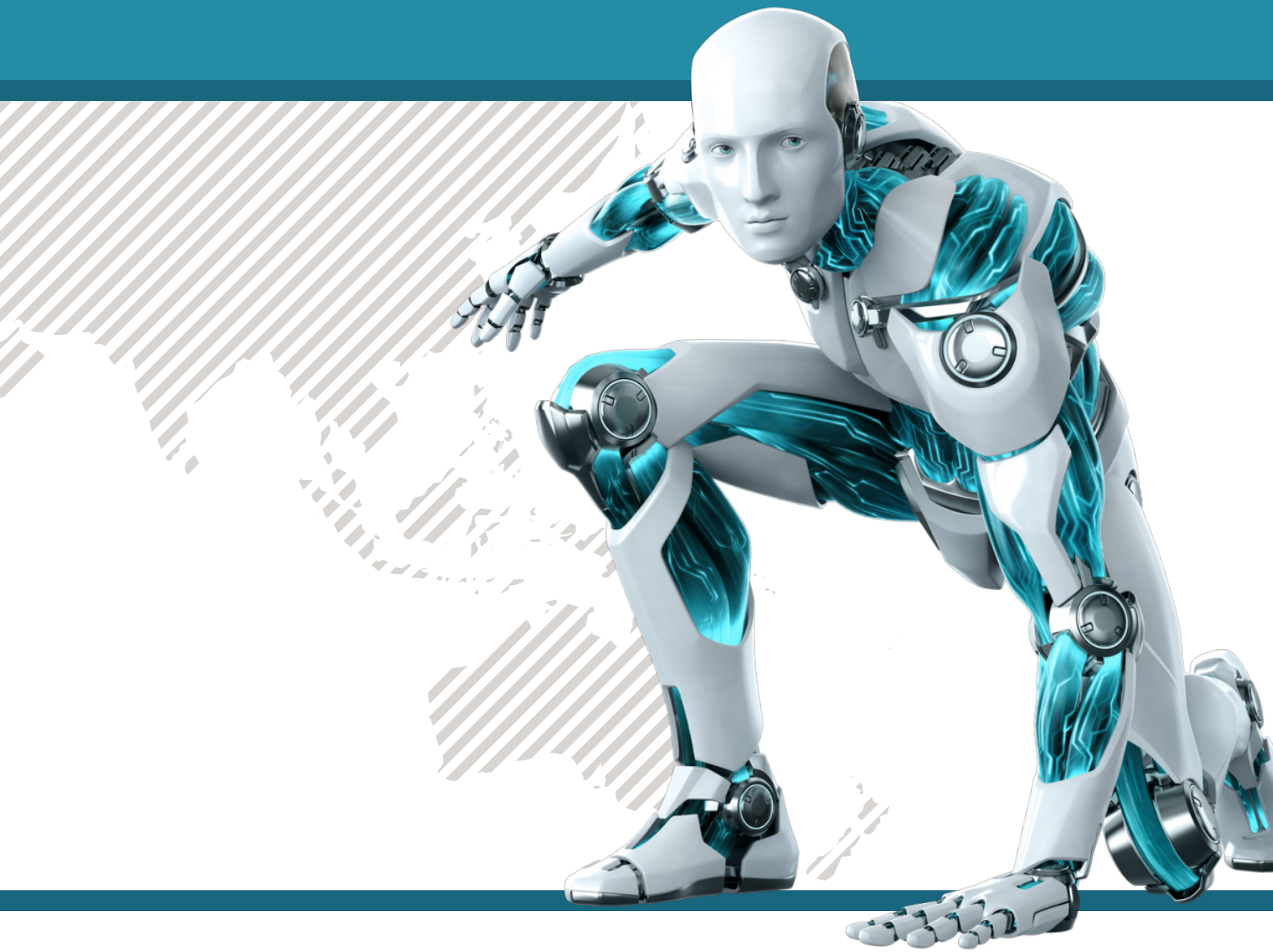
ESET ASIA CYBER-SAVVINESS REPORT 2015



CYBER SECURITY: USER KNOWLEDGE, BEHAVIOUR AND ATTITUDES IN ASIA

Contents

Background: The Threat Landscape in 2015

The cyber security landscape has evolved dramatically in recent years. Gone are the days when 'hacking' was confined to a tech savvy few, flexing their online prowess for recognition among their peers. Today, cybercrime is a multibillion black market industry, which according to analyst firm Gartner is expected to cost businesses across the world approximately US$76.9b in 2015, that's an 8.2% increase y-o-y on security spend.[1]

