Mapping a secure path for the future of digital payments in APAC

An Asia Pacific Study

APAC Corporate Communications
Kaspersky
October 2021

kaspersky

INTRODUCTION

As one of the key pillars of the digital economy, electronic payments has helped enhance the economic and social wellbeing of billions of people globally. Closer to home, the Asia Pacific (APAC) region is the largest contributor to global payments revenue, with analysts expecting the sector to exceed USD $1 trillion revenue by 2022 or 2023. With the rapid proliferation and adoption of digital payments, industry players in this dynamic ecosystem are clearly playing a high stakes game, expanding aggressively into multiple markets with creative marketing solutions in the hope that every single click would represent a small but significant step towards market domination.

Let us use the fairly innocuous example of shopping in a supermarket in Asia. Having painstakingly selected all the grocery items you need for the week ahead, you proceed to the checkout counter only to find it plastered with decals belonging to GrabPay, Android Pay and Apple Pay. To push the proverbial envelope a bit more, even the supermarket has hopped on board the digital payments express, where you can now also use their newly launched mobile wallet to make payments as well.

While you take some time to deliberate which digital payment method to transact with, the time is ripe for us to conduct a deeper dive into our adoption of digital payments, and what this means from a cybersecurity perspective. Specifically, this report seeks to map out what digital payments are used for, while bringing to you a first-hand account of what are some of the challenges users have experienced when it comes to making an electronic transaction.

In the age of digital interdependence, it is important that we are able to leverage technology fully to our benefits, while mitigating some of the risks it brings along as well. Thus, the report also includes tips and suggestions from the Kaspersky's cybersecurity experts, to equip people with the right tools and information to navigate the complexities of digital payments.

> **"The surging demand for digital payments has transformed the way we transact both online and offline. Businesses are now digitalising their operations to capture additional revenue through digital payments, while consumers are heavily reliant on it due to the ease and convenience it offers. It is clear that the demand for quick, efficient and low-cost payment experiences will encourage further innovation in this space, and we are seeing that happening with the emergence of real-time payment rails. With the digital payments ecosystem evolving at a breakneck speed, so too must our understanding of the challenges and opportunities it brings. We hope that this study can help shed some light on what some of the user attitudes are when it comes to digital payments, and plug any knowledge gaps so we can further encourage the growth of a robust and secure payments ecosystem in the region."**
>
> 
>
> Chris Connell
> Managing Director for Asia Pacific
> at Kaspersky

METHODOLOGY

The Kaspersky "Mapping a digitally secure path for the future of payments in APAC" report studies our interactions with online payments. It also examines our attitudes towards them, which hold the key to understanding the factors that will further drive or stem the adoption of this technology.

The study was conducted by research agency YouGov in key territories in APAC, including Australia, China, India, Indonesia, Malaysia, Philippines, Singapore, South Korea, Thailand and Vietnam (10 countries). Survey responses were gathered in July 2021 with a total of 1,618 respondents surveyed across the stated countries. The respondents ranged from 18-65 years of age, all of which are working professionals who are digital payment users.

Through this study, when the behaviour of the population of a market is generalised, it is in reference to the group of respondents sampled above.

Key Findings

- **90%** of respondents from Asia Pacific (APAC) have used mobile payment apps at least once in the past 12 months.
- **15%** of respondents started using digital payment methods only after the pandemic.
- Smartphones **(82%)** is the device most used for e-payments in APAC.
- **81%** of respondents said they used digital payments due to convenience.
- **41%** of those surveyed would not purchase from an eCommerce provider or seller if it had previously been subjected to any form of cyberattack.
- **38%** of users were concerned about financial loss when it came to both online and offline transactions.
- **22%** still get a bit anxious when they make payments online.
- **60%** felt that banks and payment companies should provide more incentives to encourage users to maintain good cybersecurity practices.

Kaspersky's Digital Payments Barometer

When did you start using digital payments and how often?

Across the markets surveyed, digital payments have emerged to be the leading choice for many consumers when it comes to conducting their online financial transactions, with 9 in 10 using mobile payment apps at least once in the past 12 months.

Additionally, over half of respondents surveyed shared that they used at least one form of digital payment at least once a week in the past 12 months:

- Mobile payment apps (58%)
- Internet banking via mobile bank app (53%)
- Debit card (36%)
- Credit card (33%)
- Internet banking via browser (31%)

With such high adoption rates, the top 3 reasons pertaining to consumers' familiarity and comfort around these technologies were unsurprisingly attributed to:

- Convenience (81%) – the ability to make payments anytime and anywhere
- Ease of access (46%) – digital payments are easy to navigate and helps with the management of financial data
- Privacy (39%) – Online banking and mobile wallets offer greater privacy than face-to-face transactions

Even before the pandemic, there were multiple reasons to get excited about how the digital payments boom represented a larger paradigm shift in terms of facilitating the ease of access to financial services and how it was revolutionising the way businesses and individuals conduct financial transactions.

