ESET APAC Consumer Survey 2018 Report:

Research and advice from ESET® regarding cybersecurity risks, behaviour and concerns within the APAC region

ENJOY SAFER TECHNOLOGY™

Cybersecurity is everyone's responsibility

Gone are the days where cybersecurity was mainly the responsibility of IT professionals. With everyday consumers relying on devices (such as personal computers, laptops and smartphones) for tasks ranging from banking, online shopping, transport and entertainment, the internet is integral to our lives.

Cyberattacks across APAC have grown far and wide. Retail, banking, aviation and even government sectors were not spared in recent incidents. Internet safety is therefore all the more important – it is not enough that consumers simply 'know' best cybersecurity practices, but must also take a conscious effort to implement them in their daily online interactions.

As APAC countries continue to push digital agendas and developments, consumers are spending more time on the internet, particularly through their smartphones. Indonesia has the world's highest mobile e-commerce penetration rate, Thailand leads the way in mobile banking penetration, while ride-hailing apps are the top, internet mobile service in Singapore.

From October to December 2018 ESET surveyed consumers across the region, aiming to learn about their online behaviours and habits. 2,000 respondents from each country, consisting of Hong Kong, India, Indonesia, Malaysia, Singapore, Taiwan and Thailand were surveyed. This whitepaper aims to address the differences in cyber-savviness between the countries surveyed, analysing their habits based on previous online interactions. We studied their awareness on basic cybersecurity threats, best practices and their actions online.

This report includes:

- Internet safety practices of APAC consumers when it comes to online shopping
- Internet safety practices of APAC consumers when it comes to internet and social media
- Parents and their children's internet browsing habits
- The state of cybersecurity education within the APAC region

An overview of 2018

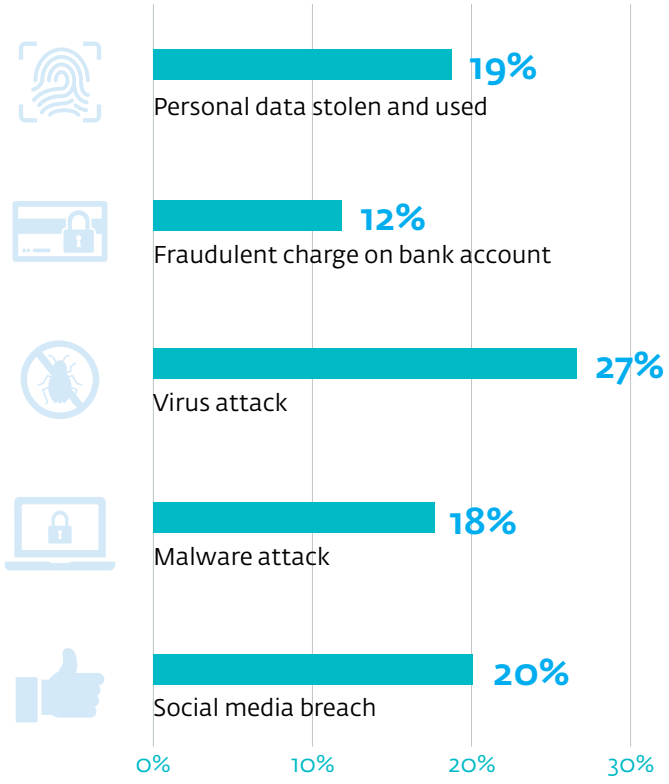
The personal information of more than a billion records of personal data were compromised in 2018 because companies failed to keep it safe.

More than a billion personal data records were stolen in 13 breaches at 11 different companies in 2018 according to personal virtual private network service provider NordVPN. ESET's APAC Consumer Survey revealed that 58% of respondents across APAC had experienced a data breach in the past 12 months.

