ONLINE DANGERS during pandemic

Cybersecurity is also finding its new normal, with the public now facing remote working risks, Covid-19 related scams, misinformation, targeted ransomware and more.

By QISHIN TARIQ
lifestyletech@thestar.com.my

WHILE the public has had their hands full trying to survive the Covid-19 pandemic, both literally and financially, another infection has been brewing online.

Fortinet Asia Pacific security strategist Jonas Walker warned that the global pandemic and resulting lockdown measures that drove people online more was leading to a wave of cybercrime.

"One of the most lethal combinations is a sophisticated attack that targets humans when they are in a state of fear, uncertainty, and doubt. Ironically, we now live in a world where human viruses and cyber viruses cross attack paths," he said in an email interview.

Walker warned that attackers were poised to take advantage of the growing pool of potential victims as workplaces, schools and shops closed and more people stayed at home, connected to the Internet, during the movement control order.

"They have anticipated the generic behaviour of individuals and prepared campaigns for the events around us by filling the Internet, and our email inboxes, with disinformation, malicious files, and links to infected web pages," he said.

These scams that dupe people into giving up confidential information by playing off their emotions, rather than directly attacking their computers or networks, are known as social engineering.

Trend Micro Malaysia & nascent countries managing director Goh Chee Hoh warned that these were harder to protect oneself against as they were designed to attack the user, potentially leading them to compromise an otherwise secure system.

"Cybercriminals often ride the wave of current news and hot topics, using them as bait. Be vigilant and do not click on suspicious or unfamiliar links," he said, adding that staying informed of the news was the simplest way to protect oneself from misinformation tricks used in social engineering.

For example, in the wake of the March 2011 earthquake and tsunami in Japan, "cybercriminals created fake news sites hosting malware, or news of technology or entertainment releases that prompt attractive giveaways, to trick victims into providing and validating personal information via email," Goh explained.

