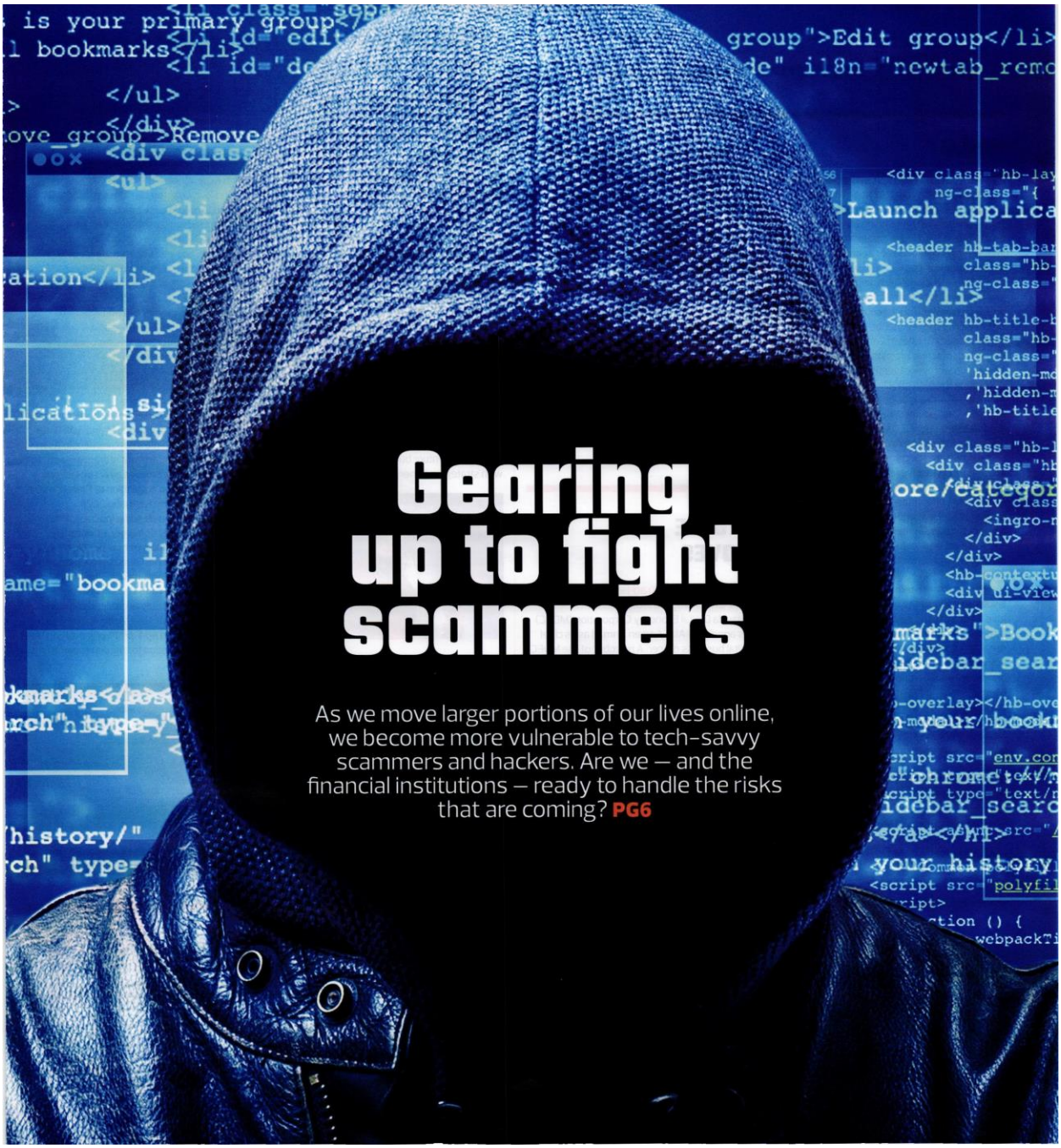


Gearing up to fight scammers

As we move larger portions of our lives online, we become more vulnerable to tech-savvy scammers and hackers. Are we — and the financial institutions — ready to handle the risks that are coming? **PG6**

COVER STORY

Gearing up to fight SCAMMERS

BY **TAN ZHAI YUN**

It is getting easier to transfer money and create investment accounts entirely online. This process is only going to become more convenient as digital banks and more fintech innovations come into play.

