KASPERSKY lab

Not logging on, but living on

Consumer Security Risks Survey 2017

Introduction

This year we have reached the stage where 50% of the world's population is connected to the Internet, compared to 40% in 2016. And, with more people online than ever before, every minute that goes by witnesses 3.5 million Google search queries, $751,522 spent, 156 million emails sent, 342,000 apps downloaded in mobile app stores and 46,200 posts uploaded to Instagram.

There's no doubt that our Internet habits are constantly evolving. And, unfortunately, attackers are carefully monitoring any trends in how we live our digital lives to devise new ways to profit from their crimes and our vulnerabilities.

With this in mind it's important for us to evaluate the changing Internet landscape ourselves, so that we can stay one step ahead of the cybercriminals and continue to develop security solutions that support our customers.

Kaspersky Lab, with help of B2B International, therefore regularly conducts global statistical studies, identifying areas where Kaspersky Lab can help support people as they spend an increasing amount of their time online. This is an important part of our mission to help Internet users protect what matters most to them.

Main findings

People don't log onto the Internet anymore, they are simply online all the time

- Outside of work, the vast majority (**86%**) are online several times a day and one in ten (**11%**) is online for over 50 hours a week
- To spend so much time online, people use multiple devices simultaneously – with the use of mobiles rising to **75%** this year and wearables rising to **31%**
- But being mobile and online brings its own Internet safety problems and Internet users don't protect their different devices in the same way – **89%** protect their computers with a security solution but only **56%** protect their smartphone

Our favourite thing about the Internet, is the way it connects us to the world

- Emailing from personal accounts is still the most popular thing to do online (**96%** said they email from any device). Also popular is watching videos (**88%**), reading news or visiting current affairs websites (**86%**) and using social media – all helpful ways, for example, of staying in touch with friends and seeing what's happening in the world (**85%**)
- But many of us (**53%**) use public Wi-Fi in the process, risking the interception or theft of data and only **44%** do this with some precautions

We rely on mobile devices to store the data we love, but precious data is being left vulnerable, and often cannot be recovered if lost

- Photos and videos of travel are rated as the most important data on people's mobile devices (**18%**)
- However, if data from a device was lost – for example if a user's device was misplaced, stolen, damaged or hacked, **21%** would never be able to recover their precious files
- When data can be recovered, the average cost of replacing it is **$636**
- This is partly because just **50%** back up their information

There are significant concerns about our cyber-happiness

- Safety concerns and security incidents affect people's happiness online. One in four (**27%**) have been affected by an online security incident of some kind in the last year
- In addition, the majority (**62%**) are concerned about someone else intercepting their data through their Internet connection
- And people are also concerned about their vulnerable family members – with **65%** of parents worried for the safety of their children using the Internet and **60%** overall being concerned about their older relatives using the Internet

But people – despite their concerns – don't know how to protect themselves

- Despite over half (**55%**) believing that the number of threats to their online security are increasing significantly, an astounding **38%** don't know how to protect themselves from cybercrime
- Furthermore, one in five (**21%**) don't believe security software is essential, seeing it as a gimmick instead

Methodology

The study was conducted online by B2B International in August, 2017. Users from 32 countries were surveyed online.

A total of 21,081 people, split equally between men and women, were surveyed.

Data was weighted to be globally representative and consistent. The global data in this report excludes findings from China.

Not all of the survey results have been included in this report. To find out more please contact Kaspersky Lab.

Section one: online mobility

The Internet has become a vital part of our lives. We don't log on to it anymore. Instead, we're constantly on. Switched on, and connected. Demonstrating this, our study found that **86%** of people are online several times a day at home, not including the time they spend online at work. Furthermore, **two-thirds** use the Internet at home for more than ten hours a week, and one in ten (**11%**) is online for over 50 hours a week.

People access the Internet on an array of devices – from desktop PCs to tablets and smartphones. This year we've noticed a decrease in the use of computers to go online, dropping from **91%** in 2016 to **86%** in 2017. Nevertheless, by far the most popular device with which to access the Internet is still a Windows PC (**81%**).

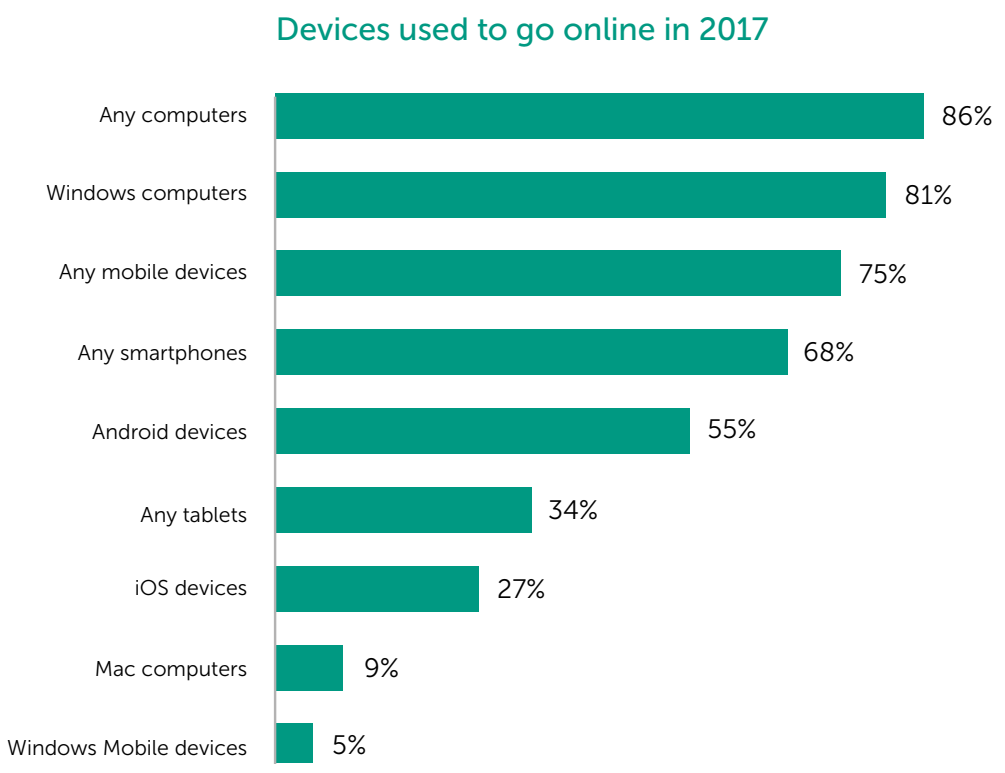
Connected dexterity has been an important feature of 2017, with people using multiple devices and platforms that access the Internet simultaneously. Over half (**60%**), for example, use a PC or a Mac alongside a mobile device and **31%** has some kind of connected device in their household such as doors, climate control, medical equipment etc. that uses the Internet to operate.