> TURN TO PAGE 2

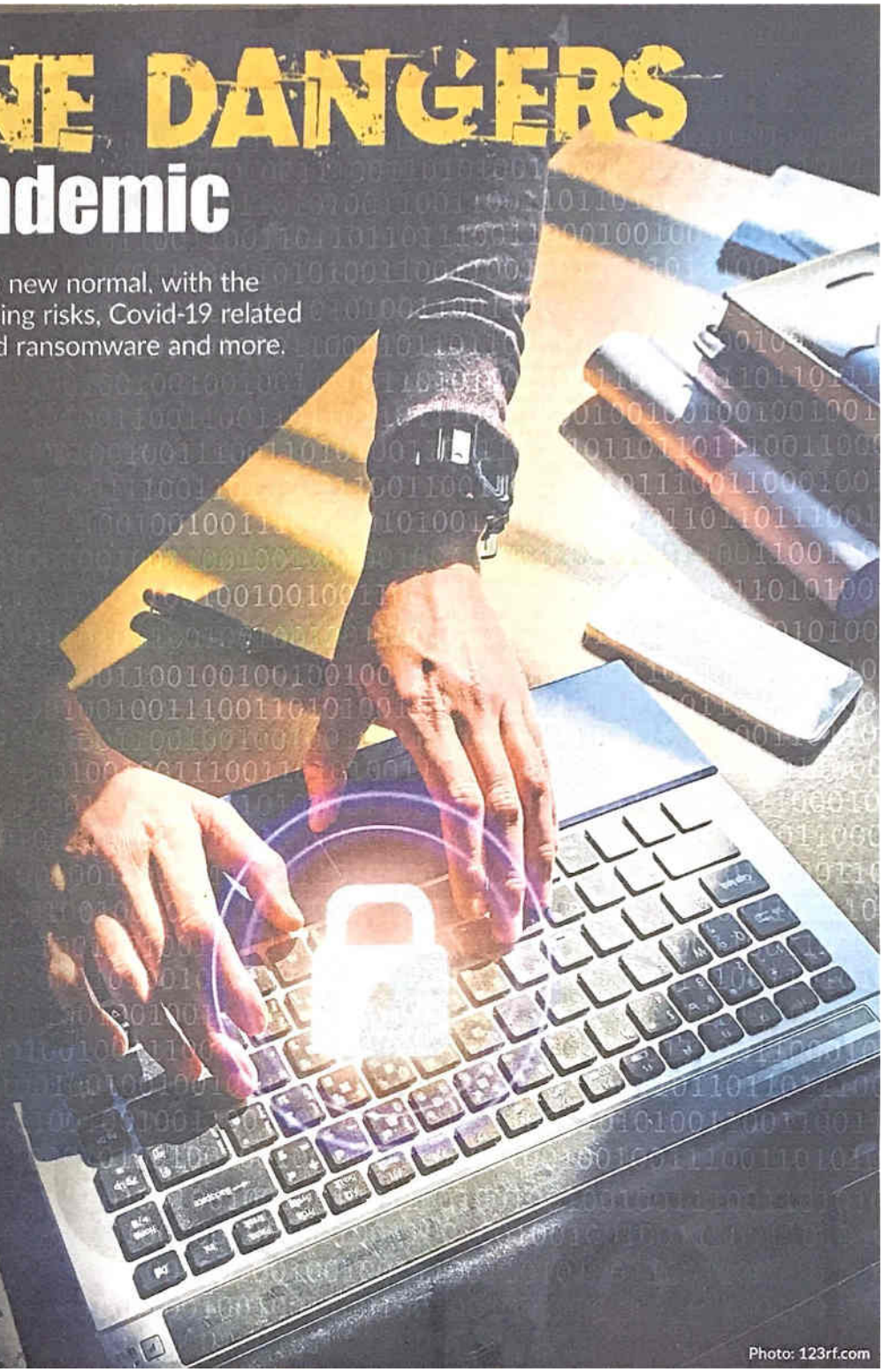


Photo: 123rf.com

> FROM PAGE 1

CYBERCRIME PANDEMIC

More recently, Trend Micro researchers found that Covid-19 was a particularly popular premise for email spam. In the first five months of 2020, roughly 92% of all the cyber threats leveraging Covid-19 were spam or phishing email messages.

"The pandemic has changed the way Internet users consume information and ramped up digital transformation. Elements such as cloud adoption, BYOD (Bring Your Own Device) and remote working have expanded the threat landscape, presenting more opportunities for malicious actors," he said.

Remote attacks

Goh pointed out that remote working, implemented by companies since March in many countries in response to stay-at-home policies to curb the spread of the coronavirus, had instead opened up companies to online attacks.

In its recent Head in the Clouds study on remote working cyber safety, Trend Micro surveyed 13,200 remote workers across 27 countries.

It found that 72% of employees felt more conscious of their organisation's cybersecurity policies since lockdown began, 85% claimed they take IT instructions seriously, while 81% agreed that cybersecurity was partly their responsibility.

Despite this appearance of being cyber secure, 56% admitted to installing and using a non-work app on a corporate device against company policy, 66% uploaded corporate data to said apps, while 39% of respondents "often" or "always" access corporate data from a personal device.

Even more worryingly, 29% felt they could get away with using a non-work app and viewed IT-backed solutions as "nonsense".

"While many employees seem to be aware of what best practice looks like, they just choose not to follow it," surmised Goh.

Cybersecurity firm Acronis' Cyber Readiness Report, which surveyed 3,400 IT managers and remote workers across 17 countries, similarly found companies unprepared to migrate from the office to their employees' homes.

The survey revealed that 92% of global companies had to adopt new technologies to work remotely, including workplace collaboration tools as well as privacy and endpoint cybersecurity solutions. Only 7% said they did not need to upgrade their existing tool set.

More than a third (35%) of companies also reported having more new devices connected to their corporate network recently, resulting in more potential entry points for cybercriminals to exploit.

This was exacerbated by the minimal or inadequate guidance provided to 47% of remote workers when switching to a work from home setup, while another 30% reported receiving no clear communication at all.

Acronis' report also found that attacks targeting remote workers had shot up, with phishing, distributed denial of service (DDoS), and videoconferencing attacks being the most commonly used tactics.

DDOS is a type of attack where hackers make a website or computer unavailable by flooding or crashing the website with too much traffic.

The report found that 39% of the global companies surveyed had experienced videoconferencing attacks, 31% reported daily cyberattacks, and half of all respondents reported encountering a cyberattack at least once a week in the past three months.

Acronis stated that phishing attacks were occurring at "historic levels", attributing it to how only 2% of companies utilised URL filtering, an oversight that led to 10% of users clicking on links to malicious websites.

URL filtering is a cybersecurity measure where businesses block employees or guests from accessing certain content or websites, usually high risk sites or not-safe-for-work content.

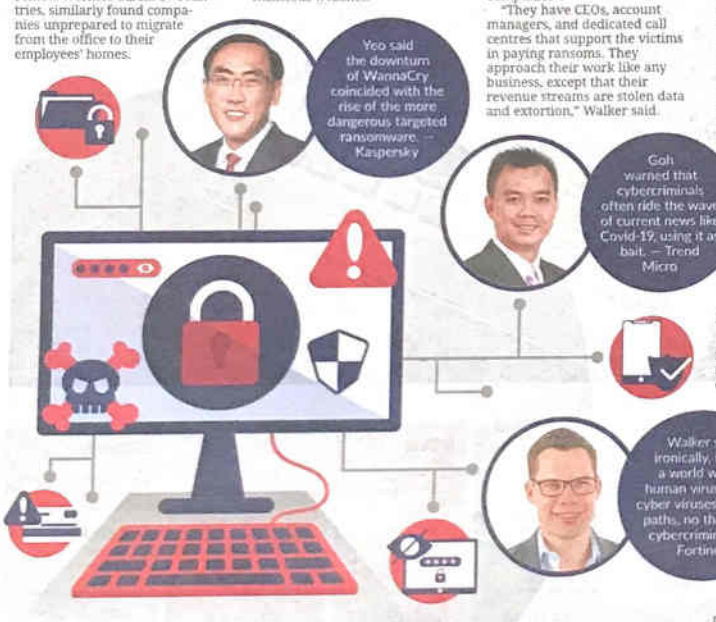
The business of crime

Asked what motivated cybercrime, Walker said most of the time, it came down to the money.