However, the COVID-19 pandemic came and threw the playbook out of the window, turbocharging our transition into digital financial services. With 85% of respondents reporting the use of digital payments prior to the pandemic, the devil is in the details – only 15% embarked on their own digital payments journey during the pandemic. While it is clear that digital payments is on an upwards trajectory, it is important to uncover the reservations consumers have if the payments industry is to capture any additional growth opportunities offered by this residual demographic.

Of the 15% who started using digital payments only during COVID-19, 48% of them expressed concerns with losing their money online, with 41% afraid of storing their financial data online, and 35% not trusting the security of digital payment methods. However, the pandemic also created a serendipitous moment which gave consumers a much-needed nudge due to:

- It being safer and more convenient than making a physical transaction, especially during the COVID-19 pandemic (55%)
- Allowing consumers to make payments while adhering to social distancing (45%)
- It was the only way one could make payments during the lockdown (36%)
- It is more secure now than before the COVID-19 pandemic (29%)
- I get incentives and rewards from using digital payment methods (29%)
- My family and friends are using it (23%)
- The government is promoting the use of digital payment methods (18%)

What do we use digital payments for and what devices do we use?

With countries in the APAC region improving their mobile connectivity and making the transition to 5G services, it comes as no surprise that the region has one of the highest levels of mobile penetration rates in the world, with smart phone adoption expected to surpass 80% by 2025. When it comes to digital payments, a mobile-first approach appears to be dominating the way in which people transact, with 63% of users making payments on Android smartphones, followed by laptops at only 25%.

Based on our observation where most digital payments are made via a mobile device, this is largely compatible with the physical and digital environments we live in, with digital payments expected to be used with higher levels of frequency:

- eCommerce sites (72%)
- Money transfer to family members and friends (69%)
- Official payments such as utility bills, fines (64%)
- Ride-hailing and food delivery apps (53%)
- Physical stores such as grocery, hawker, retail outlets (49%)
- Independent online sellers on social member (39%)
- Donation or fundraising (22%)

While these statistics might not come as a surprise, the underlying current behind our findings suggest that mobile devices and financial transactions will need to feature prominently from a cybersecurity perspective if we are to sustain the current shift to digital payments.

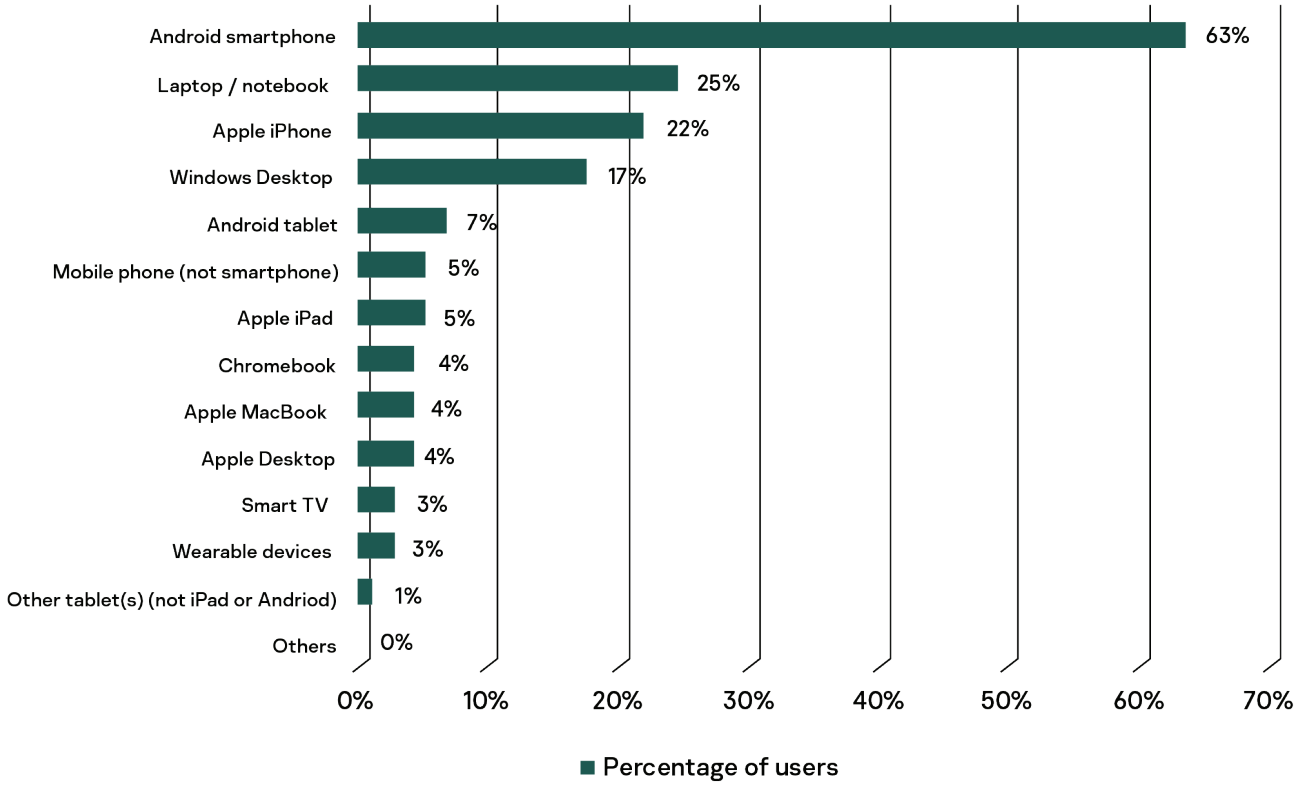

Table 1: Personal devices used for digital payments

What do consumers look for in a e-wallet provider?