As a larger portion of our lives moves online, however, we also become more vulnerable to attacks by scammers and hackers. These criminals are employing increasingly advanced technologies, alongside their usual tactics of social engineering, to trick consumers.

This was evident last year when most people were working from home because of the pandemic and conducting online financial transactions.

According to the Malaysia Computer Emergency Response Team (MyCERT), reported cybersecurity incidents spiked last April during the Movement Control Order period. The number of financial scams recorded by the Ombudsman for Financial Services (OFS) also increased significantly last year, according to reports. Similar trends were reported globally.

The question is, are financial institutions evolving in tandem to protect consumers from these incoming threats, and is consumer awareness high enough to ward off these attacks?

"Technology has changed our lives significantly. But, as it evolves, we usually overlook the risk that comes with it. For instance, many people don't use a very secure password for their bank accounts. We are not catching up in terms of risk management," says Fong Choong Fook, director of penetration testing firm LE Global Services Sdn Bhd (LGMS), which conducts cybersecurity testing, computer crime investigation and digital forensics.

"What's worse is that technology is moving so quickly that we cannot even keep up and understand the risks that are coming. For instance, when 5G comes, everything will be connected to the internet, including our cars and appliances. We are going to be exposed to more risks then."

Even Internet of Things (IoT) service providers will have to focus on cybersecurity. This will become more important as 5G is launched in Malaysia, Fong says. The global mobile operators' association GSMA has released the IoT Security Guidelines and IoT Security Assessment for this purpose.

"We have seen too many companies get hacked, especially in the last 12 months. Many large organisations got hit with ransomware, not because they are not aware about security but because they didn't think that hackers would be interested in them," says Fong.

Hackers no longer pick their targets, though. "They don't hack manually anymore. They use automated tools and software to find loopholes and vulnerabilities in IP addresses, which could belong to anyone," he says.

Hackers are also developing increasingly sophisticated malware. LGMS regularly decodes such malware to apply the lessons in the company's test cases. "The bad guys are getting very organised. When you look at the malware, you realise it cannot be the work of just a few individuals. It's a collaborative effort."

That is not to say that financial institutions have not put in place sophisticated cybersecurity measures. Banks, insurers, e-money issuers and designated payment operators have to follow Bank Negara Malaysia's Risk Management in Technology (RMiT) guidelines, while capital market entities have to follow the Securities Commission Malaysia's guidelines for management of cyber risk.

As banks introduce more new digital products that emphasise convenience and speed, they will also have to invest more in cybersecurity.

Some things could be done better, say the interviewees. But one thing they emphasise is that technology always needs to be paired with education. Many scam attacks are successful because consumers are not careful.

"When it comes to cyber-protection, it's always defence in layers. You can have a very sophisticated fraud detection system, but if your customers and internal operators are not fully trained or well versed in protecting themselves, the best tools won't be able to help you," says Anthony Tai, executive director at Deloitte Risk Advisory Sdn Bhd.

The wealth of personal information available online has also increased consumer vulnerability.

"Scams are always carried out using the same modus operandi. It's the way they gain your information and your trust that changes. It's very scary now because scammers know everything about you, since it's easier to find information about you online," says Tai.

SCAMMERS VERSUS THE PEOPLE

A common method that scammers use nowadays is phishing, where they trick the victim to press a link that installs malware into the victim's devices. Scammers could also trick victims into sharing sensitive information, such as their credit card CVC number, via phone calls while pretending to be someone else.

There are also cases in which victims are tricked into entering their account number and passwords into fake websites or apps that look like the real ones.

"People can buy malware off the dark web and run it. Creating a website is also very easy," says Tai. But there are some things that scammers still cannot achieve. "In fake websites, you will see that the spelling of the URL is off or the certificate is not valid."

The Transaction Authorisation Code (TAC) scam remains a popular scheme. The scammer will initiate a transaction using the victim's bank account and then call the victim, claiming to have accidentally registered the wrong phone number.