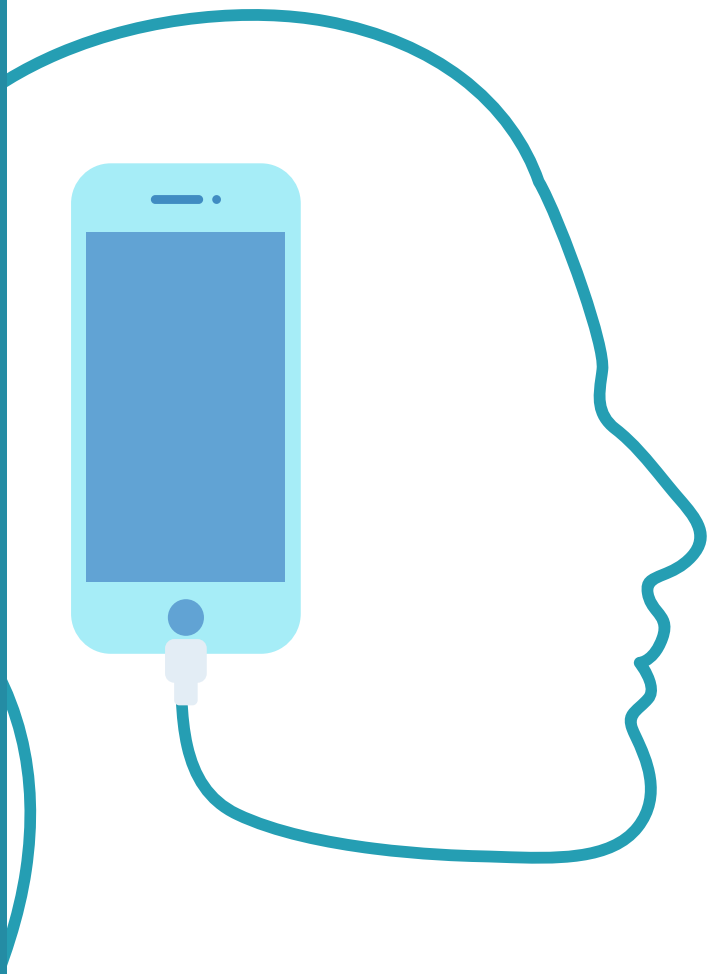
In the past, the only cyber threats users had to worry about came from viruses and unsophisticated Trojans. Today cybercriminals are better funded than ever before, employing increasingly sophisticated and targeted attacks that seek to exploit any vulnerability in a company's or individuals' network.

The results of a breach can have far-reaching implications, for businesses resulting in loss assets and/or data, including confidential information and company secrets. It can also result in disruption to a company's operations, or worse, loss of reputation and customer confidence. For individuals, the results can be just as damaging, leading to the theft of personal information, identity theft, monetary theft or personal computers being employed by hackers as 'drones' for their illegal online activities. Of course this activity also has overarching economic implications for society, costing governments billions of dollars each year.

[1] Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware http://www.gartner.com/newsroom/id/2828722

Asia-Pacific threat landscape

In Asia-Pacific, cybercrime dominated media headlines throughout 2014 and into 2015, with high profile attacks targeting Malaysian Airlines, M1, SingPass and more. This has made cyber security a boardroom issue and a key priority for governments across the region, resulting in tightened regulations and increased spending on more stringent security measures. According to a recent report by Gartner, the effects of this sea change will become particularly noticeable in South East Asia, which is expected to reach US$62b in IT spend by 2018, with Singapore, Malaysia, Indonesia and Thailand accounting for 83% of the spend, spread across data centres, software, IT services, devices and telecoms.[2]



Tech-savvy region

These figures are unsurprising given that Asia-Pacific is home to some of the most tech-savvy nations in the world, owing largely to high levels of connectivity across the region, wide availability and affordability of connected devices, plus the sheer number of users.

As technology continues to develop and evolve, so does cyber risk, as more threat vectors are opened up, increasing the number of vulnerabilities that exist for hackers to exploit.

High mobile penetration

As Google points out in its Consumer Barometer Report, Asia is leading the way forward when it comes to smartphone usage and engagement, with Singapore boasting the highest smartphone penetration rates in the world (85%). Nielsen highlights that the number of consumers in Asia owning more than one mobile device is also increasing, a trend which is particularly evident in Malaysia, where close to half (47%) own more than one mobile phone, followed by Hong Kong (31%), Singapore and China (29%).[3] According to Nielsen, tablet ownership is likewise seeing significant growth in Asia-Pacific with Singapore seeing 30% growth since 2013 to 47% in 2014, Hong Kong up 27 points to 57% and Malaysia up 23 points to 42% for the same period.[4]

---

[2] Enterprise IT spending in SEA to reach US$62bil by 2018: Gartner Digital News AsiaMar 25, 2015: https://www.digitalnewsasia.com/business/enterprise-it-spending-in-sea-to-reach-usd62bil-by-2018-idc#sthash.eY3zO6Er.dpuf

[3] Digital, Social & Mobile in APAC in 2015: http://wearesocial.sg/blog/2015/03/digital-social-mobile-in-apac-in-2015/

[4] The Asian Mobile Consumer Decoded: http://www.nielsen.com/ph/en/insights/news/2014/asian-mobile-consumers.html

Connected

According to global digital marketing agency We Are Social, in partnership with IAB Singapore, Asia-Pacific has the highest number of Internet users in the world, with over one third of APAC's population being active Internet users. The number of active mobile connections has also grown more than 11% from last year to 92% in March 2015.[5]

Growth in Cloud

Cloud is another technology which is expected to see major growth across Asia Pacific in the next few years. A joint study by Microsoft Asia Pacific and CityNet, revealed that despite the fact that the majority of Asian cities have yet to adopt cloud technology to any great extent (22%), this figure is expected to see rapid growth over the next 3 years, jumping to 46.9%.[6]

Support for IoT

Trends like the Internet of Things (IoT), which is expected to see more devices coming online and becoming connected to the network than ever before, is expected to transform the Asia-Pacific region, increasing convenience and efficiency around the way we live and work. A 2015 report from IDC Government Insights, predicts that governments across the region will support the development of IoT enabled landscapes, via investment in cloud, big data, mobility, social business, smart city programs, connected smart machines and intelligent sensors.[7] We can already see this happening in countries like Singapore and Hong Kong, and expect it to revolutionise life as we know it today.

