehensive if there are third parties (sub-contractors), situated in foreign countries, collaborating with the local main contractors or other sub-contractors (which might not be revealed) to handle the local Government or non-Government projects that could contain personal data. The direct or indirect involvement of these foreign entities may enable them to come into contact with such confidential personal data which could further increase the risks of data breaches. It may be more difficult to make them accountable or even prosecute them since they may be situated in a different jurisdiction with no comparable data protection and reciprocal arrangement.

So, since the main contractors or the sub-contractors (especially those which are SMEs) are the ones who may engage the service of such foreign contractors or service providers, the former should be made accountable for it.

One way to do this may be to include clauses in the written undertakings to hold the signatory or director(s) who signed on behalf of the organisations (local contractors) personally liable if there is a significant data breach incident caused by the foreign contractors and it is not possible to penalise these foreign contractors due to the absence of reciprocal agreement and comparable data protection in the countries they are located in. The justification is that the signatory or the director, who acted on behalf, should exercise due diligence in knowing the foreign contractors well before engaging them and it is their duties to inform their engagement with essential details to the Government or non-Government service buyers. If they wilfully withhold any such important information or provide false information in order to obtain the contracts, which could potentially affect personal data security and make enforcement difficult to carry out, they should be held personally liable with criminal intent to cheat or deliberately withhold crucial information for personal gains. In such a case, the organisations and individuals could be penalised separately under the PDPA and the Penal Code as well.

An analogy is the Company Act which does not allow limited liability protection of a company (separate entity) to protect the personal wealth of the directors who act as signatories on behalf of the company when there is fraud and intent to cheat. So, should the PDPC hold the company responsible only when it is the signatories who represent the companies to sign the statutory undertakings? Certainly, contradiction should not happen.

5) With reference to the following:

Improved controls for unsolicited commercial messages

53. The PDPA's DNC Provisions and the SCA's Spam Control Provisions both aim to address consumer annoyance and provide consumers with greater control over the unsolicited marketing messages they receive. At the same time, they help ensure organisations communicate more effectively with consumers who are interested to receive information on offers of products and services. Technological advancements have fuelled the increased use of marketing tools such as instant messaging ("IM") platforms, making it easy to send commercial communications to a large number of recipients.

54. As the PDPA and SCA impose overlapping requirements on unsolicited marketing text messages, MCI/PDPC has reviewed both legislation to make it easier for organisations to comply with their requirements. The proposed amendments also take into account developments in the current landscape. Specifically, MCI/PDPC intend to make the following amendments:

a) SCA will cover messages sent to IM accounts: Unsolicited commercial messages sent to IM accounts via platforms such as Telegram and WeChat are currently not covered by the DNC Provisions and the Spam Control Provisions. To address this gap, the SCA will also cover commercial text messages sent to IM accounts and in bulk. Please refer to clause 38 of the draft PDP (Amendment) Bill.

[Redacted]

Comments: As an individual, I personally feel stricter regulations should be imposed on such foreign apps being used in Singapore as they may lead to scams, unsolicited marketing calls, prank calls and even malwares/viruses being installed in the smartphones without the knowledge of the installers since users need to grant access to the confidential information stored in their smart devices in order to use them.

As we move to cashless society with more frequent use of mobile apps, the more the statutory laws here should enforce the use of such apps and accountability of those companies which require their staff to use it involving their personal data. Moreover, the creators or owners of such foreign apps are situated in foreign countries like China which may not have reciprocal agreement and comparable data protection laws, which will make it harder to penalise them when there is a significant volume of data leaks and breaches caused by them. (Please refer to Annex: Picture E)

The only thing we can do to make the local companies and/or directors liable for introducing the use of such apps at the corporate and personal level correspondingly. Only then the local companies, especially the SMEs, and/or directors will be more aware of the importance of protecting personal data and being compliant with the local personal data protection laws which could be very different from those in some foreign countries where the apps come from instead of relying on their own personal interpretation of the data protection laws in those foreign countries. (Please refer to Annex: Picture F)

Conclusion

With the rapid advancement in technology, a lot of personal data becomes digitalised. They are more easily prone to hacking, data breaches, theft and misuse since network technologies, which make them easily transferable, may too inadvertently make them accessible worldwide if reasonable protection and good cyber hygiene are absent.