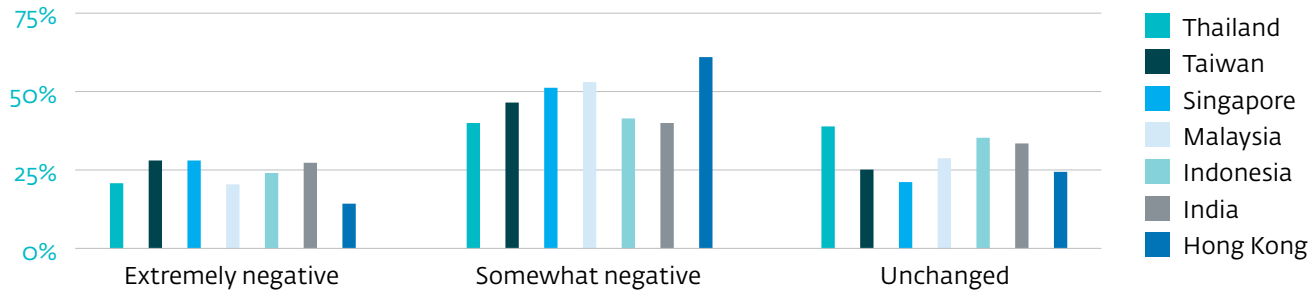
Beyond being an invasion of privacy, data breaches can affect the reputation of the companies. The biggest breach of the year exposed the data of half a billion customers of the Marriot hotel group's Starwood properties, including the St Regis, Westin, Sheraton, Aloft, Le Meridien, Four Points and W Hotel brands. 77% of respondents from ESET's APAC Consumer Survey indicated that they would feel negatively about companies that suffer from a data breach.

"Data is increasingly more valuable as we digitalise more and more of our lives," said Nick FitzGerald, ESET Senior Research Fellow. "Although some breaches still only involve basic attack methods, cybercriminals are also evolving, using more sophisticated techniques to infiltrate their targets and steal their data."

HAVE YOU EXPERIENCED / SUFFERED FROM ANY OF THE FOLLOWING BREACHES
in the past 12 months?



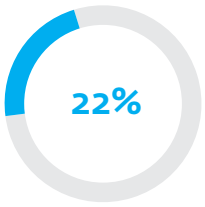
When you hear of a **COMPANY THAT HAS SUFFERED A CYBERATTACK OR BREACH,** does your opinion of that brand change?



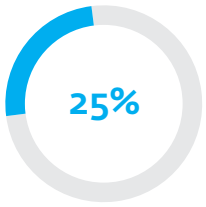
However, all is not lost for the affected companies. Following such data breaches, victimised companies often make public statements about the situation to provide a degree of transparency. So long as such reputation recovery tactics are seen as genuine, this is a good approach according to our survey respondents. The most common response in the ESET APAC Consumer Survey to the question 'What is the best way for companies to regain your trust after a hack or data breach?' was that companies should apologise and tell customers what happened and how it was resolved.

"Organisations should be upfront about these occurrences to instil trust in their consumers and those affected that they are doing everything to resolve the problem. In that way, consumers say that they would feel a greater sense of genuine care from the organisation," added Nick.

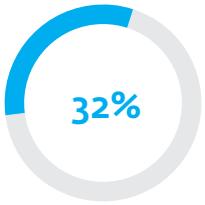
What is the best way for **COMPANIES TO REGAIN YOUR TRUST AFTER A HACK OR OTHER DATA BREACH?**



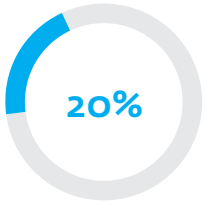
Reaffirm its privacy policy in a clear message



Provide proof that the right systems are in place



Apologise and tell customers what happened and how it was resolved



Compensate victims affected by the hack or breach

Are online shoppers easy targets?

Unsafe online behaviour and lack of awareness are making it simple for hackers.

Online shopping and e-commerce have become commonplace over the past few years. Global tech companies such as Apple, Grab and Alibaba are also capitalising on this with their own versions of mobile wallets. Consequently, merchants have adapted by offering cashless payment methods - three-quarters of supermarkets and convenience stores in Singapore, Malaysia and Thailand have now started accepting Alipay alongside other e-wallet methods. This has led to QR code payments ballooning to nearly $16 trillion within the first quarter of 2018, as reported in a survey by Nielsen and Alipay, by CNBC.

Stored payment and delivery information, though convenient, also renders consumers vulnerable to a suite of cyberattacks such as having fraudulent transactions charged to their accounts, and their personal information being misused. Moreover, as online shopping seasons gain popularity, online retailers and the personal information they store, coupled with weak passwords are a hacker's treasure trove. It was not surprising that the previous year saw breaches from large, global retailers. Thankfully only 32% of APAC respondents from ESET APAC Consumer Survey indicated that they save their information online. Still, this number ought to be lower given the vulnerability of online retailers.