Given the various technological developments that are taking place in this area of the world, it's no surprise that hackers are tuned in, and ready and willing to make the most of any vulnerabilities to the constantly changing technological landscape.

Cyber Attack Trends

As highlighted in the ESET Cybercrime Trends & Predictions 2015 report, we expect to see a rise in the number of attacks targeting 'things', as more devices come online. The attacks we are witnessing in Asia are becoming increasingly sophisticated, and Advanced Persistent Threat (APT) attacks or 'stealthy continuous attacks which target a specific entity' have been a major topic for discussion over the past two years. We expect this trend to continue, particularly focusing on payment systems, as more currency circulates online. We also expect to see a continuation in ransomware attacks across the region, along with those targeting digital currencies like Bitcoin.[8]

> "As infrastructure in the Asia-Pacific region continues to improve, an increasing number of consumers are adopting technology for day-to-day tasks. Online retail is a great example of this – it's estimated to be a $525.5b industry in the region. Online banking, mobile wallets, and wearable devices too are poised for similar growth and impact. As more consumers and devices connect to the Internet, the risk of cybercrime is also increasing. It's vital that we remain vigilant and continue to take proactive measures to secure our data and online activities. With the right security solutions in place, and by taking simple precautionary measures, it's possible to stay protected and feel confident online."
>
> - Lukas Raska, Chief Operating Officer, APAC, ESET

[5] Digital, Social & Mobile in APAC in 2015: http://wearesocial.sg/blog/2015/03/digital-social-mobile-in-apac-in-2015/

[6] Microsoft-CityNet survey shows Asian cities lag in cloud adoption: http://news.microsoft.com/apac/2015/02/24/microsoft-citynet-survey-shows-asian-cities-lag-in-cloud-adoption/

[7] Asia/Pacific City Governments Will Kickstart Pervasive Adoption of Internet of Things Technologies in 2015: IDC Government Insights: http://www.idc.com/getdoc.jsp?containerId=prSG25415815

[8] Cybercrime Trends & Predictions for 2015: http://www.welivesecurity.com/2014/12/18/cybercrime-trends-predictions-2015/

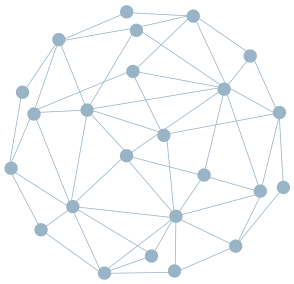
Why did ESET undertake this report?

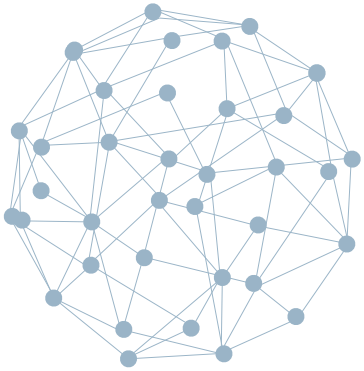
In 2015, ESET®, a global pioneer in proactive protection for more than two decades, compiled its Asia Cyber-Savviness Report 2015.

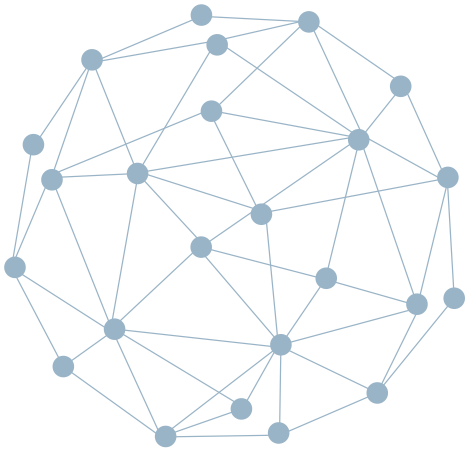
Taking in 1,800 respondents across Hong Kong, India, Indonesia, Malaysia, Singapore and Thailand, the survey aimed to provide insight into the attitudes of Internet users across Asia on the topic of cyber security, also uncovering levels of cyber security knowledge and investigating how this translates into how people behave online, the activities they engage in and the precautions they take while surfing the internet.