The use of mobiles has continued to increase – with **75%** of people using these devices to access the Internet in 2017, up from **67%** in 2017. Furthermore, **41%** prefers to use their mobiles when they are at home, an environment where they may have access to alternative connected devices such as a desktop which might have a larger screen or greater storage capabilities.

Other moving technologies are also being used for accessing the Internet. Wearables, for example, are gaining popularity with **31%** owning some kind of wearable device (compared to **24%** last year). And, of those who have their own car, **14%** of these cars are connected to the Internet.

Although they use and own multiple devices that access the Internet, people don't worry about protecting every device in the same way. Only **89%** protect the computers they use to go online with Internet security software and only **56%** protect their smartphones. Less than half (**48%**) have a password or other form of lock on their mobile devices and only **22%** use anti-theft, leaving the mobiles and data on them accessible to anyone. This is concerning, given that mobiles are gaining in popularity and as many as **6%** has had their device lost or stolen, in the last 12 months.

Being mobile and online brings its own Internet safety problems. Our 2017 data shows that Internet users this year have become more concerned about sharing information about their location when using their smartphones, or indeed other connected devices (**61%** compared with **39%** previously). However, there is still a lack of awareness among users around how smartphones actually access location data, with just **53%** checking permissions on their mobile devices, although many apps are able to access location data while they work in the background – without the knowledge of owner.