As the APAC region continues its relentless transition into a cashless society, the adoption of e-wallets have been instrumental in changing the way we pay. Currently, 46% of APAC's 1.8 billion online population use an e-wallet on a regular basis, with the likes of Paytm, Kakao, Line, Grab, Stocard, Gojek, Apple Pay and Samsung Pay shining a path forward. With such high levels of adoption, are we already past the tipping point? What are some of key considerations consumers have when it comes to using a e-wallet?

As people become more acquainted with digital technologies such as e-wallets, so does their familiarity with the cybersecurity implications of digital payments. The ability to offer added layers of security in the form of biometric recognition and two-factor authentication was at the top of everyone's list of considerations (52%), followed by promos, cashbacks and lower transfer fees (40%), with interoperability and connectivity to other payment methods such as banks and third party payment methods (37%) rounding off the top three.

Apart from the above, a high level of anonymity and immunity from data breaches and cyber attacks also factored prominently in our survey at 34%. Also, the nature of digital payments is now truly global with the ability to make cross-border payments critical for a quarter of the e-wallet users in APAC.

Interestingly, the government and the sense of nationalism also have roles to play in this development. More than one in five admit they will use an e-wallet initiated or owned by their local government and some 14% of also stated that they would only use a locally developed e-wallet.

Such trends are worth taking note of for future start-ups wanting to dip their hands on this rapidly evolving and well accepted technology.

Why a fraction is too much friction for digital payments

With multiple digital payment players competing for a slice of the payments pie featuring low transaction costs – the business of digital payments is inherently a low value, high volume game – especially when it comes to the matter of retail payments. In turn, the digital payments ecosystem is particularly vulnerable to the whims of consumer attitudes and preferences. When we consider how the benefits of digital payments are distinguished by their ability to offer a friction-free payment experience, the need for us to understand consumers' perceptions and attitudes on digital payments becomes heightened.

When asked about the conditions needed to be achieved before one would consider using digital payments, an overwhelming 53% of respondents surveyed in our report indicated that they would shop more at stores that accept digital payments. Almost half (41%) also indicated that they would not purchase from an eCommerce provider or seller which was subjected to a data breach or any form of cyberattack.

Other key sentiments also include how more than a third (37%) would only purchase from stores and sellers which offered online or mobile payments. From this, it is clear that digital considerations about cybersecurity and payments factor heavily into a consumer's purchasing behaviour, but let us find out how this translates into reality based on some of the experiences our respondents have shared:

- Digital payments are convenient (75%)
- Digital payments are easy to learn and understand (45%)
- Digital payments are more secure than I expected, and I find it easy to resolve disputes/loss of money (32%)
- Access to the internet helps me make digital payments with ease (31%)
- Cost saving (29%)
- I trust digital payments fully (23%)
- I still get a bit anxious when I make online payments (22%)
- I would rather pay with cash than digital payments (17%)
- I find it challenging to pay with digital payments (12%)

These figures paint a fairly straightforward picture of how respondents interact with the idea of making digital payments, but it is clear that with only a third confident in the security of digital payments and a quarter trusting digital payments fully, trust has become a top pain point when it comes to the adoption and experience consumers have with digital payments.

In fact, when we break down the experience of paying for something into online and offline transactions, 31% of those surveyed were more concerned about their money when making an online transaction, as compared to 12% who had misgivings about paying for something in person. While 38% were equally concerned about financial loss when it came to both online and offline transactions, such sentiments are generally more reflective of our natural inclination to avoid losing money.

How can financial institutions and digital payment providers better calibrate their approach towards digital payments?

As with most things in life, it generally takes two hands to clap. While the respondents surveyed in this report have largely agree that trust is a big issue when it comes to their adoption and use of digital payments, most felt that financial institutions and digital payment providers should step up to play their part in building a secure payments ecosystem.

For example, 60% felt that banks and payment companies should provide more incentives to encourage users to maintain good cybersecurity practices (e.g. changing passwords frequently, etc.). More than half of the respondents (58%) also welcomed more public education on the threats related to digital payments, while 35% believe that bank applications should only be used for mobile financial transactions.