Contractors and sub-contractors, especially those which are SME companies, which may not attach importance to personal data protection as much as the larger ones, and some foreign organisations, should bear greater responsibility and accountability for their involvement in handling significant amount of local personal data in both local Government and non-Government projects.

So, the amendments to the PDPA are timely to deal with challenges of the digital economy. However, if a significant number of the SME companies do not take a serious view of the PDPA or hold the view that PDPA is not applicable to them due to their inconspicuously small size, then PDPA and PDPC may be perceived as two toothless tigers. Must we wait till more data breach incidents significantly affect the reputation of Singapore as a secured data centre (which is worth a lot more than the S$1 million penalty imposed for data breaches) permanently before any further decisive actions can be taken?

If Singapore wants to distinguish itself as a safe data centre from other competing countries, it will need to move forward in this race with the necessary legislations to give the investors better assurance and peace of mind. This can help strengthen and sustain a long-term confidence in Singapore as a reliable and relevant economy.

Annex

Picture A:

Sunday, May 5, 2019 | The Sunday Times

Top of the News | A7

Your medical records, bank account details, e-mail passwords and Netflix login can be bought for

$1,000 on the Dark Web

Calvin Yang

On the data black market, thieves peddle stolen medical records, bank account details, e-mail passwords and even Netflix logins.

Priceless to you, perhaps. But on the Dark Web, an online space that can be accessed using only special software, they can be traded for less than $1,000.

Prices can fluctuate drastically based on the type of data and demand for them. But in general, those belonging to prominent figures, such as politicians and celebrities, will fetch a higher price.

Still, cyber-security experts and hackers say every datum has a price tag. And no quantum can be put on the loss of privacy and, potentially, identity.

The Sunday Times explores this secretive cove where, all too often, leaked data ends up for sale after a breach.

STOLEN MEDICAL DATA

Data from Singapore has been traded on the cyber black market.

Between 2017 and last year, user logins and passwords from Singapore government agencies and educational institutions were put up for sale on the Dark Web.

The organisations included the Government Technology Agency (GovTech), the health and education ministries, and the police.

The Smart Nation and Digital Government Group said GovTech was alerted to the presence of e-mail credentials in illegal data banks in January this year.

It added that the credentials were not leaked from government systems, but from officers who used them for personal and non-official purposes.

"Around 50,000 of them are government e-mail addresses.

"They are either outdated or bogus addresses, except for 119 of them which are still being used," the group said in March, adding that as an immediate precautionary measure, all officers with affected credentials have changed their passwords.

In recent years, stolen medical records have become a hot commodity. Observers say healthcare organisations hold the personal and financial details of patients, which can be more valuable to illegal peddlers than those on a stolen credit card.

After Singapore suffered its worst cyber attack in June last year, there were worries that the data would be put up for sale.

Hackers had entered the database of public healthcare cluster SingHealth to steal the personal data of 1.5 million patients and the outpatient prescription information of 160,000 people, including Prime Minister Lee Hsien Loong.

This was followed by two more high-profile incidents.

In January, the confidential details of 14,200 HIV patients were stolen and leaked online.

Another breach, revealed in March, involved the personal information of more than 800,000 blood donors which was exposed online for more than two months, accessed illegally and possibly stolen.

Though there has been nothing to suggest the stolen data has been put up for sale, concerns remain.

Medical records comprise doctors' reports, lab results, drug prescriptions and family history, among other confidential health information.

These records also reveal a person's full name, identity card number, date of birth, address and contact details.

Mr Azly J. Nor, who runs tech consultancy Blackwilder, believes the data in health records is the most accurate available to build a person's entire identity.

"Medical data consists of your personal identification, which you can't change, and which will last for your lifetime," he said. "You can even access the family's medical history from the patient's record, insurance information, ethnicity as well as medical prescriptions."

Potentially, such medical records can be stripped apart, repackaged in different ways and sold.

Mr Halim Santoso, Asia sales engineering director of American software company Symantec, said: "A person can use my details to apply for a $50,000, $100,000 car loan. This is the monetary impact."

Observers say leaked health data may also be of interest to insurance representatives who want to push new products to the market.

A computer forensics expert working at technology-based risk consultancy TRS Forensics. Experts urge Internet users to practise good cyber-hygiene habits, such as updating their software regularly for security patches, using different passwords for various accounts, and avoiding suspicious links or e-mail attachments from unknown senders. ST PHOTO: DESMOND WEE

Insurance firms contacted did not comment on whether their agents have purchased such data.