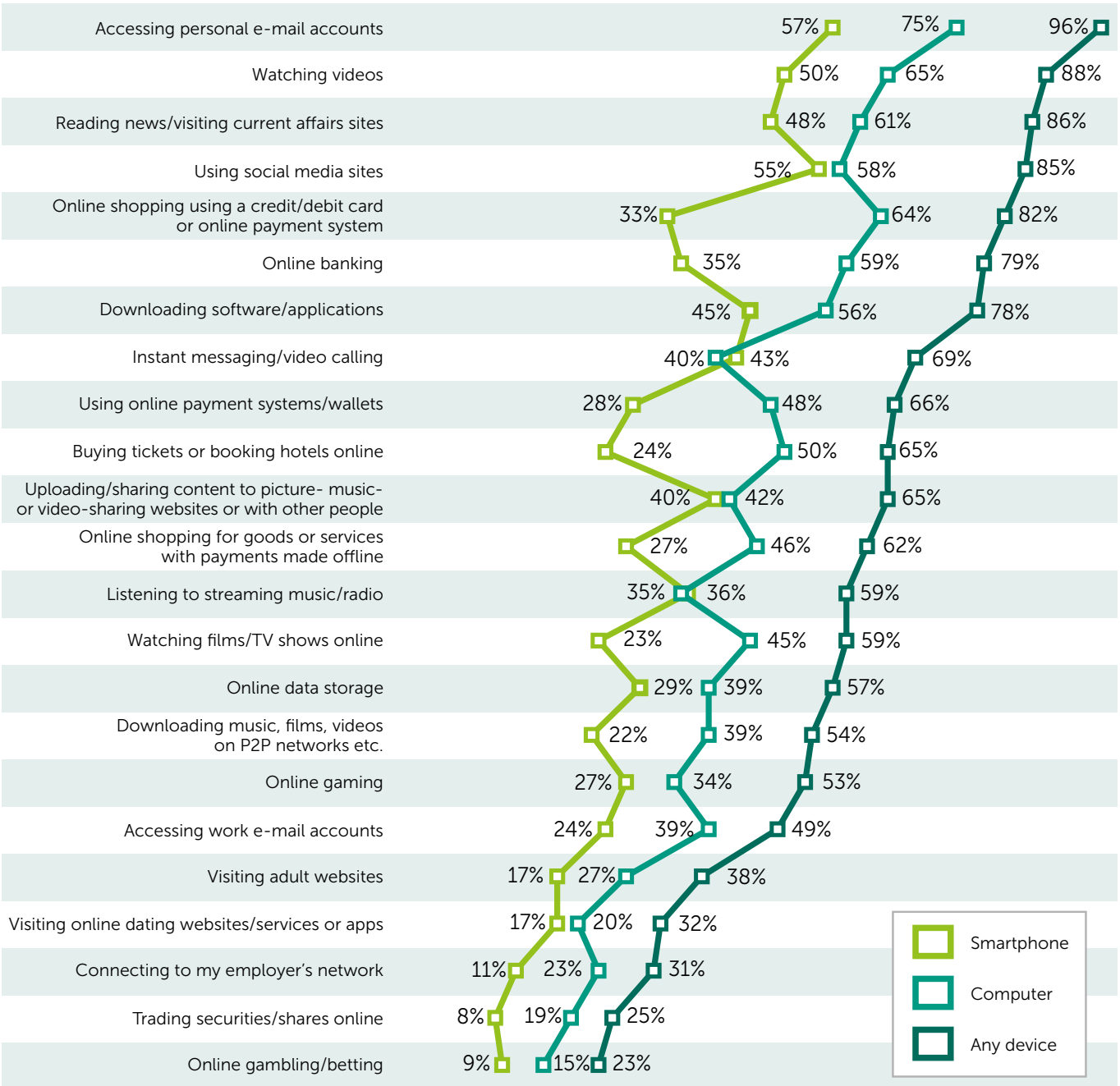
Section two: online and active

People get up to a lot online – from shopping for daily essentials to entertaining themselves in their spare time – and they do this on multiple devices. For transactional activities such as shopping and banking, they tend to use their desktops, but are more likely to turn to their smartphones for entertainment.

For example, **64%** of people use their desktop/ laptop PC to shop online making online payments and a third that number (**33%**) shop this way on their smartphones. Similar numbers bank online, with their desktops and smartphones respectively. However, the pattern is different around gaming, with a third using both their computer (**34%**) and their smartphone (**27%**).

The study shows that overall, our favourite online activities allow us to connect with the world around us. Emailing from personal email accounts is still the most popular thing to do online (**96%**), followed by watching videos (**88%**), reading news or visiting current affairs websites (**86%**) and using social media (**85%**).

Internet users' most popular online activities



Online gaming remains popular among Internet users, with **53%** agreeing that they game online. This activity is most popular among younger users (**67%**) compared with older users (**25%**).

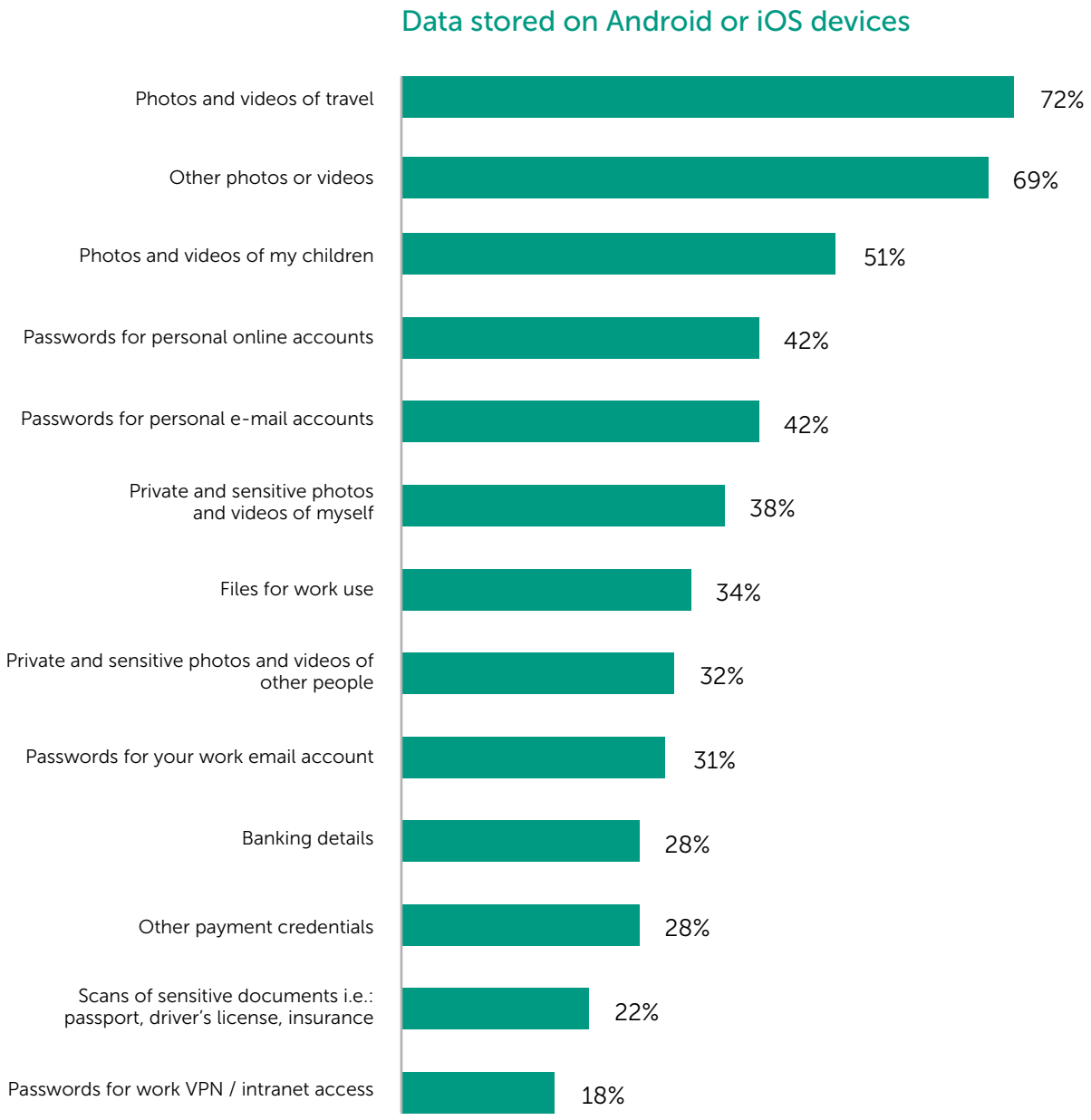
Online activities don't just change according to device type, the study also shows us patterns in how people access the Internet – with many using potentially insecure public Wi-Fi services to conduct a wide variety of their online activities.