From this, it is evident that the public has placed a high level of expectation on financial institutions and payment providers to take the lead when it comes to creating more awareness around the security of digital payments. Hence, it is important for businesses to be perceived as taking the lead in this area, as this could potentially differentiate themselves from others and allow them to develop higher levels of trust and engagement with their users.

What are some of the challenges for businesses when it comes to the adoption of digital payments?

Apart from the obvious benefits to consumers, those surveyed in our report also felt that digital payment methods such as mobile wallets can offer a positive boost for businesses (59%), with a similar percentage holding the view that small and medium businesses (SMEs) should start using digital payment methods. However, a significant quarter (26%) also felt that the infrastructure (e.g. internet, lack of device support, etc.) was somewhat lacking in their country.

While pivoting to a cashless economy can be challenging for SMEs, many continue to stay the course as digital payments offer not only the promise of creating productivity and process improvements in the form of reducing fraud but also open up new revenue streams, and accelerate their entry into new customer demographics and markets. Significantly, this points to the need to provide the right kind of support, especially for SMEs if they are to capture the additional growth opportunities presented by the digital payments boom.

> **"There are no questions about the efficiency and convenience digital payments has to offer, with consumers wanting the same thing at every touch point of the online or offline purchasing journey. Businesses and individuals need to be quick to adapt to the new realities of a digital economy, and it is comforting to see that many have managed to pivot successfully to e-payments in such a short period of time. However, the speedy adoption process of digital payments need to be tempered with realism – one that takes into consideration some of the sentiments people have around trust if they want to strengthen and future-proof their digital payments architecture."**

Chris Connell
Managing Director for Asia Pacific
at Kaspersky

Are we doing enough to protect ourselves?

In a digital world where convenience is often the key foundation for every solution that is developed, security software is viewed as an easy way to implement the first layer of defence for many users, so what are some of the things that people do when it comes to protecting themselves?

Today, the ubiquitous nature of technology has created greater levels of convenience for us. At the same time, this has also generated multiple touchpoints for cybercriminals to infiltrate and compromise our cybersecurity when it comes to digital payments.

Whether it is via the proliferation of phishing scams or mobile malware, it is important to establish some basic standards when it comes to cybersecurity, and the use of security solutions can help get your financial affairs in order.

Our findings showed that 49% of respondents understood the need for antivirus software to protect one's money and online data, but felt it was equally important to supplement it with other software or services. While it is encouraging that almost half of all respondents have developed an acute sense of awareness when it comes to protecting themselves when making an online transaction, almost a quarter (22%) felt that the use of antivirus software was sufficient, followed by 18% where respondents were uncertain or unaware about how antivirus could help them mitigate the risk of financial loss. More alarmingly, approximately 12% felt that antivirus software was not an essential tool in the fight against cyber threats seeking to compromise one's financial data and property

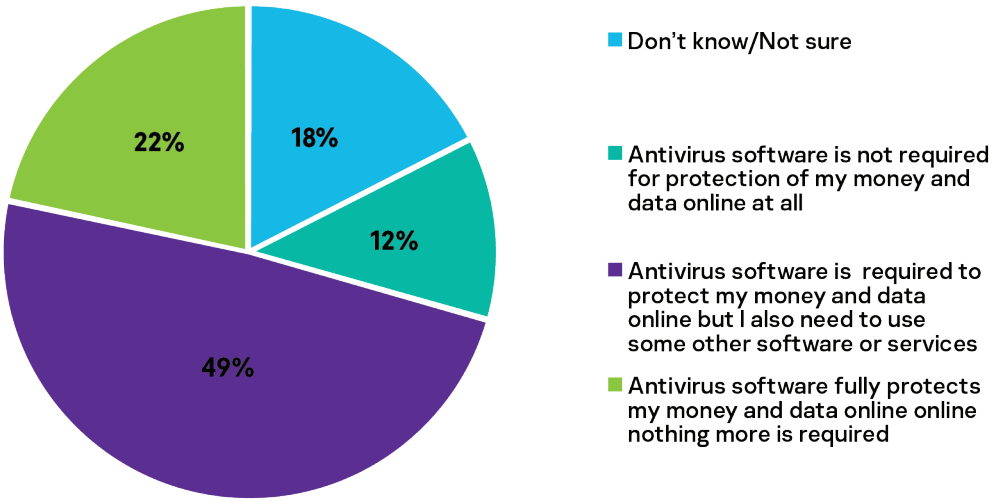

Table 2: Which of the following statements best reflect your opinion about the efficiency of antivirus software for digital payments?

"While antivirus solutions may not represent the catch-all solution to all cyber threats looking to steal our money and personal data, they should be understood as an effective safety net as most advanced solutions these days are able to filter out most of the generic attack vectors. In fact, the true significance of antivirus solutions should be best understood as an advanced warning system where the user can adopt containment strategies and alter their own personal protocols when it comes to digital payments. If this is supplemented with other preventive measures such as good cybersecurity awareness and regular password changes, the process of keeping oneself safe can actually be quite simple and straightforward."