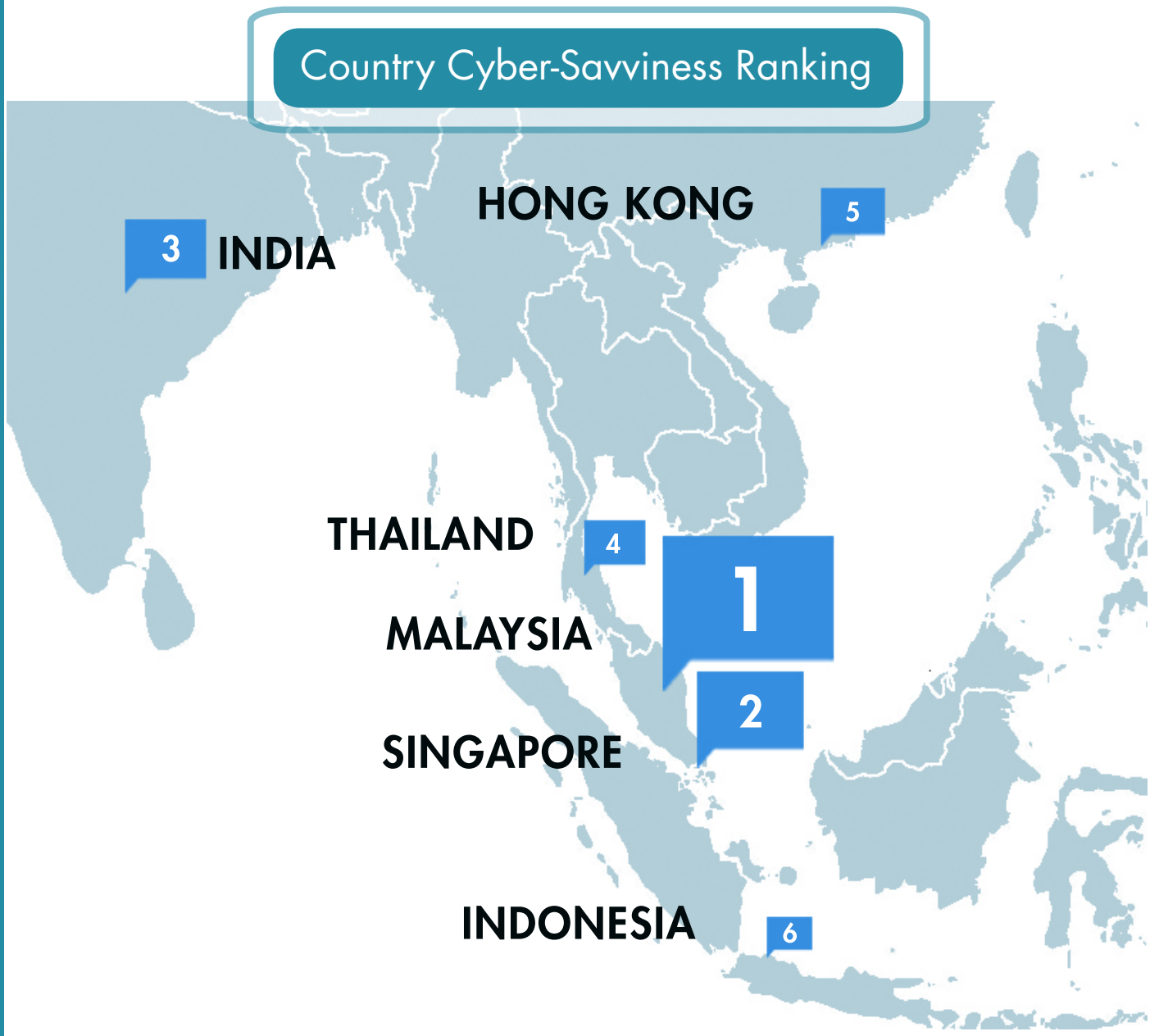
Report Methodology

The ESET Asia Cyber-Savviness Report 2015, was commissioned by ESET. The survey was conducted from April - May 2015 by a third party research company, via an online and mobile survey. Respondents were aged between 18 - 55 years, with a 52% male to 48% female split across the countries surveyed.









Knowledge Gap

The results of the survey indicate a lack of basic cyber security knowledge and understanding across all six countries. Overall, the scores were very close, with Malaysia coming in at first place for overall cyber-savviness, with a 29.9 percent score, ahead of Singapore (27.2%), India (27.3%), Thailand (26.7%), Hong Kong (25.6%), and Indonesia (25.1%).

Bottom Rung: Indonesia

Survey results showed that Indonesia was the least cyber-savvy nation out of the six countries surveyed. Indonesia ranked second to last when it came to cyber knowledge, also ranking as the second most likely nation to take risks online (behind India). The country also scored low on the proactive steps taken to increase online safety.