53% use public Wi-Fi, with **88%** of these conducting risky activities in the process, putting their data in danger of interception or theft. For example, **64%** access social media via public Wi-Fi, **23%** log into their gaming accounts this way, **38%** log into websites/ accounts without additional precautions and one in four (**26%**) even conduct online transactions (such as banking, shopping or payments).

Only a quarter (**26%**) said they always behave more securely when they are using new and potentially insecure Wi-Fi – for example in a hotel or public place – to access the Internet while **56%** do nothing to protect themselves from public Wi-Fi at all.

Section three: a treasure trove of memories

Perhaps it's no surprise that the people that own Android or iOS devices such as smartphones, tablets etc, are relying on these to store a wide range of data – some of which is particularly sensitive, such as work files, passwords, and videos or photos of their children, which users wouldn't want to fall into the wrong hands.



There was an awareness among our survey respondents that the data they store on their devices is important to them. Photos and videos of travel (**18%**), address books/ phone contacts (**18%**), personal files (**17%**), and personal email messages (**16%**) were rated the most important data stored on people's devices.

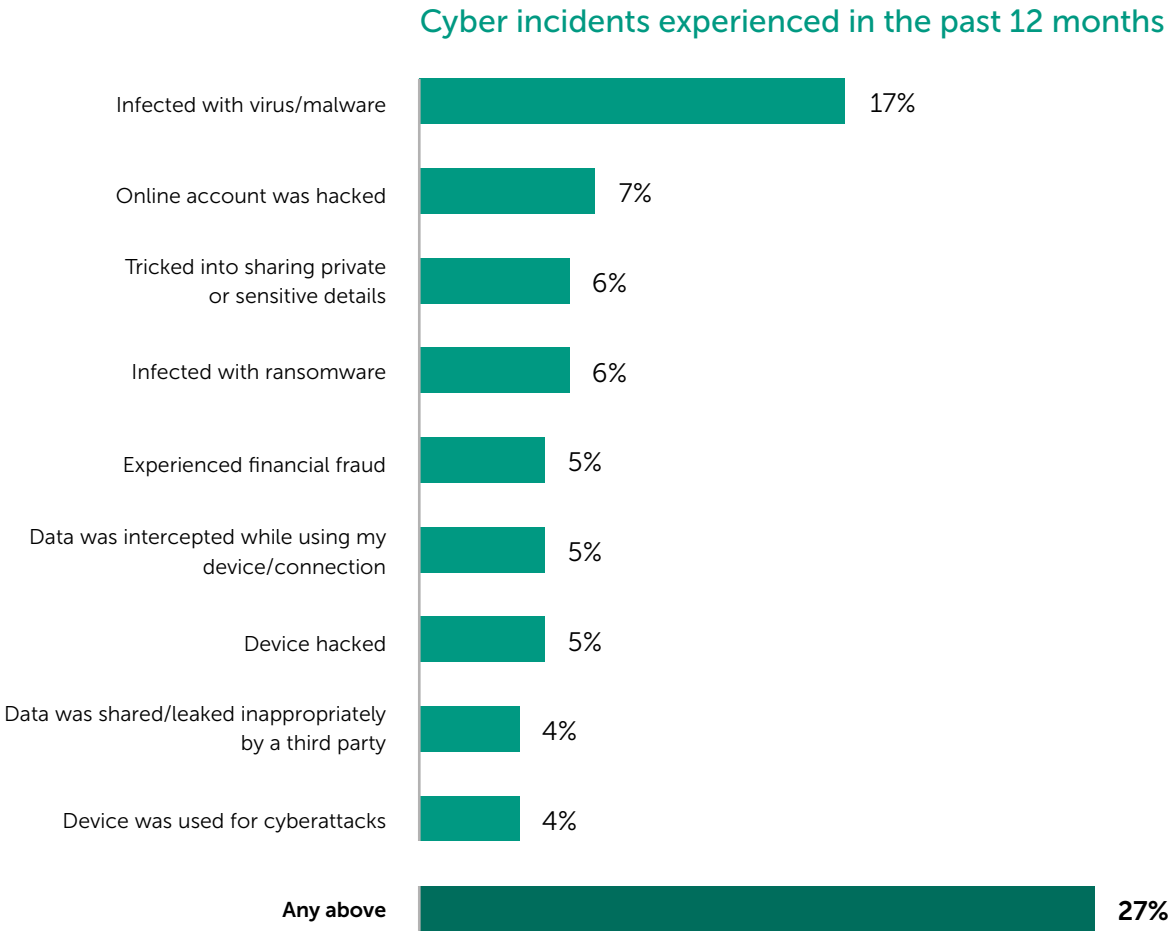
Yet, despite the data on their devices being important, we also found that many are not putting precautions in place to protect that data, with too few (just **50%**) backing up the information on their devices.

Not putting precautions in place leaves precious data vulnerable to being lost forever – for example, despite photos and videos of travel being rated as the most important data stored on their mobile devices, if these files were lost, **28%** would never be able to recover them. Furthermore, it's expensive when it all goes wrong – the average cost of replacing data, should people lose access to their devices, is **$636**. There is clearly more work for us to do, if we are to help people avoid these problems.

Section four: threats to our cyber-happiness

It's evident that digital devices have been thoroughly engrained into our lives. But they are not without their problems and, as we rely on these devices more and more to access the Internet, connect with the outside world, and store data that is important to us, security incidents that put these devices under threat can have a devastating impact. Threats to our cyber-happiness are by no means insignificant, with one in four (**27%**) been affected by an online security incident of some kind in the last year.

Threats are wide-ranging and harmful, and this section of the report highlights the impact of some of the most prevalent cyberthreats.