"The scammer will tell the victim a sob story, like 'I'm sorry my TAC was sent to your phone by mistake, but I need to send money immediately because my father has been hospitalised.' The victim may give the TAC number, which allows the scammer to transfer money out of the victim's account," says Tai.

In itself, the TAC scam is not due to weaknesses in cybersecurity measures but the victim's behaviour. Even the way in which the scammer gets hold of the victim's bank account and password in the first place could be because of that.

"The most common method through which the victim's information is compromised is the victim probably used a public WiFi connection somewhere to do online banking. When financial transactions are conducted on an unsecured WiFi, the hackers can capture all the information, including your user ID and password. Once they know your phone number, they can launch their attack," says Tai.

> *"It's very scary now because scammers know everything about you, since it's easier to find information about you online."*
> Tai

> *"Technology is moving so quickly that we cannot even keep up and understand the risks that are coming."*
> Fong

SECURITY TIPS FOR CONSUMERS

- Use strong passwords that comprise letters and symbols
- Use multi-factor authentication
- Avoid use of unsecured public WiFi
- Do not download pirated software or plug-ins
- When you receive a phone call or message asking for sensitive information, verify the source
- Scrutinise the URL. HTTPS is more secure than HTTP.
- Check the security of the site by clicking the padlock icon in the address bar
- Hover over a link to check its destination before clicking it
- Check for warnings from banks' websites regularly

The device used to connect to public WiFi will remember those credentials. Even after the person has left the premises, the device will continue to seek for those credentials whenever the WiFi function is on, says Fong.

"For instance, if your phone was previously connected to KLIA's free WiFI, it will continue broadcasting later on to see whether KLIA's free WiFi is around. There is actually a box that can answer the phone and say it is the KLIA free WiFi, even though it isn't, and connect with the phone," says Fong.

Through the box, the hacker can intercept anything the person uploads or downloads via the WiFi connection. What is worse, says Fong, is that hackers can apply the rogue access point attack technique, where they use the box to pretend to be the victim's home WiFi connection and trick the victim's devices to connect to the box.

Meanwhile, phishing attacks remain a threat. The victim might unknowingly download malware when they click a link in an email or message.

"If they hack you using malware by deploying a key logger, they will capture whatever you are entering via your keyboard, which could be your user ID and passwords. It could also be ransomware, where the scammers encrypt your computer [and demand payment]," says Ubaid Quadiri, executive director of emerging technology risk and cyber at KPMG Malaysia.

Is it possible for hackers to control a victim's device through a phishing attempt? To do so, the hacker needs to make the victim download a spyware into the device.

"By clicking the link, you will not be infected. But if the link prompts you to install something and you click 'OK', then they can use your phone to make calls, look at your messages and even contact people using your number," says Fong.

"This is particularly dangerous when people use their phones to watch dramas [on illegal sites]. Usually, the browser will prompt you to install something. Some of these plug-ins contain malware."

FINANCIAL INSTITUTIONS VERSUS SCAMMERS

An irony that technological advancement has brought to light is that, while online banking has allowed people to transfer funds faster than before, it allows scammers to do so as well.

In a previous interview with *The Edge*, OFS said it was extremely unlikely that the victim could recover stolen funds once it had been transferred out by a scammer into cash.

That might seem contradictory: Has technology not developed quickly enough to prevent this from happening? For instance, could an artificial intelligence (AI) system be installed so banks can monitor for abnormal transactions? That way, the bank can immediately freeze abnormal transactions and inform the customer.

"That's possible. It's just that putting in these controls costs money. Some banks do put in fraud detection solutions like this for corporate customers. The system can raise a red flag on abnormal transactions," says Fong.

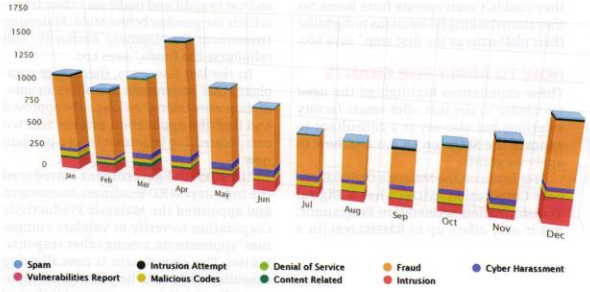
It could also be cumbersome, given the high number of transactions that go through the system and risk of generating false positives.