Vitaly Kamluk,
Director, Global Research & Analysis Team (GReAT) for Asia Pacific at Kaspersky

What do we do to protect ourselves?

Engendering higher levels of cybersecurity awareness only represents one part of the puzzle. Although one can be equipped with the latest tips on how to protect oneself from threats when using digital payment methods, the critical threshold for an effective cybersecurity is often set at the point where customers are attempting to translate knowledge into practice. So what are we doing to protect ourselves and are we doing it right?

An interesting insight arising from our findings is that over a third (38%) of respondents kept the amount of money in their accounts that they use to a minimum, with a quarter (26%) not connecting their salary/main account to any mobile wallet applications. With the popularity of mobile wallets and prepaid debit cards, the emergence of this as a coping mechanism appears to suggest that consumers have adopted a ring-fencing strategy – one where their main account is well shielded from regular usage or access. Again, the spectre of changing passwords frequently continues to surface in cybersecurity conversations, as only approximately a third felt that it was important to change their passwords on a regular basis. Based on research we conducted earlier this year, our solutions prevented 25% more password stealers in Southeast Asia during the first three months of 2021 when compared to the same period in 2020, with most countries in the region recording an increase in password stealing attempts. While respondents appeared to understand the need to download apps from verified sources, it appears that there is more work to do when it comes to getting people to change their habits on passwords.

When it comes to developing the right product, the findings shared above indicate that payment service providers should focus not only on coming up with a seamless end-to-end digital payment solution from a transaction-based perspective. Instead, the promise of a seamless experience should be extended to include the notion of cybersecurity, where it is important to adopt a 360-degree approach – one that takes into account customers' needs and insights about their motivations, as well as consulting cybersecurity companies at each stage of the product development cycle.

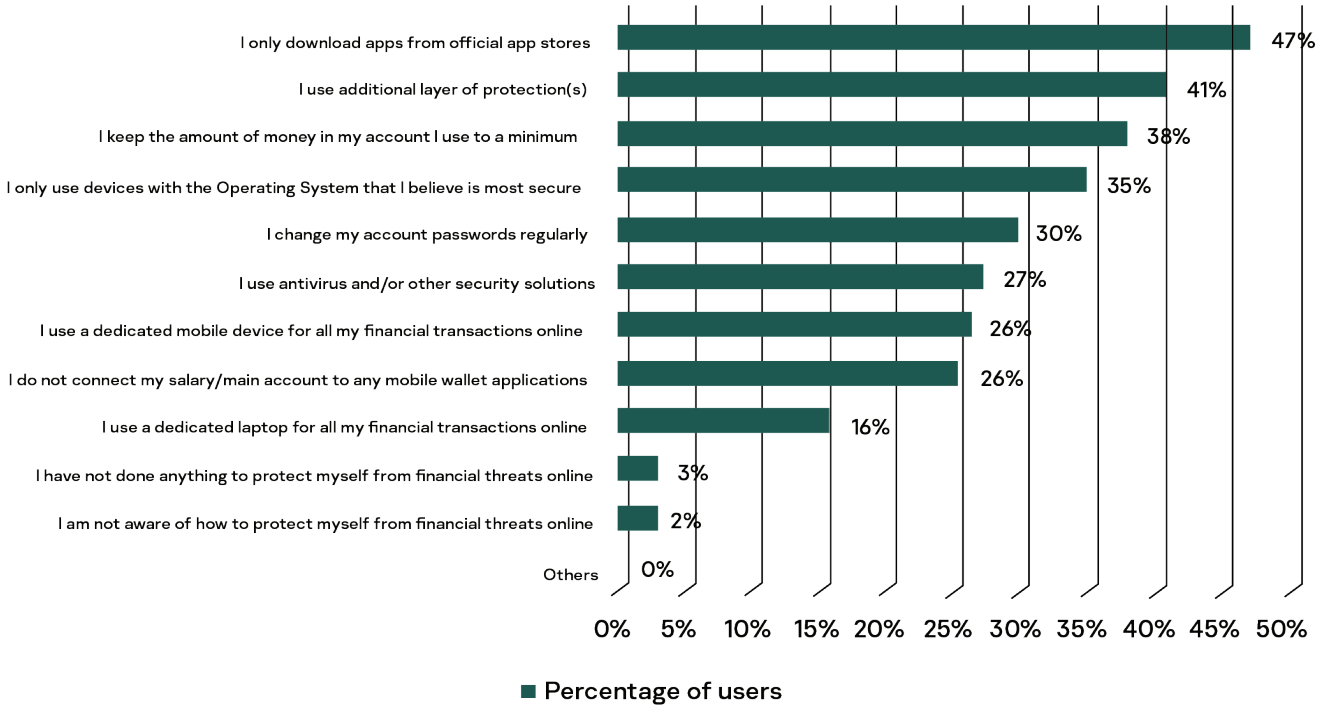

Table 3: Steps taken to protect oneself from threats

For example, if users are more likely to go along with a particular operating system to conduct their financial affairs, then it is important for financial institutions and payment service providers to look into delivering constant patches and updates to ensure that they are well protected.