Malware

2017 was a year characterised by high profile cyber-attacks and malware developments, with **37%** of Internet users having either experienced, or been targeted by, a virus or malware this year. When they've been a victim, **36%** have incurred financial penalties and this was **$118** in average, making this cyberthreat a painful one to be targeted by.

Ransomware

This year has also seen several worrying ransomware threats, with some (such as WannaCry) hitting the headlines and crippling businesses around the globe, making consumers much more aware of the threat generally. We found that one in six (**16%**) have either experienced or been targeted by ransomware. Plus, when they have been a victim, only **30%** have managed to restore all of their encrypted or blocked files, one in three (**34%**) have ended up paying a ransom to criminals to get their files released – and this isn't cheap, on average, a ransom costs victims **$271**.

Hacking accounts

Around one in six people (17%) has either experienced or been targeted by account hacking in the last year. Of those who have had their accounts hacked, 41% has had their email account targeted, 37% has had their social media account hacked, 18% has had their banking accounts targeted, and 16% has had their gaming account hacked. Account hacking can earn criminals money on the black market – for example, hacked gaming accounts can fetch $1 each, so it's a potentially lucrative area for criminals that can hack and sell on mass.

Data leaks

With consumers entrusting so much information to third parties – for example financial data such as card payment details, passwords, and personal information such as addresses, birthdays and more, data leaks are a threat – and unfortunate reality – of today's cyber landscape. Where data has been leaked inappropriately, in one in three cases (30%) people's banks have been responsible, 29% has had data leaked by their social media company, and a quarter has had data leaked by their email account provider (25%).

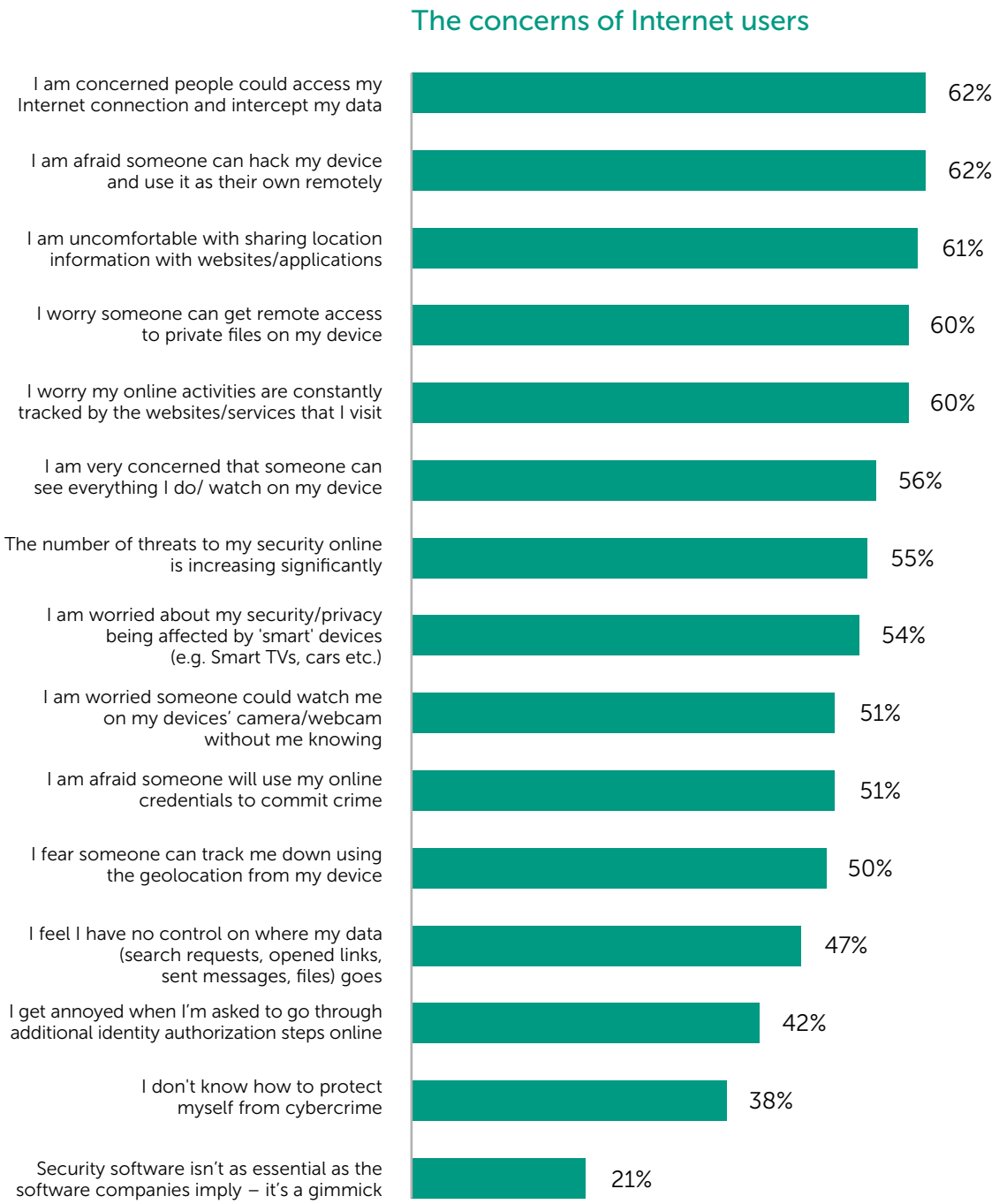
Fraud

Financial fraud or scams are another unfortunate reality of today's cyber landscape, with over one in ten (12%) either being targeted by, or experiencing financial fraud in the last 12 months. Moreover, when they have been a target of fraud or an online scam, the average losses have been calculated at $430, with 27% losing more than $1000.