Unlike medical records, credit card details are time-sensitive. The cards can be deactivated, the accompanying data may expire and fraudulent charges can be disputed.

"Credit cards have a limit, and financial companies have a lot of mitigating controls, like requiring you to use a PIN and a one-time password," said Mr Santoso.

"They also have back-end controls to identify risky or suspicious transactions, and once they identify a transaction as suspicious, they can lock the card."

OTHER DATA OUT THERE

In future, data may well be "the most valuable currency", said Mr Allen Yeo, manager of cyber-security services at Wizlynx Group.

At the budget end are e-mail passwords, which are aplenty on the Dark Web and sometimes sold for less than $1.50 each.

Frequent flier miles, which can be redeemed for free travel and upgrades to business and first-class seats, are also sold. You can get about 900 miles (1,450km) for $10.

Netflix login details are available for about $8 apiece.

Even social media accounts have price tags, from $2 for an Instagram account to $7 for a Facebook login. Accounts with more followers can command higher prices.

At the other end of the market is data that is hard to obtain. Fresh bank account passwords cost at least $100, but the higher the account's balance, the more expensive the asking price.

Medical records can command up to a few hundred dollars each, depending on how complete they are.

Mr Tan Kah Leong, a director at technology-based risk consultancy TRS Forensics, likens the trade to the stock market, where prices fluctuate according to the forces of supply and demand.

THE SELLERS

Malicious insiders are common sources of data leaks.

Experts say that besides disgruntled employees, rogue insiders can include third-party vendors who handle projects outsourced by firms.

There is little stopping these service providers – some situated in countries with cheaper labour – from making copies of the data and putting them up for sale.

Mr Bhone Htet Kyaw, cyber-intelligence analyst at cyber-exposure specialist Cyber Intelligence House, said external hackers, too, can "access databases and servers that are not updated and patched for the latest weaknesses".

Information can also be accidentally exposed by the organisations themselves: For example, by an employee who has misplaced his laptop that holds sensitive data.

Even firms that discard physical documents without first shredding them can be at risk.

Some peddlers may sell stolen data to aggregators, who reassemble the information into fuller profiles. This boosts the value of the data, which may have been collected from several breaches.

One data dealer, who sells credit card accounts, said the price increases as the information on an individual becomes more complete.

For an additional $50, he provides the credit card holders' "fullz" profiles, which are bundles of information such as addresses, phone numbers and other sensitive data.

Dark Web market vendors do not care who the buyers are or what they do with the data, said Mr Htet Kyaw. "They will sell their data to anyone who is willing to buy."

THE BUYERS

Cyber-security experts narrow it down to two types of buyers: shady political players and financially motivated syndicates.

Mr Lavi Lazarovitz, security research team lead at security software firm CyberArk, said confidential data in the hands of a rival state might put government officials and other stakeholders at risk, or at least cause embarrassment.

He said well-funded organisations that have a political agenda may seek such data, which offers "valuable information for reconnaissance and enhances the effectiveness of social engineering attacks".

"(Such) data is pure gold for intelligence agencies. Singapore is known to have rivals – political and financial – and, so, intelligence agencies can use this data to support their interests," he said.

Elsewhere, there are financially motivated cyber criminals who rely on the data to engage in illicit transactions or commit identity fraud.

Mr Yeo Siang Tiong, general manager for South-east Asia at cyber-security firm Kaspersky Lab, said: "Someone who is willing to pay can actually have someone else's credentials for social media logins, banking details and even remote access to servers and desktops."

To prevent this, experts urge internet users to practise good cyber hygiene habits, such as updating their software regularly for security updates, using different passwords for various accounts, and avoiding suspicious links or e-mail attachments from unknown senders.

But there is not much users can do when their data is managed by others.

Mr Azly said: "A user can do only so much to protect himself, but the responsibility ultimately lies with the platform handling their data. If entities like SingHealth can't even secure their data, what more can the user do?"

callyang@sph.com.sg

READ MORE $3,800 for forged Spore passport online A8

When 'dark' is not all evil

Tan Ee Lyn

The Dark Web is not all about drugs, porn, stolen identities and data. It also plays host to an enormous amount of legal content from research papers to some major newspapers and even social media sites such as Facebook.