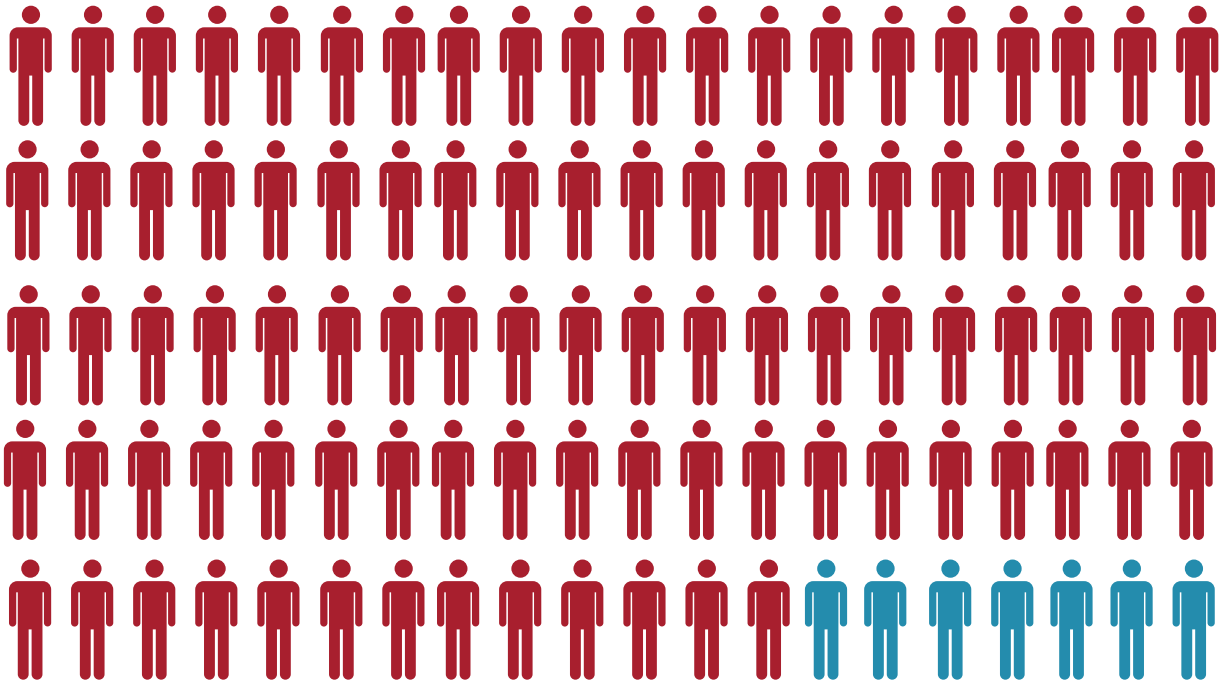
Calculating Cyber-Savviness

Cyber-savviness calculations were based on a number of factors including how knowledgeable respondents were when it came to cyber security (based on the number of questions they answered correctly); the number of proactive actions they take to protect themselves, and how much cyber-risk they expose themselves to while surfing online.

Country Cyber-Knowledge Ranking

93%

say they worry about cyber security



When do people worry about cyber threats?

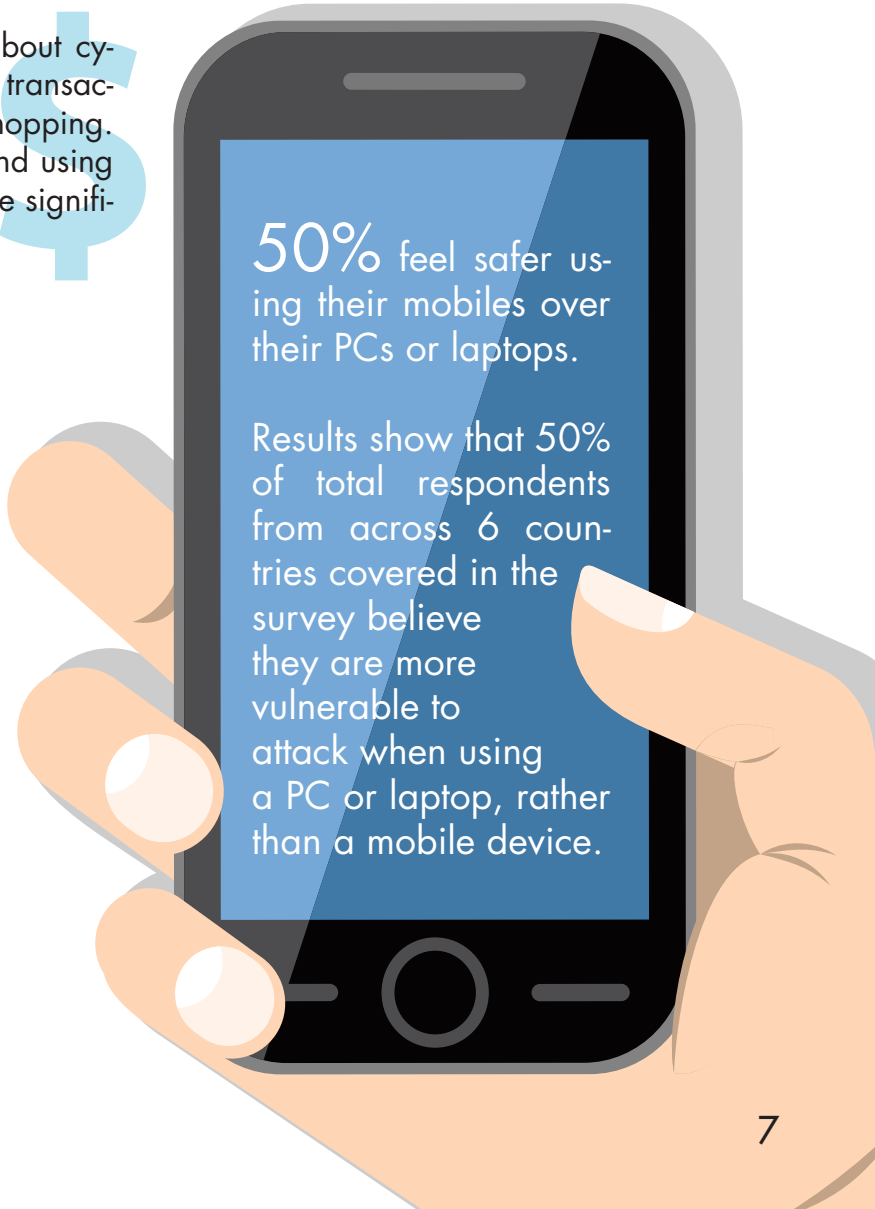
Overall, respondents were most worried about cyber threats for services that involve direct transactions, such Internet banking and online shopping. However, when it comes to social media and using apps on their mobile devices, concerns were significantly less.