Section five: attitudes towards cybersecurity

Despite the high costs involved in data recovery if it all goes wrong, and number of people that have fallen victim to cybercrime in the last 12 months, a surprisingly low one in five (**21%**) believes they could be a target for cybercrime. Internet users do have some very real concerns about their online security, but in many instances these concerns do not amount to them feeling personally targeted.

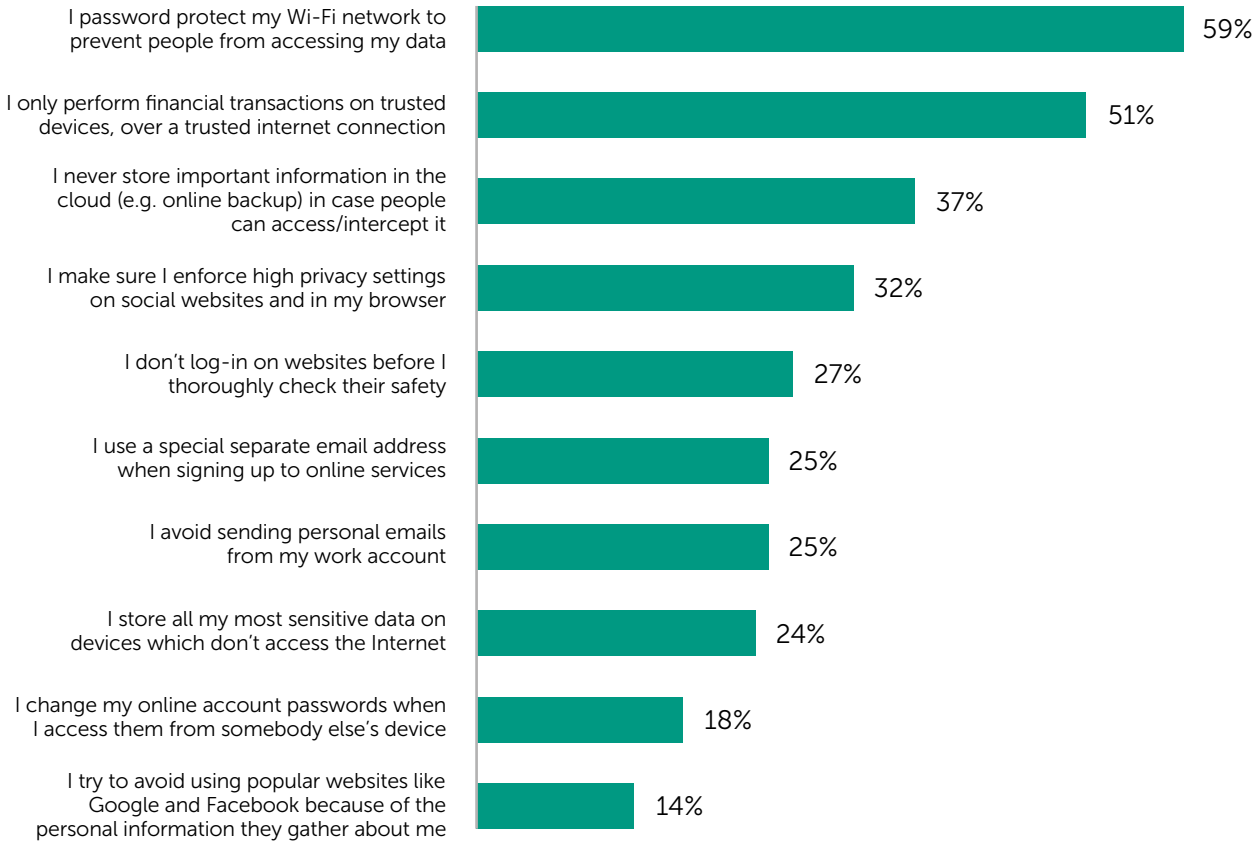
Internet users are most concerned that someone else could intercept their data by gaining access to their Internet connection (**62%**). This is swiftly followed by the fear of someone hacking a device and using it as their own remotely.



Despite over half (**55%**) believing that the number of threats to their online security are increasing significantly, an astounding **38%** don't know how to protect themselves from cybercrime, and one in five (**21%**) don't believe security software is essential, seeing it as a gimmick instead.

Only around half actually put any methods in place to help protect themselves from cybercrime and these range from using passwords to prevent other people from accessing their Wi-Fi networks (**59%**) to going to the extremes of avoiding popular websites such as Facebook and Google, because they are worried about these organisations collecting data about them (**14%**).

How Internet users protect themselves



There is an acceptance among Internet users about the importance of using passwords to protect themselves from cybercrime – **52%** said that if a cybercriminal managed to get access to the personal information on their devices, they would be most concerned about their account passwords falling into the wrong hands. These, after all, are the key to unlocking private data.

But Internet users, on the whole, do not treat their passwords appropriately. Only just over half (**62%**) would be able to quickly restore their personal online account passwords if they lost their devices, despite respondents to our survey generally accepting that passwords are more valuable than ever before – because they protect finances, online payments, shopping and more.

31% have just a few passwords that they choose from when creating new accounts, **13%** use a template or regular pattern that they modify to create new passwords and **10%** stick to just one password that, once hacked, could unlock everything.

Furthermore, many have done something risky with their passwords, such as sharing their passwords (with a family member (**29%**), friend (**11%**) or colleague (**5%**), and **51%** store their passwords insecurely by, for example, writing them down in a notepad or in a public place.