People use these parallel sites on the Dark Web primarily because their governments have blocked access to them or because they want to stay anonymous and conceal their physical location and usage from surveillance or traffic analysis.

By using the Dark Web and browsers like Tor, users such as whistle-blowers, activists and journalists are able to communicate and exchange information anonymously without compromising their identities and locations.

Tor was originally developed by the US Navy to protect government communications. The aim was to protect the personal privacy of network users, and allow them to conduct confidential business. Tor is now widely used to access the Dark Web.

"Just because the name is 'dark' doesn't mean it's all evil," said a Dark Web user, who asked not to be identified. "What it means is that there is a parallel Web of resources that are not searchable and reachable by the usual ways that people employ."

WikiLeaks, for example, has a parallel website on the Dark Web, which allows users to browse and whistle-blowers to upload documents.

Associate Professor Chang Ee Chien of the School of Computing at National University of Singapore (NUS) said: "If a person wants to upload to WikiLeaks, say, from Russia, Syria, he can upload through the Tor network. It protects the identity of the user."

"The Dark Web... protects the identity of the Web server."

Sites hosted on the Dark Web also offer anonymous e-mail services which journalists, activists and their sources can use to communicate.

Journalists are also increasingly using it as a source of content for their work.

"Tor provides senders' anonymity, so the journalist can hide his identity," said Assistant Professor Kang Min-suk of the School of Computing at NUS.

In places where access to major newspapers and social media sites like Facebook has been blocked, the Dark Web is simply a place for people to read and connect.

In 2017, The New York Times made itself available on the Dark Web for readers who were blocked from accessing it via the regular channels or because they care about online privacy and worry about local network monitoring.

Prof Kang raised the possibility of activists using the Dark Web to disguise and protect their Web servers. "If, for whatever reason, they are in conflict with their government and they want to hide the location of their server, they can do that," he said.

"So, in using the Dark Web, they can reveal their identity."

But Prof Chang warned that nothing is foolproof, and the authorities with resources will be able to track down the users.

tanel@sph.com.sg

Tor was developed by the US Navy to protect government communications. It is now widely used to access the Dark Web. ST PHOTO: LIM YAOHUI

Picture B: https://www.channelnewsasia.com/news/commentary/faceapp-sharing-photos-facebook-social-media-deepfake-data-scam-11824208

By Frederic Ho

★Commentary | Commentary

Commentary: Careful with photos you post online. You may be putting your digital identity at risk

22 Aug 2019 06:29AM
(Updated: 22 Aug 2019 06:30AM)

Bookmark

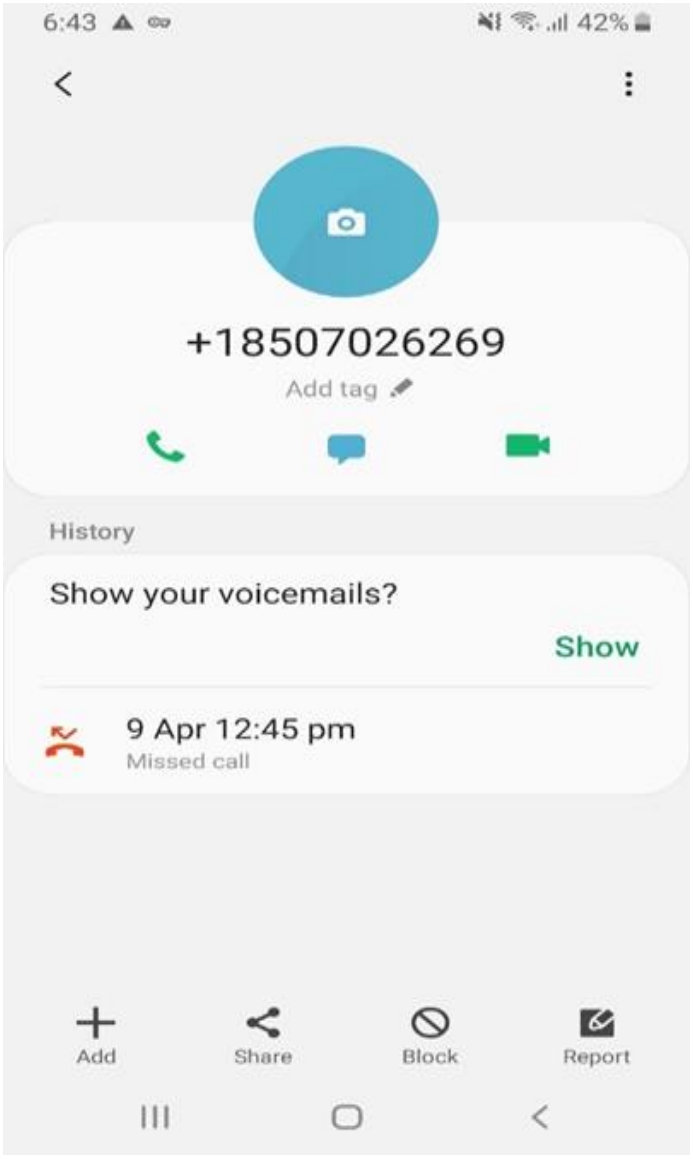
Bad actors may use photos manipulated using deepfake technologies to log into user accounts, says Jumio's Frederic Ho.