With the exception of Thailand, all the countries in our survey are mobile-first countries, with an average of 61% of respondents saying they use their mobile phones for online transactions. This is a cause for concern, given that mobiles have yet to be equipped with robust cybersecurity solutions. Exacerbating this is the growing availability of free Wi-Fi.

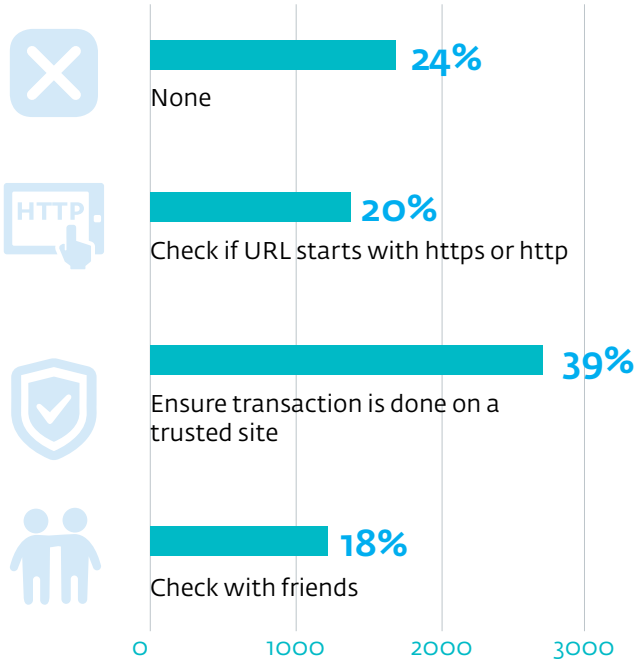
Nick explains, "As public Wi-Fi is often unsecured and free for all to access, users are exposed to more threats around Wi-Fi interference. The most common one being a 'Man-in-the-Middle attack' where a hacker maliciously intercepts communication between two parties".

DO YOU SAVE YOUR CREDIT CARD DETAILS
on your computer for an easier shopping experience?

Despite consumers being familiar with online activities, there is a gap in knowledge of best practices when it comes to such online activities. Most APAC consumers also voted for secure payment as a "more important" factor when selecting sites to purchase from. However APAC consumers have indicated that they may not be prepared in protecting such information. Only 39% of respondents ensured that their transaction was done on a trusted site, before proceeding to make a transaction.

"The gap between the knowledge and concerns of shoppers and their actions is an issue that cybersecurity providers and relevant authorities need to address," concludes FitzGerald.

ONLY 20% OF RESPONDENTS KNEW HOW TO CORRECTLY IDENTIFY A SITE'S SECURITY,
with the majority opting for a regularly mistaken method



Parental guidance should be a necessity

Facebook, Instagram, YouTube, Twitter, Snapchat...the list of social media platforms continues to grow every day. With the vast availability of smartphones, tablets, laptops and desktops, it's no surprise that children are spending prolonged periods of time online.

Without the right supervision, however, children put themselves as well as their families at risk.

ESET's survey findings revealed that only 29% of respondents deploy parental controls on the devices which their children use. The findings also revealed that 29% of respondents also give their children permission to download programs and apps on their own.

"Parental controls should be reinforced more, especially with the emergence of social engagement or content platforms. At a young age, a child's curiosity should be nurtured as well as protected. Parental controls filter accessibility to possible illicit content that may have a negative impact on children. Parental controls also indirectly teach children the value of money when purchasing things online. This is a valuable lesson for children to learn at a young age, to ensure that they do not take online purchases for granted" said FitzGerald.

In addition to parental controls, parents themselves should also be responsible for their children's actions online, which 36% of APAC respondents are doing by monitoring their child's activity while on their smart devices.

ONLY 29%
deploy
PARENTAL CONTROLS
across APAC

PARENTS AND WHETHER THEY GIVE PERMISSION TO THEIR CHILDREN TO DOWNLOAD APPS

As parents, we utilise smart devices as a means of educating and entertaining our children. It is therefore important to ensure that the content, platforms and other users that they engage with, are safe. Cybercriminals may look to take advantage of a child's trusting nature, in exchange for personal or financial information that would lead to a scam or identity theft.