Similarly, if users are keen on changing their passwords regularly, the right kind of protocol should be built into the user experience to ensure that they are able to do so on a frequent basis. Inevitably, the proactive implementation of such measures will increase your customer base and show that you care about keeping your customers safe and satisfied when transacting on your payment platform.

What have you done after encountering a threat when using digital payment methods?

Unfortunately, the complexity and sophistication of cyber threats mean that even with the best cyber defences, the occasional breach may occur. Therefore, what we do in the aftermath of a cyberattack is equally important as what we do to prevent them.

When it comes to proactive steps taken after digital payment methods were compromised, our survey found that most respondents:

- Change passwords and other security settings on their banking and mobile wallet apps (61%)
- Called their bank or payment service provider (46%)
- Informed family and friends (43%)
- Installed antivirus solutions on all their devices, regardless of whether they were infected (28%)
- Installed antivirus solutions only on infected devices (27%)
- Created a new mobile wallet account (14%)
- Did nothing because they weren't sure about what to do (6%)

> **"There are no questions about the efficiency and convenience digital payments has to offer, with consumers wanting the same thing at every touch point of the online or offline purchasing journey. Businesses and individuals need to be quick to adapt to the new realities of a digital economy, and it is comforting to see that many have managed to pivot successfully to e-payments in such a short period of time. However, the speedy adoption process of digital payments need to be tempered with realism – one that takes into consideration some of the sentiments people have around trust if they want to strengthen and future-proof their digital payments architecture."**

Vitaly Kamluk,
Director, Global Research & Analysis Team (GReAT)
for Asia Pacific at Kaspersky

The impact of cybersecurity threats on digital payments

In the APAC region, while the adoption of digital payments has been on the rise over the past few years, the rapid evolution of the payments ecosystem has also introduced new security risks that both businesses and individuals need to consider and address. For example, a study conducted by FICO found that 78% of banks in APAC saw their fraud losses increase with the introduction of real-time payment platforms and mobile payments, with almost a quarter (22%) expecting fraud to rise significantly.

With so many users using digital payment methods, cybercriminals are becoming more effective and convincing with ways to steal user data and money. The famous Chinese philosopher Sun Tzu once said: "If you know the enemy and know yourself, you need not fear the result of a hundred battles". More than 2000 years after his passing, his philosophical ruminations about military strategy continue to find their relevance in today's digital age. Having explored how well we construct our cybersecurity practices in relation to digital payments, the million-dollar question for this section is – how well do we know the enemy, or cyber threats in this instance, and how often do we come across them?

Nearly all respondents in APAC (97%) were aware of at least one type of threat against digital payment methods, while over 2 in 3 (69%) have personally encountered at least one type of threat. Additionally, from what we can see based on the statistics outlined above, there is a positive correlation with our adoption of digital payment methods and our awareness of the risks and threats that are associated with them. In many ways, this could be attributed to the volume of coverage cybersecurity incidents have been getting in the media.

However, it does appear that more awareness needs to be developed when it comes to understanding how malware can compromise our financial transactions, especially when we take into account that a majority of users have yet to experience a malware attack. According to our Financial Cyberthreats in 2020 report, the geography of attacks became more diversified and extensive, with an increasing focus on mobile banking with malware designed to steal Android users' credentials and funds.

Cyber Threat	Threats encountered	Awareness of threats
Fake websites	25%	73%
Phishing scams	24%	69%
Bank account / credit card fraud	16%	66%
Social engineering scams via text messages or calls	31%	66%
Data breaches	12%	62%
Fake offers and deals	26%	61%
Fake and fraudulent apps	17%	57%
Ransomware	9%	51%
Other malwares	7%	50%
Love scams	9%	46%
Dark web	5%	39%
None	31%	3%

Table 4: Percentage of respondents' actual encounters of threats vs awareness of threats against digital

When we examine other cyber threats such as fake websites, phishing scams, fraudulent offers and deals, it was clear that the level of awareness could be attributed directly to having more encounters with them. Where this relationship becomes unclear, is when a high percentage of respondents were aware of bank account/credit card fraud, but a relatively smaller proportion of them experienced a cyber-incident pertaining to that particular digital payment method. Simply put, this could suggest that financial institutions are ticking all the right boxes when it comes to developing a payments infrastructure that is effective in identified fraudulent transactions.

On the other hand, other cyber threats which featured more prominently (fake websites, phishing scams, fraudulent offers and deals) could possibly support the argument that it is not just about

having the right cybersecurity solutions, but the human element will take greater precedence when it comes to developing a strategy for mitigating the risk of cyber threats when it comes to digital payments.

How much did you lose from the incidents you encountered online?