FaceApp's old-age feature is the latest social media craze. (Photo: FaceApp)

SINGAPORE: From the popular boy band The Jonas Brothers to celebrity chef Gordon Ramsay, users of FaceApp around the world have been having a blast sharing their AI-altered photos on the Internet.

Picture C: Source: https://www.straitstimes.com/world/europe/concerns-raised-over-leak-of-biometric-data-in-uk

Picture D: Screenshot of odd phone number


6:43
42%
+18507026269
Add tag
History
Show your voicemails?
Show
9 Apr 12:45 pm
Missed call
Add
Share
Block
Report

Picture E:

Man in row with bank over hacked phone

Danson Cheong and Lester Hio

Mr Philip Loh had his phone hacked into and credit card details stolen last year, with six flight tickets costing $12,327 being bought in Eastern Europe. He appears to be the victim of a malicious program that the public was warned about last month. ST PHOTO: ALICIA CHAN

"System update in progress. Please wait," read the prompt on Mr Philip Loh's Samsung Galaxy Note 4 smartphone last September. Thinking nothing of it, he went to bed.

Meanwhile, hackers got hold of his credit card details. Six flight tickets were purchased in Eastern Europe – from countries including Russia, Estonia and Latvia. The total price was $12,327.

Now the 47-year-old first aid trainer is entangled in a dispute with United Overseas Bank (UOB) as he tries to get the charges waived.

The bank, which insists its security system was never compromised, is asking him to pay $5,000 of the $12,327, having reduced the amount out of goodwill, or it would take legal action, said Mr Loh.

"How can I pay for something I didn't purchase? I've never even visited those countries before," he told The Straits Times.

When he woke up on Sept 30 last year, his phone was still "updating". He forcibly rebooted it by removing the battery, only to find SMS alerts from UOB on the purchases, as well as the one-time passwords (OTPs) used to authenticate them.

Shocked, he cancelled his credit card before going to the police and Consumers Association of Singapore (Case) for help.

Mr Loh appears to be one of the victims of a malicious program that the Association of Banks in Singapore (ABS) warned the public about last month. He insists he has entered his credit card details on his phone only twice or thrice in the past year – to buy movie tickets online.

He was told by the bank that one of the reasons the payments could not be waived was that they were made under the "3D secure payment system" – which authenticates online transactions by sending an OTP to the customer's cellphone. The Straits Times understands that because the hackers obtained the OTPs, the payment system was not compromised.

UOB said: "We review each customer dispute case thoroughly and take into account a number of contributing or mitigating factors. These include whether a customer had provided his credit card information on a phishing site or if transactions were authorised with an SMS OTP. In this present case, the bank's security measures were not compromised."

An ABS spokesman said that in some reported cases, consumers provided their credit card information on websites without checking if they were legitimate. "These allowed hackers to 'take control' of their smartphones to perform fraudulent online transactions."

Case executive director Seah Seng Choon said banks need to keep in mind shifting security vulnerabilities. "If a third party can hack into the system and perform transactions in this manner, it shows that the system needs to be reviewed to protect consumer interests."

Information technology lawyers said crooks are starting to get the better of two-factor authentication systems. "The question is: Is it fair for consumers to bear the liability when it is the system that has been compromised by hackers?" said lawyer Bryan Tan.

dansonc@sph.com.sg
lesterh@sph.com.sg

Who's liable for the loss incurred?

Who absorbs the loss when online credit card fraud takes place – the customer, the merchant or the bank?