Most worried nation: Malaysia

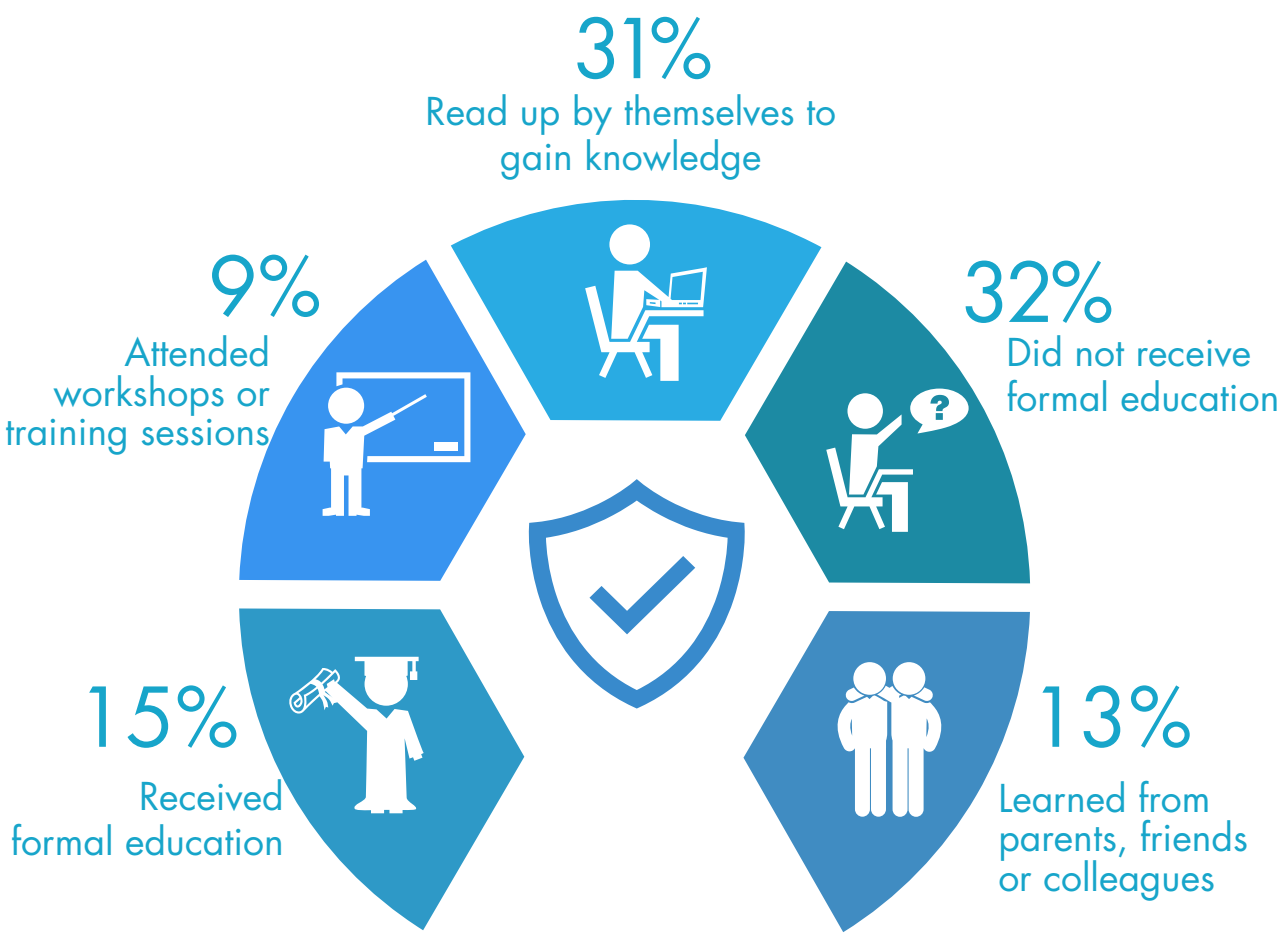
Malaysia was the country that worried the most about cyber security – with the highest scores for each worry category – which in each case was above the regional average – Internet banking (81%), online shopping (75%), paying bills and taxes (67%), and contracting cyber threats from free apps (54%).

Least worried nation: Indonesia

Indonesia was the least worried nation, when it came to cyber security, with low scores for each worry category. This is interesting, given they were also the lowest when it came to cyber-savviness.



Where did respondents learn about cyber security?



Thirst for knowledge

78.2% of respondents who did not receive formal education said they are interested to learn more about cyber security

More education required

According to the results, there is a lack of education on the topic of cyber security across the countries surveyed, with a third of respondents stating that they had not received formal education and had no knowledge on the subject.

Only 24% of respondents reported receiving education around cyber security, either at school or in the workplace, while the majority (44%) stated that they gained their knowledge by reading up on the subject on their own (31%) or finding out information from family, friends and colleagues (13%).