When it comes to measuring the material impact of a cyber-incident involving digital payments, the top 5 threats resulting in financial loss are:

- Fake offers and deals (10%)
- Fake websites (9%)
- Social engineering scams via text messages and calls (9%)
- Bank account/credit fraud (9%)
- Phishing scams (7%)

Based on the findings outlined in the table below, the amount of financial loss arising from cyber threats targeting digital payments appear to be mostly capped up to USD $5,000, with a very small proportion of respondents having reported incurring a loss of more than USD$ 5,000. This in line with industry standards that the average online spend for the APAC region hovers around USD $2,181. Despite the low levels of financial loss due to cyber threats, every single dollar quickly snowballs into quite a significant amount, especially when we consider that the retail payments industry operates on a low value, high volume business model.

Amount lost from threats	Fake offers and deals	Fake websites	Social engineering scams via text messages and calls	Bank account/credit fraud	Phishing scams
Less than USD $100	24%	23%	15%	21%	14%
USD $101 - 500	9%	7%	6%	14%	7%
USD $501 - 1,000	4%	3%	1%	9%	5%
USD $1,001 - 5,000	2%	1%	3%	6%	3%
USD $5,001 - 10,000	1%	2%	2%	2%	1%
More than USD $10,000	2%	2%	2%	2%	2%
None	59%	62%	71%	45%	69%

Table 5: Percentage of respondents experiencing material impact of a cyber-incident involving digital payments

How, if it all, did encountering these threats when using digital payment methods affect you?

At the same time, the impact of a cyber threat when it comes to digital payments does not just impose a financial burden on consumers, but also affects them from a psychological perspective. For example, 62% of respondents said that they became more vigilant after experiencing a cyber incident, with 31% feeling anxious about recovering their lost money.

The concept of trust in digital payments also manifested itself in an interesting manner, where our survey found that 33% of respondents trusted their banks/digital payment provider to resolve the issue, with 20% sharing that the encounter of a cyber threat affected their confidence in digital payment providers. Based on this, it appears that consumers exhibit a higher degree of tolerance when it comes to experiencing a cyber issue for digital payments as long as banks and digital payment providers were willing to rectify the issue, as compared to a fifth of respondents which made it clear that any cyber incident would compromise their faith in digital payments.

From what we can gather from the survey, the adoption of digital payment methods appears to have taken on the quality of a double-edged sword, with convenience representing the positive benefits and cybersecurity risks being the less desirable aspects of digital payments. On the contrary, the qualification of digital payments in such binary terms is premature in our opinion. As with all emerging technologies, there is no inherent good/bad quality to them – how we harness them for positive gains depends on how we interact with them. If we are to leverage digital payments to their full potential, it is important that every stakeholder, whether it is government; digital payment providers; users; and even cybersecurity companies need to come together to create a robust, secure and future-proof payments ecosystem.

A wish list for digital payments

While the digital payments ecosystem continues to grow from strength to strength with unparalleled levels of adoption, the sheer market size of the APAC region continues to provide a long runway for growth. In an industry marked by fierce competition, a key differentiating factor for payment companies should not only just be determined by the innovations they bring, but also judged by the strength of their payments architecture. So how can businesses set themselves for success over the long haul? When it comes to a list of security features consumers would like to see, here's what matters most to them:

- The implementation of one-time-passwords (OTPs via SMS for every transaction (61%)
- Biometric security features and two-factor authentication (52%)
- Automated detection and intervention for fraudulent transactions (42%)
- Tokenisation – protection of sensitive data by the random generation of a code (28%)
- Point-to-point encryption (25%)

In general, these are all useful preventive measures that can potentially enhance the cybersecurity standards in the digital payments space. However, these options should not be viewed on an isolated manner, but considered as part of a comprehensive and holistic framework for thinking about cybersecurity.

For example, there are challenges associated with the use of two-factor authentication, especially when it comes to SMS-based authentication. The use of SMS-based 2FA can be unreliable at times, as password-bearing SMS messages can be intercepted by a Trojan lurking inside the smartphone, or through a basic flaw in the SS7 protocol used to transmit the messages. In such cases, it would be advisable to use authenticator apps which are entirely self-contained, with the SMS option used only as a last resort to minimise an organisation's exposure to data breaches.

Additionally, there are also concerns about the use of biometric solutions as an authentication method, which was identified by respondents as one of the technologies to be concerned about (36%). While biometrics are easy to implement and hard to alter, nothing can take away the fact that they are a form of digital data – and this means that they are vulnerable to hacking and misappropriated for nefarious purposes.

Think Mission Impossible – where spies use voice recordings and printouts of someone's fingerprint system to get access into the mainframe. Barring the unforeseen circumstance where fingerprint scanners that draw a blood sample from your finger are implemented on a commercial basis, a modicum of vulnerability is to be expected from biometric technology.

Other technologies consumers are wary off also pertain to scams being facilitated by the use of Deepfakes (63%), along with the use of smart assistants for digital payments (44%). For the former, Deepfakes remain a relatively new phenomenon, but it has been one identified by the banking industry as a threat to look out for. For example, the CEO of a British energy firm was tricked out of $243,000 by a voice Deepfake of the head of his parent company requesting an emergency transfer of funds.