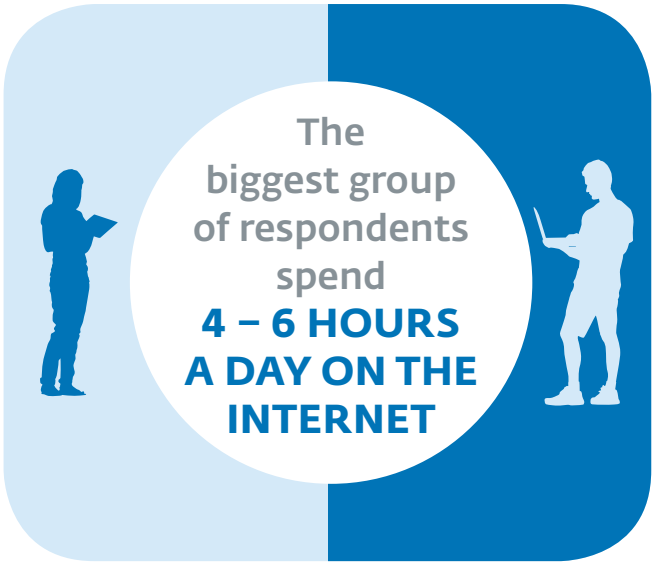
"Monitoring our children's activity online is necessary, especially if we want them to learn and be safe online. Being new to the internet can either be a fulfilling or daunting experience for them. It is therefore important to mitigate the risk of them encountering a cybercriminal to dampen their experience. Furthermore, it is also to ensure that they do not pick up bad habits such as cyberbullying. At the end of the day, we want our children to cultivate good habits and etiquette both online and offline," added FitzGerald.

When share becomes scare – cybercrime on the rise from unsafe social media behaviour

With increased internet access, people are spending more time online. Social media has also become all-pervasive, and at the same time, a hotspot for cybercrime.

Smartphones are the device of choice to go online due to their convenience and portability, and unsurprisingly 67% of survey respondents choose to access the internet via their mobile devices. Furthermore, 68% of respondents from the ESET APAC Consumer Survey spend upwards of three hours a day on the internet, with roughly 10% spending as much as 10 hours a day. A significant majority of respondents in all countries (64% or greater) except Thailand (45%) claimed to spend up to six hours a day on the internet. Thailand was the only country in this survey where a majority of respondents (55%) claimed to spend 7 or more hours per day on the internet.

With increased access to the internet, it becomes easier for users to indulge in different platforms on the internet. Most online platforms require a password to create an account and it is often the only form of security used to protect any personal information on the platform. Taking a look at password uniqueness across platforms, just under half (48%) of APAC respondents use similar passwords across platforms. Most notably, 70% of respondents from Hong Kong mentioned that they used similar passwords across platforms. Ideally, there shouldn't be any users who use similar passwords across platforms as it gives hackers an 'easier time' trying to breach multiple platforms. They simply have to guess one password, or obtain access to them through one of the many public disclosures of login credentials from popular internet services, to access the rest.



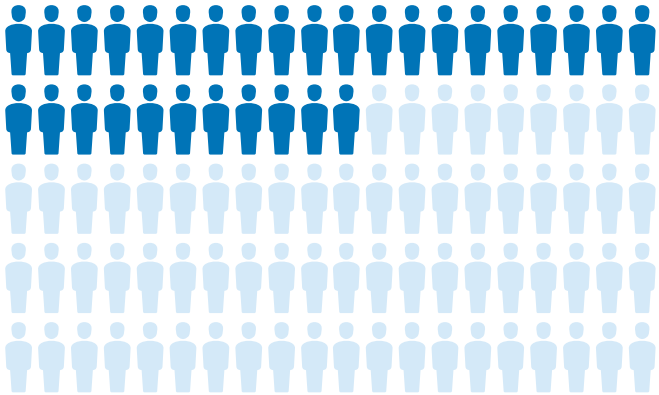
Social media is one of the most popular uses of the internet today, and with good reason. It has become the new way to easily keep in touch with friends and family. However, social media users take it one step too far and tend to overshare. Often details such as their location, holiday details or other personal data is shared, making them vulnerable to cybercriminals or worse.

JUST UNDER HALF (48%) OF RESPONDENTS
use similar passwords across platforms

Notably,
70% OF HONG KONG RESPONDENTS
indicated that they used similar passwords across platforms

According to our survey, 79% of respondents do some form of vetting before chatting with strangers or do not chat with them at all. However, this means that 21% of the respondents do freely chat with strangers on social media, opening themselves up to possible cases of identity theft.