Complicating this question is the 3D Secure payment system, which was set up in 2001 by Visa and adopted by other credit card firms and banks.

In the system, when customers make online payments, they must key in a one-time password (OTP) sent to their cellphones by the bank.

Before this was implemented, if a fraudulent transaction was made online, the merchant paid the price as the bank did not then have to pay the merchant.

But responsibility has shifted to the banks now with merchants signing up for 3D Secure, as the banks must authorise the payment request and pay the merchant based on such authentication.

Liability could also fall on the customer, especially if his card details were given away deliberately or negligently.

But, with cellphones increasingly targeted by hackers, 3D Secure may not be as safe as before: hackers can break into the customer's phone and steal the OTP as well as other sensitive data such as passwords.

This means the customer can reject responsibility, too.

The OTP can be sent to a more secure hardware token, but most banks opt for SMS OTPs for convenience.

"Currently, the banks decide the method of OTP delivery from the many options available," said Visa's country manager for Singapore and Brunei, Ms Ooi Huey Tyng.

Some experts, such as Mr Thomas Zink, research manager at market research firm IDC, said consumers should not be liable for fraudulent transactions if they were not acting "fraudulently or without reasonable care".

Most of the time, users will have to trigger or approve the installation of malware.

But IT lawyer Bryan Tan said it can be hard for the layman to detect these insidious programs, and they are almost always downloaded unintentionally.

"If you are a designer of malware, you are not going to put big flashing lights and say this is malware. You are going to make it as insidious as possible," Mr Tan pointed out.

Experts say that consumers should be extra vigilant about the content they access on their mobile phone.

To better protect themselves against mobile malware, they should also be mindful when opening e-mail links.

Lester Hio
Danson Cheong

Picture F:

Report flags lack of cyber preparedness among SMEs in Singapore

The Straits Times 17 Oct 2019

Over half of cyber incidents at SMEs in past year were caused by known risks: Survey

Seow Bei Yi
Business Correspondent

Nearly two-thirds of the Singapore SMEs surveyed reported experiencing a cyber incident in the last year, even though nearly half said their organisation assumes it will never experience one.

More than half the number of cyber incidents that small and medium-sized enterprises (SMEs) here experienced in the past year or so were caused by a risk leaders had already identified, found a survey by Chubb Insurance.

Such incidents included data loss through system malfunctions and getting hit by ransomware.

Flagging a clear gap between perceived and actual preparedness, the second annual Chubb SME Cyber Preparedness Report released yesterday also showed that 53 per cent of the cyber incidents in the past 12 months or so were caused by employees.

This was either through administrative or clerical errors, or the loss or theft of a company device, such as a laptop or USB drive.

The Singapore figures were based on a survey of 300 respondents from SMEs here.

This was part of a larger survey involving 1,400 respondents, with the rest from Hong Kong, Australia and Malaysia.

Nearly two-thirds of the Singapore SMEs surveyed reported experiencing a cyber incident in the last year, even though nearly half said their organisation assumes it will never experience one.

In Singapore, 30 per cent of the data files breached involved e-mail traffic of the senior team.

Research and development data made up 24 per cent, while intellectual property data and financial performance data accounted for 23 per cent each.

"While Singapore performed slightly better than other markets in protecting customer records, collectively this data was still accessed in 40 per cent of all breaches," said the report.

"In 12 per cent of incidents, the SME wasn't even aware of what data was breached."

Mr Andrew Taylor, cyber underwriting manager for Chubb Asia-Pacific, said: "With more businesses going digital in Singapore, it's unsurprising that cyber incidents are on the rise. SMEs need to keep pace and educate themselves about all the cyber threats they face."

The survey also found that despite a rise in the number of cyber incidents, Singapore SMEs are "less worried about the impact on their business".

Compared with last year's survey, fewer firms were worried about the impact of a cyber incident on their relationship with customers, revenue and sales, reputation, or the cost of the incident.

While 60 per cent of SME leaders overall believed that insurance has a role to play in protecting them against cyber risk, only 34 per cent of SMEs are currently insured against cyber incidents.

Similar to last year's findings, 59 per cent of SME leaders believed that large corporations are at greater risk of cyber attacks.

Over half of the SMEs surveyed were not confident that staff with access to sensitive data are fully aware of their data privacy responsibilities, although a larger proportion of leaders are identifying better training in cyber-risk management as an important next step.

byseow@sph.com.sg