Section six: family matters

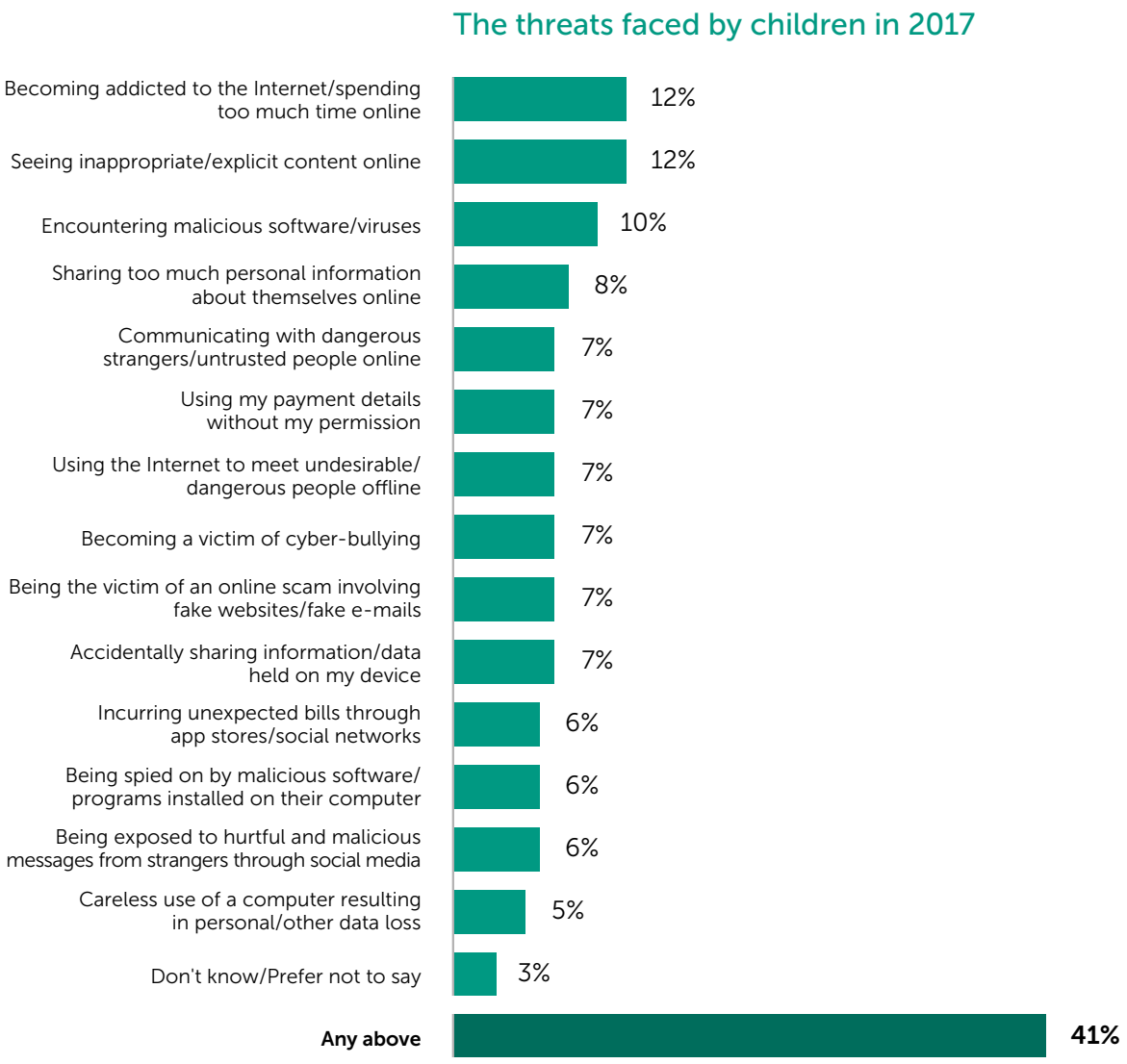
People's Internet concerns are not just limited to worries about their own safety online, they also worry about the safety of their loved ones – in particular older relatives and children who may be vulnerable to cybercrime because they are less aware of the dangers and thus more exposed.

Children

To find out more about these concerns, our study questioned parents with kids under the age of 18. **65%** of these parents agreed that their kids use the Internet and that they are concerned about their safety. Furthermore, over half of parents are concerned that their children have uncontrolled access to inappropriate content online (**57%**), that using the Internet can negatively affect their health (**53%**), and that online threats to their kids are increasing (**51%**).

Parents are most concerned about their children seeing inappropriate or explicit content online (**36%**), becoming addicted to the Internet (**33%**), or communicating with strangers (**32%**) who might be dangerous. **32%** of parents are also concerned that their kids may become the victims of cyberbullying.

The sad reality is that young people do come across harm online. Almost half (**41%**) have recently faced at least one form of online threat. One in ten parents said their children have become addicted to the Internet (**12%**) and the same number have seen inappropriate/ explicit content online (**12%**), shared too much information about themselves (**8%**) or encountered malicious software/ viruses (**10%**). Of course, these stats only include what parents know about their children's experiences online and the true figures may in fact be higher than these.