Knowledge vs Risk

People take risks despite knowing better

Results show that despite respondents knowing that certain actions could put them at risk or make them more vulnerable when online, it was not enough to stop them from doing it. While levels of education can be tackled, this trend is worrying, indicating that people will continue to take risks, despite knowing better. This was the highest for people using public wi-fi, despite knowing that it could be dangerous, not enabling two factor authentication technology to increase security or disconnecting from the internet in the case of a breach.

Public Wi-Fi Use

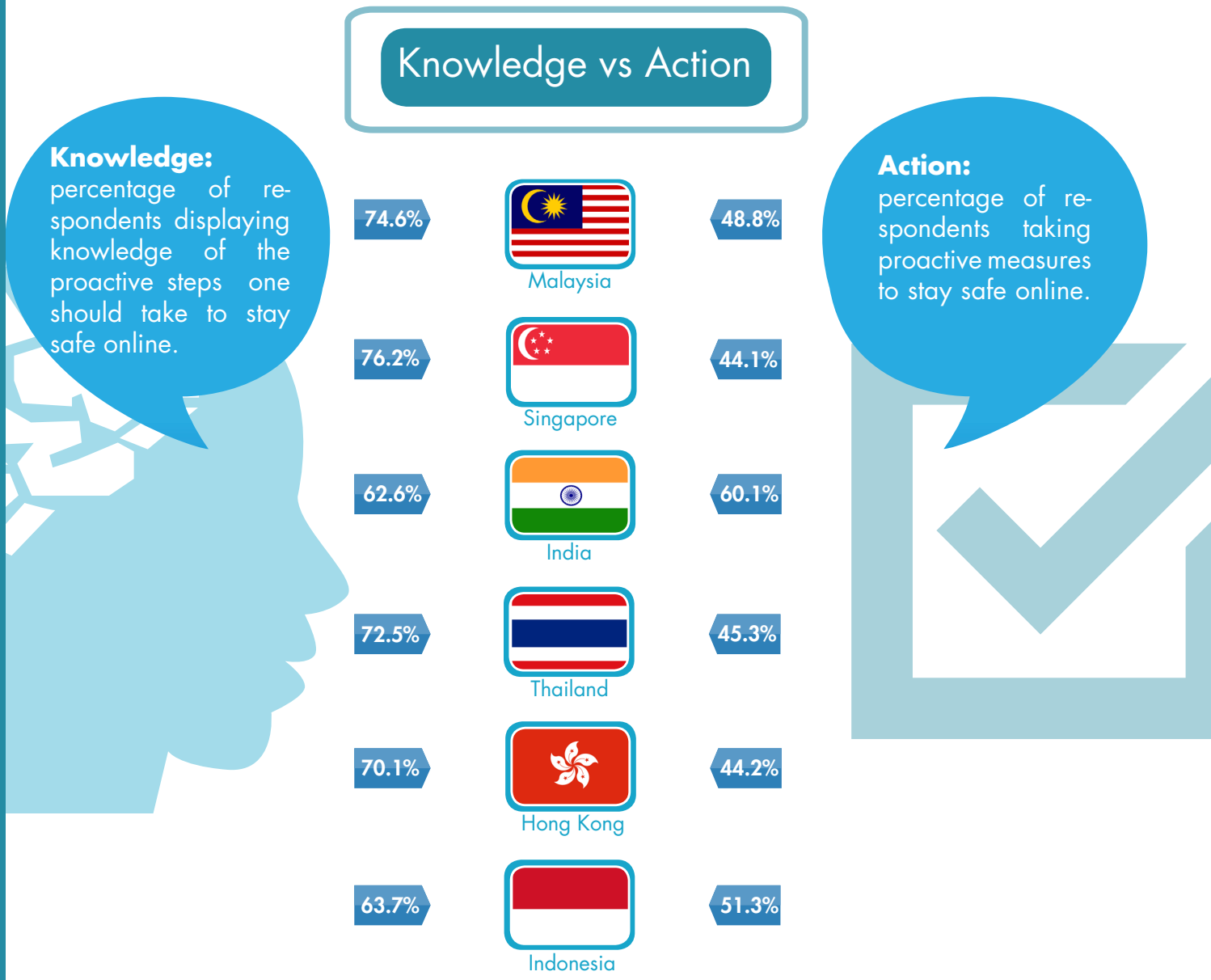
- ✓ 63% of respondents agree that it is dangerous to connect devices to unsecured public wi-fi networks.
- ✗ 59% of respondents still use public wi-fi networks when they are available.

Two Factor Authentication

- ✓ 83% believe two factor authentication should be enabled when available.
- ✗ Only 14% enable two factor authentication when available.

Reacting to a Breach

- ✓ 88% of users agree that a device which has been compromised should be disconnected from the Internet.
- ✗ Only 57% of users actually disconnect from the Internet in case of a security breach.



Most proactive nations: India and Indonesia

The survey found that users in India and Indonesia take the most proactive steps to secure their devices and online activities. Measures taken include changing their passwords regularly, backing up their data, and installing the latest versions of cyber security software.

This is particularly interesting, as these countries were the most likely to engage in online activities that might leave them vulnerable to attack.

