CONSUMER SECURITY RISKS SURVEY

FROM SCARED TO AWARE: DIGITAL LIVES IN 2015

KASPERSKY lab

Contents

Introduction

In 2015, just under half (43%) the world's population has an Internet connection: 3.2 billion people, compared to 2.9 billion in July 2014.

The Internet brings communications, shopping, entertainment, news, education, work and more to anyone, anytime, anywhere and on any device. But our threat research shows that these same channels can be, and increasingly are also used by criminals, malicious attackers, terrorists and even bullies. Some are simply out to hurt, disrupt or destabilize; others are after money or identities; and a few of the most dangerous have set their sights on political or business intelligence or even critical national infrastructure such as electricity networks. In one way or another, everyone is at risk.

And all those people and groups with malicious intent keep a close eye on evolving digital technology. Every new development, every new device and every new operating system is explored for vulnerabilities. They also exploit human behaviour, such as a lack of digital literacy and an innate tendency to trust.

In order to better understand how Internet users across the world perceive, prepare for and are impacted by current online threats, Kaspersky Lab, together with research company B2B International, undertakes a comprehensive annual global research study. The study explores device ownership and Internet use, as well as awareness and experience of current cyberthreats.

Analysis of the study findings and the ability to track some of them across recent years enables Kaspersky Lab to monitor improvements and setbacks and to identify areas where it can provide support, so that people across the world feel more empowered to protect what matters most to them.

See this link for the report from the previous study.

Main findings

Consumers use different devices on different platforms to go online

- Two-thirds (67%) of the Internet users surveyed use several devices to go online, including smartphones, tablets, laptops and desktops; and 23% mainly uses a mobile device to access the Internet at home

Users go online at home, while travelling, at work, in cafes, shops and elsewhere

- 13% of consumers use public Wi-Fi to log onto websites and accounts, and 8% uses them to shop or bank online

Users store important information on devices

- 88% stores private or personal information on digital devices; 48% stores passwords or account login details and 28% stores financial data – the estimated median value of replacing all digital assets stored on devices is $682

However, they often fail to protect their personal privacy and identity

- Just 36% has implemented strong privacy settings – and 13% doesn't take any precautions at all
- 42% has shared online their contact details or a picture of themselves (45%), and 30% has revealed their date of birth or address; up to a fifth has shared explicit content

Digital devices are being lost, damaged or stolen – particularly among the young

- One in seven (14%) respondents has lost a device or had it stolen, and 12% has damaged a device. 15% of the data lost was never recovered

Users are concerned about the threats facing older people and children

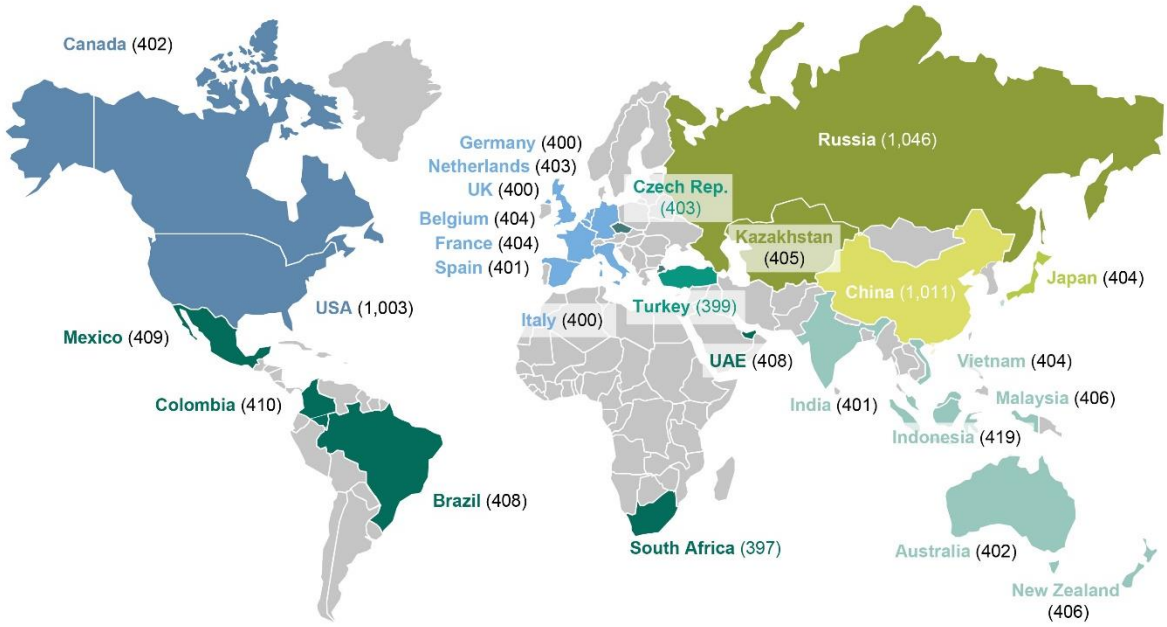
- Adults worry that older relatives may not know how to protect themselves from malware (52%), online scams (50%), theft (45%) or dangerous strangers (23%)
- Half of parents believe that online threats to their children are increasing – but 20% takes no specific action to keep them safe