As financial institutions increasingly rely on technology, including video, to help speed up the know-your-customer (KYC) process, the possibility that what they're seeing or hearing is not real heightens the need to develop solutions that can tackle the problems created by Deepfakes.

Where smart assistants are concerned as a form of security threat in digital payments, the immediate scenario that jumps out would probably be a family member doing a good impersonation of your voice and going on an uninhibited spending spree on eCommerce platforms. However, the real threat comes via its 24/7 connection to the internet.

With over 21.5 billion IoT devices in 2021, this translates into the same number of opportunities for cyber criminals looking to exploit your IT weaknesses. Just two years ago, we detected more than 100 million attacks on smart home devices in the first half of 2019.

While the path to compromising the security of your digital payments is not direct, cyber criminals can still do so by stealing your personal data and using them to conduct financial transactions. However, this can be remedied with the constant delivery of security patches, along with well-established protocols to help support customers for fraudulent cases – these additional measures can go a long way in offering users that additional degree of comfort and reassurance.

> **To develop a long-term and sustainable growth strategy, digital payment companies need to take into account some of the wants and needs of their users. While some of the preventive measures are not entirely new and have been around for some time, it is crucial to consider how security features can be integrated in a manner without compromising the user experience. Such a strategy should focus on quality not quantity, as the addition of too many features may potentially put off new and existing users from their digital payment offering. What is required, is to track where the cybersecurity gaps are when it comes to each stage of the payment process, and fit in the right IT measures in a calibrated manner.**

Chris Connell
Managing Director for Asia Pacific
at Kaspersky

How to safeguard your financial data

This report highlights a need for us to take proactive, protective steps to ensure our financial information is kept secure, both online and offline. Here are some important steps we can all take to ensure we are protected and secure:

- It is better to be safe than sorry – beware of fake communications, and adopt a cautious stance when it comes to handing over sensitive information. Do not readily share private or confidential information online, especially when it comes to requests for your financial information and payment details.

- Use your own computer and Internet connection when making payments online. As like how you would only make purchases only from trusted stores when shopping physically, translate the same caution to when making payments online – you'll never know if public computers have spyware running on them recording everything you type on the keyboards, or if your public Internet connection has been intercepted by criminals waiting to launch an attack.

- Don't share your passwords, PIN numbers or one-time passwords (OTPs) with family or friends. While it may seem convenient, or a good idea, these provide an entryway for cybercriminals to trick users into revealing personal information to collect bank credentials. Keep them to yourself and safeguard your private information.

- Adopting a holistic solution of security products and practical steps can minimise the risk of falling victim to threats and keeping your financial information safe. Utilise reliable security solutions for comprehensive protection from a wide range of threats, such as Kaspersky Internet Security, Kaspersky Fraud Prevention and the use of Kaspersky Safe Money to help check the authenticity of websites of banks, payment systems and online stores you visit, as well as establish a secure connection.

CONCLUSION

The value of protecting financial information and resources is nothing new – many of us have already been practising this even before the concept of digital banking came about – from hiding away extra money under mattresses, to storing our savings in the bank. As we go digital, our methods of saving and accessing these resources have evolved as well. On a daily basis, we make payments and cash transfers through the convenience offered by digital payment platforms. With new digital financial services continuously being launched, each with their value propositions pulling us ever-deeper into the digital economy, there begets a higher demand for cybersecurity.

In this report, we explored the various attitudes consumers have toward digital payments – be it the factors that have brought them into the digital financial ecosystem, as well as their grasp of and trust in digital payment services. It is widely recognised that digital considerations about cybersecurity and payments play a large role in influencing consumers' decision making and subsequent actions. However, despite the convenience and even cost savings going digital has brought us, our research findings have highlighted some disconnect, in that consumers still need to continue to be proactive in taking the steps to protect themselves.

For instance, rather than depend on banks and financial institutions to provide incentives to encourage users to practice good cyber hygiene habits, taking concrete steps to do so should be more intrinsically ingrained.

As we continue entering deeper into the financial ecosystem, protecting our interactions with digital payments become increasingly important as more aspects of our financial services transition online. From our research findings, a few takeaways can be gleaned. We are naturally inclined to avoid losing money and are generally careful about where and how we make our transactions in order to ensure this. As we become more entrenched in the digital economy, there is no running away from the fact that at some point or another, there will be an eventual need make digital payments.

Limiting the use of such solutions will become increasingly difficult. However, it is comforting to note that almost all users of digital payments were familiar with at least one measure to protect themselves from threats and know what to do in the instance of encountering a threat. While the statistics paint a positive picture of familiarity with cybersecurity on digital payment methods, we cannot be complacent.

The APAC region will continue to enjoy more innovations in the digital economy and such developments will drive the regional economy to greater heights. At Kaspersky, we embrace the power that we can harness through technological innovation and also ensure that these new technologies are secured.

kaspersky