Respondents were least likely to…

Back up their data regularly (37%), change their passwords regularly (33%) or download media (videos, music, apps) from official sources (49%), despite knowing that these actions would help them to stay safe online.

Gap between knowledge & action

It is important to note that countries such as Malaysia, Singapore and Thailand, which had the highest scores in overall cyber-savviness and knowledge, came in near the bottom when it came to taking the right steps to protect themselves. This gap between knowledge and action might, in some instances, be attributed to complacency and is a worrying trend. Hackers tend to look for the path of least resistance, and users might be leaving themselves vulnerable by not taking simple protective measures.

Conclusion

The results of the survey indicate that despite having some of the strongest adoption rates for connected technologies of anywhere else in the world, Internet users in countries across Asia-Pacific still have some way to go when it comes to protecting themselves against online threats.

As more innovative and disruptive technologies continue to make their way into the marketplace, it's important for individuals and enterprises to be able to embrace and enjoy all that these technologies have to offer. We know that there are a lot of cyber criminals out there, trying their best to exploit any vulnerability they can find to make a fast buck, however cyber space does not have to be a scary place. In fact, by following some easy steps, businesses and individuals can be confident that they are protected while surfing the web.

What do users need to know?

1.Use strong passwords

Strong passwords will mean the difference between whether your accounts are easy pickings for cybercriminals or not. Always try to have a unique password for each account and avoid using keywords which may be easily guessed, for instance your date of birth or surname.

Do: Use a combination of letters and numbers, using lowercase and uppercase letters.
Do: Change your password every 3-6 months.
Don't: Write them down or share the information with anyone.

2.Make best use of security settings

It's always useful to remember that the software and applications you use on a daily basis have security settings that can provide additional security while you are active online.

Do: Enable 2FA wherever possible to strengthen security around your financial transactions.
Do: Update browser settings to increase security while online, including clicking to allow trusted websites online and ensure the pop-up blocker is enabled.
Do: Limit the amount of personal information and images that are available via social media to people outside of your friend group.

3.Use cyber security software

It's crucial to ensure you have a security solution in place to keep you protected from viruses, malware, spyware and other potential attacks while browsing online.

Do: Make sure all firewalls are switched on and other features are activated.
Do: Make sure the software you are using is reputable.
Do: Update the software regularly.

4.Secure your mobile devices

Always keep in mind that your smartphone and other mobile devices are just as vulnerable to attack as a PC or a laptop (they are small computers afterall), so steps need to be taken in order to make sure you stay protected.

Do: Download applications only from trusted sources (official app stores).
Do: Make sure your device is password protected and if lost or stolen, data is wiped remotely to avoid it ending up in the wrong hands. Similarly, if your work device is lost or stolen, this should be reported to your workplace IT department immediately to minimise risk to the company network.
Don't: Store sensitive or critical data on your mobile device.

5.Keep your system up-to-date

Make sure you keep your system secure by carrying out regular updates.

Do: Keep your applications and operating system current with the latest system updates.
Do: Turn on automatic updates to prevent potential attacks on older software.
Do: Perform regular back-ups of all important data and store it securely.

6.Avoid scammers at all costs

The online world is full of scammers waiting on unsuspecting users to fall for their tricks and schemes. Don't be one of them!

Do: Be careful when answering emails. Always check the source of the message and verify the source.
Do: Make sure that websites are secure especially when making online purchases. Make sure the URL address is authentic and that you have not been redirected to another website.
Don't: Respond to emails requesting personal information, ID or financial information – even if it comes from a reputable source, i.e. your bank. Please note that your bank would never ask for this kind of information via email, so it's likely to be a phishing scam.
Don't: Click on banner ads – even if they seem to be from a legitimate website, as they may be hiding malicious code that could harm your computer.

7.What to do if your computer has been compromised

If you think your computer may have been hacked or has been infected by a virus, there are a number of things you should do to limit potential damages and restore your security perimeters to ensure your online safety.

Do: Disconnect from the network / the internet immediately.
Do: Run a virus scan and check for infection.
Do: Reset your passwords and do a full security audit on any accounts you think may have been compromised – including calling up your bank to refresh security arrangements.
Do: Ensure your wireless router is secure.
Do: Update your system to ensure no settings have been changed.
Do: Check online (via a different device) to see whether there are any other reported cases, and whether there are patches or other solutions available to solve the problem.
Do: Seek help from an IT professional if you are unsure how to solve the issue.

About ESET

ESET® is the pioneer of proactive protection and the maker of the award-winning ESET NOD32® technology, is a global provider of security solutions for businesses and consumers. For over 26 years, the Company continues to lead the industry in proactive threat detection. By obtaining the 80th VB100 award in June 2013, ESET NOD32 technology holds the record number of Virus Bulletin "VB100" Awards, and has never missed a single "In-the-Wild" worm or virus since the inception of testing in 1998. In addition, ESET NOD32 technology holds the longest consecutive string of the VB100 awards of any AV vendor. ESET has also received a number of accolades from AV-Comparatives, AV-TEST and other testing organisations and reviews. ESET NOD32® Antivirus, ESET Smart Security®, ESET Cyber Security® (solution for Mac), ESET® Mobile Security and IT Security for Business are trusted by millions of global users and are among the most recommended security solutions in the world.