An initiative that could make this more commonplace is having an industry-wide fraud detection system, which is a project that Payments Network Malaysia Sdn Bhd (PayNet) is interested in exploring, says Tai. The large amount of data coming through the system will enable better detection of trends and cybercriminals.

The challenge, Tai says, is convincing banks to get on board, since it is not going to be cheap or easy to implement, and clear data governance is needed.

He explains: "Cooperation between financial institutions is key if you want to be effective in combating fraud and cybercrime. They have to be very open and transparent about what is happening in their organisations and the trends they are seeing. I hope PayNet can be the catalyst to drive this industry-wide dialogue or, at least, to get the banks to decide on a framework on what sort of information can be shared."

Reported incidents based on General Incident Classification Statistics 2020



MYCERT

> *"A bank's website [has] multiple layers of protection such as firewalls, intrusion prevention system and data leakage prevention."*
> *Ubaid*

This is already done by SWIFT, also known as international wires, which introduced a new protocol called SWIFT gpi in 2018. It enables banks to send a stop-and-recall request once they detect a suspicious transaction, so the payment is not processed further.

The good news is that many local financial institutions have invested in and plan to invest in more technological solutions to prevent fraud — from onboarding to the transaction monitoring stages — according to a report by global fraud specialist GBG.

"The moment you go into a bank's website, there are multiple layers of protection such as firewalls, intrusion prevention system and data leakage prevention. On top of that, banks have fraud monitoring or security operations centres to monitor for security events," says Ubaid.

For instance, multi-factor authentication through TAC and mobile secure verification are steps that financial institutions have deployed to protect consumers.

As long as financial institutions comply with the RMiT, their cybersecurity should be sufficient, says Ubaid. They will, however, have to stay agile and update their measures as new products are introduced.

"One of the things that banks don't have here is threat intelligence. In 2019, Bank Negara did mention it was establishing a Financial Threat Intelligence Platform to monitor threats on the web," says Ubaid.

Overall, Fong believes good guidelines are specific and have to be updated frequently. This is something that Malaysia could strive towards. "Singapore has one of the best benchmarks and frameworks on cybersecurity for its financial institutions," he says.

DATA, BIOMETRICS AND THE CLOUD

An entirely online onboarding process often requires the submission of personal information, such as photos of one's identification card, to the financial institution or fintech platform online for the e-Know Your Customer process.

It can be a matter of concern, therefore, when one wonders how securely this data is stored. This worry is exacerbated by news about data leaks, whether done by internal actors or hackers.

The leaked personal data can be used by hackers to profile victims, says Fong. "There is no strong enforcement of the Personal Data Protection Act (PDPA), which is itself incomplete compared with privacy laws in countries like Singapore. Many people don't know what they can or can't do with other people's data."

So far, cases of data breach by staff who leak customer data are not common in financial institutions, the interviewees say. There are controls put in place under the guidelines that determine data governance. Tai says the penalties imposed by the PDPA are also significant.

As a consumer, the best thing one can do is to read the terms and conditions before signing up for new services.

"Find out what they can do with your data. Don't reveal too much about yourself. For instance, when you open an e-commerce account, why do they need to know your education level and household income?" says Fong.

Many online banking apps and fintech platforms also use biometric authentication for login purposes. Fingerprint authentication is quite secure, Fong observes, while there are still some loopholes with facial recognition systems.

"We managed to hack one of the facial recognition tools on the Apple phone by using a fake 3D-printed face. There have also been cases where siblings can pass for each other using this tool," says Fong.

On the other hand, many financial institutions and fintech platforms now rely on cloud services. Cloud security controls is a potential vulnerability that scammers could take control of, says Ubaid. Scammers could also exploit the third parties that manage the cloud.

"We recommend that organisations review their cloud security controls in line with the security benchmarks and regulatory compliance guidelines, such as the TRM guideline issued by Bank Negara and Cloud Security Alliance requirements," says Ubaid.

"Ensure cloud monitoring is integrated with broader security and fraud monitoring within the organisation. Also, perform periodic vulnerability assessments and threat detection." E