To make things worse, 31% of respondents revealed that they have shared personal information with strangers over social media; personal information that may help cybercriminals commit identity theft or host a social engineering campaign targeted at their loved ones. This not only affects the user involved, but their close friends and family. If as many as 30% of respondents have shared personal information with strangers, more needs to be done to educate the public on the dangers of oversharing on social media as well as the extent of the damage it can cause.



31% OF RESPONDENTS
admitted to sharing personal information with strangers via social media

"With increased internet access, people are spending more time online. It is heartening to see that people in the APAC region generally have safe online practices. However, more can be done to increase awareness of security and privacy best practices to ensure that everyone will be safe online," commented FitzGerald

Knowledge is power when it comes to cybersecurity

As many APAC nations push forward on digitising businesses and e-commerce, data becomes increasingly more important.

Data allows businesses to cater their products and solutions to consumers, based on our online behaviour and habits. Furthermore, our personal data is a digital footprint of our identity online, thus making it even more important to be kept confidential and safe.

Like a double-edged sword however, the evolutionary use of data comes hand-in-hand with cyberthreats which are becoming increasingly sophisticated. Therefore, aside from the importance of data, understanding the evolving cyberthreat landscape and how cybersecurity solutions aid in protecting users is critical.

The ESET APAC Consumer Survey showed 27% of respondents being confident in their understanding of cyberthreats. This is worrying as it suggests the other 73% of respondents might only have a superficial understanding of cyberthreats.

When asked where most cyberattacks originate from, respondents polled 'Downloading files from the internet' as their top choice. While this isn't wrong, consumers should be made aware of the different ways in which cyberthreats can affect them and how sophisticated they have become.

"As we continue down the road to a more digital future, it is important for consumers to understand the types of threats that they could potentially face and how they can avoid them. It is inevitable that we will need to share our data online, but doing it safely is what makes a big difference," said FitzGerald

"It is encouraging however to see that 78% of APAC respondents have indicated that they are receptive to learning more information about cybersecurity. Education should be the first step towards prevention and protection in our fight against cyberthreats and cybercrimes," added FitzGerald.

While many consumers have the perception of cybersecurity solutions being just 'antivirus' protection, this needs to change as the threats evolve and become more sophisticated.

78%
of APAC respondents are open to learning more about cybersecurity

27%
of APAC consumers are confident in their knowledge and understanding of cybersecurity

40%
of APAC respondents learnt about cybersecurity through personal reading, showing an opportunity for formalised education to be provided

Tips and tricks to stay safe online

While it may seem like all online threats are out to get you, there is still hope. Here are some tips to keep yourself safe online:

Tips for Online Shoppers

- Online shoppers should definitely avoid saving payment information on the retailer's portal, to prevent any potential loss of data through a data breach.
- Ensure that transactions are done on secure networks and not on public networks.
- Online shoppers should also always check that the websites they are making transactions on are secure, and that they are on the retailer's official website.
- Links from banner ads could potentially lead online shoppers to an imitation site of the retailer, which are done in an attempt to steal personal and financial data.

Tips for Internet and Social Media Users

- Consumers who frequent social media platforms should avoid using similar passwords across platforms. This puts all their accounts at risk, should the password be guessed.
- Consumers should also avoid storing passwords on their browser as the browsers offer no protection if someone gets hold of the physical device. A password manager comes highly recommended as the way to manage the different passwords.
- Be wary when using public Wi-Fi to access the internet. Always take some precautionary measures when logging in, in case cybercriminals set up false networks to lure unsuspecting people in. Some ways to ensure safety include checking if the website uses https, using a virtual private network or simply not accessing sensitive information while connected to public Wi-Fi.

Tips for Parents

- Avoid giving free reign of your smart devices to your children as they may not necessarily know how to ascertain the safety of the websites they are surfing.
- Parental controls should be considered if parents wish to grant their children access to their smart devices, without their supervision. Parental controls on laptops are especially important as they are designed to block inappropriate or dangerous websites.
- Exercise restraint in allowing children to conduct online transactions with a credit card as they may inadvertently share credentials on a non-secure site or take for granted the spending.

By applying some of these tips, you may very well avoid a terrible online experience, or dodge the attempts of a cybercriminal.


ENJOY SAFER
TECHNOLOGY™