He elaborated that most breaches were driven by cybercriminals who steal sensitive information to sell on the Dark Web, or hold systems ransom by encrypting them.

He said cybercrime had become a literal business, with more than half of all attacks managed by cybercrime organisations that are "better organised than most companies".

"They have CEOs, account managers, and dedicated call centres that support the victims in paying ransoms. They approach their work like any business, except that their revenue streams are stolen data and extortion," Walker said.



Ransomware is a type of malicious software that encrypts the files on an infected computer, after which attackers would demand a ransom from the victim in exchange for restoring access to the device or files.

Two recent notable cases of ransomware attacks included the WannaCry and NotPetya cases, which both happened in 2017.

The European Union's law enforcement agency Europol stated that WannaCry hit more than 200,000 computer systems in 150 countries. This crippled the systems of many organisations, from the UK's National Health Services to car manufacturers and universities across the globe.

NotPetya also had widespread impact, locking up systems of multinational companies and public services. Then-US Homeland Security adviser Tom Bossert was reported as saying the attack caused about US$10bil (RM41.82bil) in damages.

Bossert and the United States' intelligence agencies also categorised the attack, which mostly affected Ukrainian services and companies, as a form of cyber warfare by the Russian military. The Russian government denied the accusation.

Shifting patterns

In a recent report, cybersecurity firm Kaspersky reported that ransomware attacks were on the downtrend, with the number of cases detected and blocked on computers of small to medium enterprises (SMEs) in South-East Asia dwindling from 1.4 million hits in the first half of 2019 to about half a million in the first half of 2020, largely due to more software systems being updated to reduce vulnerabilities to such attacks.

Singapore logged the largest reduction of ransomware detections at 89.79%, followed by Malaysia at 87.65% and Indonesia at 68.17%.

However, Kaspersky South-East Asia general manager Yeo Siang Tiong warned that this was no reason for companies to let their guards down, as the downturn of untargeted ransomware like WannaCry coincided with the rise of the more dangerous targeted ransomware.

"It is good news that ransomware detections against SMBs in the region have lessened in quantity, but the recent headline-grabbing incidents involving Maze ransomware and the recent WastedLocker attack – which allegedly earned US$10mil (RM41.72mil) in one infection – should be a clear reminder for all companies, however small, that we need to beef up our cybersecurity now more than ever against this costly threat," Yeo added.

In the event of such an attack, he recommended that companies immediately disconnect and isolate the infected computer from any network or the Internet.

Yeo also urged companies not to negotiate with cybercriminals, as there was no guarantee the encrypted files would be safely unlocked once the ransom was paid.

Giving in to their demands would only encourage hackers to keep operating, he added.

Staying safe

Fortinet's Walker said a robust cybersecurity strategy was critical for organisations and advised them to invest in their people as much as possible.

Training should also be provided on the four core pillars of cybersecurity: identifying authorised and unauthorised devices on the organisation's network, reducing unnecessary access, patching, and adding applications to the safe list, he said.

Patching refers to applying software updates to fix an exploit or bug, figuratively patching a hole in security.

"From a technical point of view, it's important to keep track of administrative accounts and passwords in general. Every employee should use multi-factor authentication wherever possible and use a password manager," Walker said.

Trend Micro's Goh agreed, saying effective password management – by choosing secure passwords that only the user knows and changing it regularly – was essential to staying safe on the Internet.

"Once you are compromised, it doesn't matter what security you use, your account is compromised," he said.

He warned those working remotely that home networks were usually much less secure than corporate offices, making them an easier attack path.

Yeo said the public's increasing reliance on social networks also made it easy for hackers to discover more personal information on them, which are then used to "customise convincing attacks".

"Social networks today are at a stage where the quality of the user experience heavily relies on a large amount of personal information; whether that be financial, location, shopping patterns, eating preferences or relationship status. While it is an essential tool which we can use, especially at this time of pandemic, it is still essential that we boost our online defenses against cybercriminals," he said.

Asked if the onus was on companies and organisations holding users' data to protect them, or on individuals to look out for themselves, Yeo said all parties had to work together for a holistic approach to cybersecurity.

"There is no silver bullet against all types of online threats. Our defences against them should consist of people, processes, and technology.

"This means individuals should be vigilant, protocols on data should be defined, and adaptive cybersecurity tools should be deployed by all organisations, no matter how big or how small," he summed up.