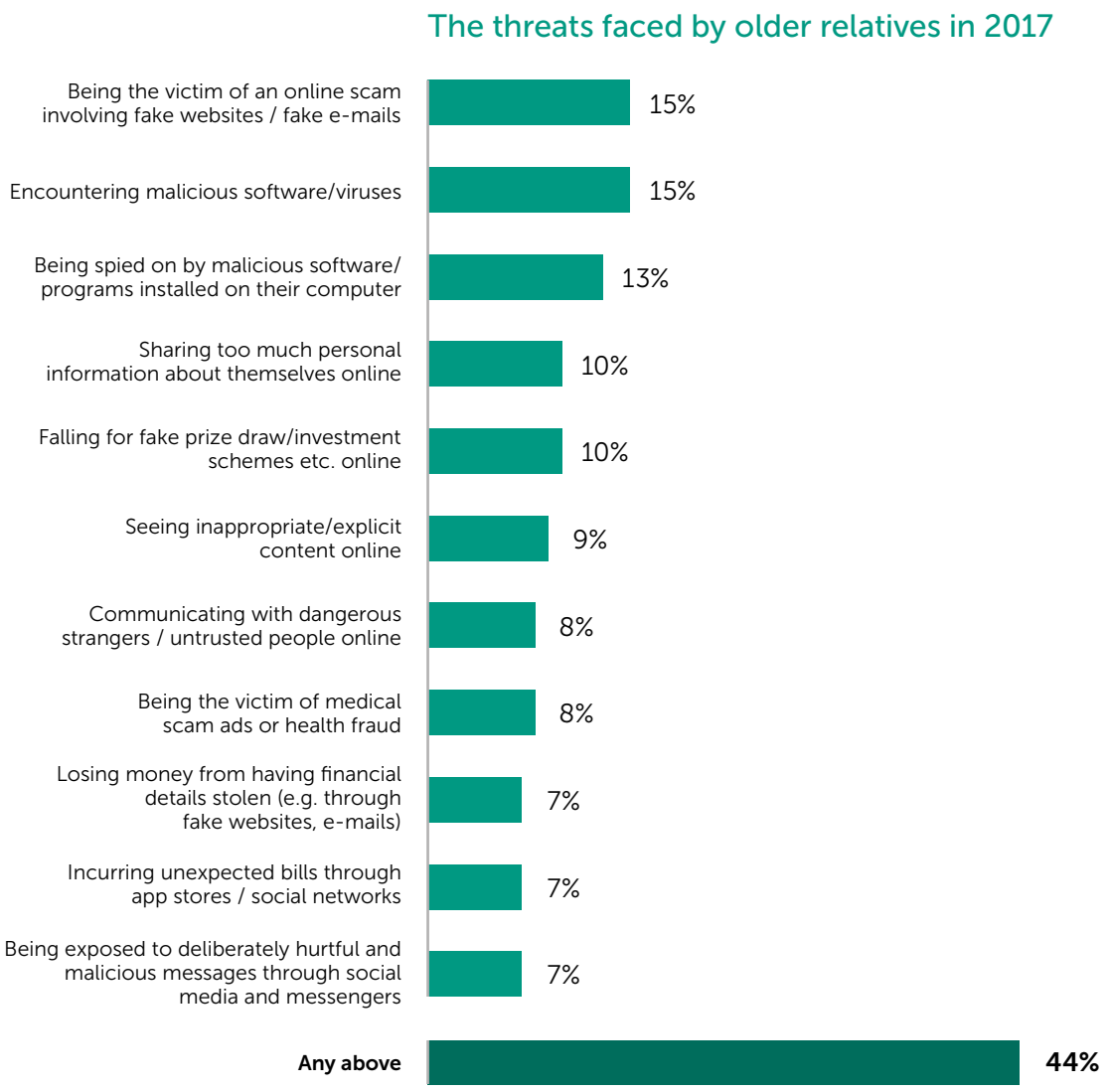


Our study shows us that parents employ a variety of methods to try and help keep their kids safe online, the most popular of which are talking to their children about online threats, to help educate them (**37%**), and limiting their time online (**33%**). Interestingly, **48%** of parents in APAC, who are perhaps more strict than parents elsewhere, said they limit the amount of time their children spend online, compared to **30%** of parents in Europe.

Older relatives

It's not just children's online safety that people are concerned about. Older relatives are also vulnerable, with **84%** of older generations now also using the Internet at home several times a day. Making them vulnerable to cyberthreats too.

60% are concerned about their older relatives – including parents and grandparents – using the Internet. The biggest concerns are around them being spied on via malicious malware on their device (**43%**), encountering malicious software (**42%**) or becoming the victim of a scam involving fake emails or websites (**55%**). These concerns do unfortunately sometimes become a reality, with **44%** of Internet users admitting that their older relatives have experienced an IT security threat or incident. These threats have often resulted from online scams involving fake emails and websites (**15%**), or malware infection (**15%**).



Despite concerns, people do little to help protect their older relatives from their growing vulnerability, with only **34%** agreeing they have installed an antivirus solution onto their older relatives' devices and a quarter (**33%**) admitting they do not protect their older relatives at all.

Conclusion

People are not logging on anymore because they are living online, always connected. Digital habits are constantly evolving, and with Internet users embracing a variety of different digital devices to stay connected – from mobiles to cars, and from desktop computers to wearables – there is an ever-growing number of vulnerabilities for cybercriminals to exploit. Indeed, cybercriminals are, unfortunately, all too aware that people are still failing to protect themselves effectively, giving criminals multiple opportunities to target the young, the old, the unprotected, and the unaware.

The results of this consumer study have shed further light on the findings of another major study into people's online protection. Updated earlier this year, the Kaspersky Cybersecurity Index is based on slightly different data to this current report, but it nonetheless revealed that in 2017 **78%** of Internet users don't believe they are targeted by cybercriminals, **41%** do not have every device protected, but a worrying **27%** have been affected by a cyberthreat.

This study has put yet more perspective on these Kaspersky Cybersecurity Index figures, by looking in more detail at the gaps in people's protection. We have found that many do not fully understand how to protect themselves against cybercrime, some may have bad password habits which might trip them up, and others may be making simple mistakes, all of which can have dangerous ramifications in this ever-evolving landscape.

Kaspersky Lab is committed to helping Internet users overcome their concerns about the online world and protect their data and devices effectively; empowering them to make informed decisions about what they do online, how they do it, and how to protect what matters most to them – including their loved ones and their data – in the process.
To find out more about our approach to online security, and find a security solution to suit your needs, click here.