Users and their acquaintances encountered many cyberthreats online in the last 12 months

- 45% has encountered malware and 44% say they know of others who have been affected
- 25% has experienced account hacking, and 32% say they know of others who have been affected
- 48% has experienced a financial threat, and 42% know of friends, colleagues or family members who have been affected

Methodology

The study was conducted online by B2B International in June 2015. Users from 26 countries were surveyed online, up from 23 in 2014.



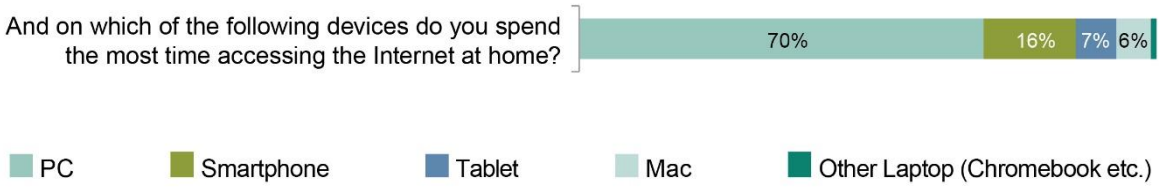
A total of 12,355 people aged 16 and over were surveyed (11,344 excluding China), equally split between men and women. One in three (29%) was aged under 24, 26% was aged between 25 and 34, 19% was aged 35 to 44, 14% was aged 45 to 54, and 12% was aged 55 and over. Just under half (42%) of those surveyed had children aged 16 or younger in the household.

The data was weighted to be globally representative and consistent. Data from China has been removed from some of the global results due to its high overall weighting and marked difference in attitude and behaviour compared to most of the other geographies surveyed.

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

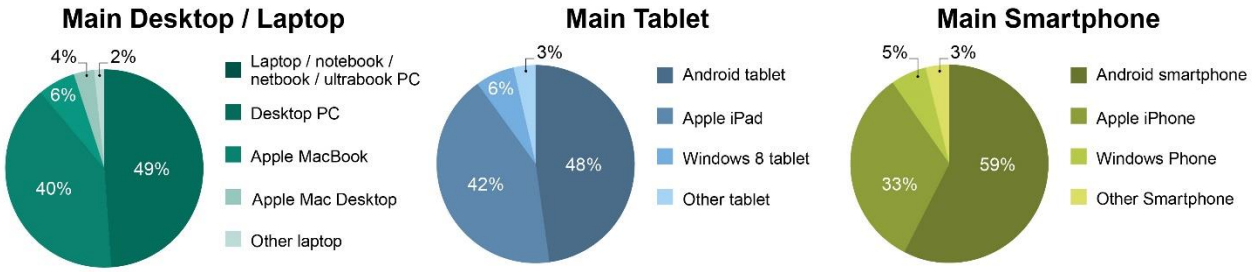
Section 1. Device usage

Two-thirds (67%) of the Internet users surveyed use several devices to go online. Although for 70% the PC continues to dominate Internet access at home, for 23% online access is mainly through a mobile device.



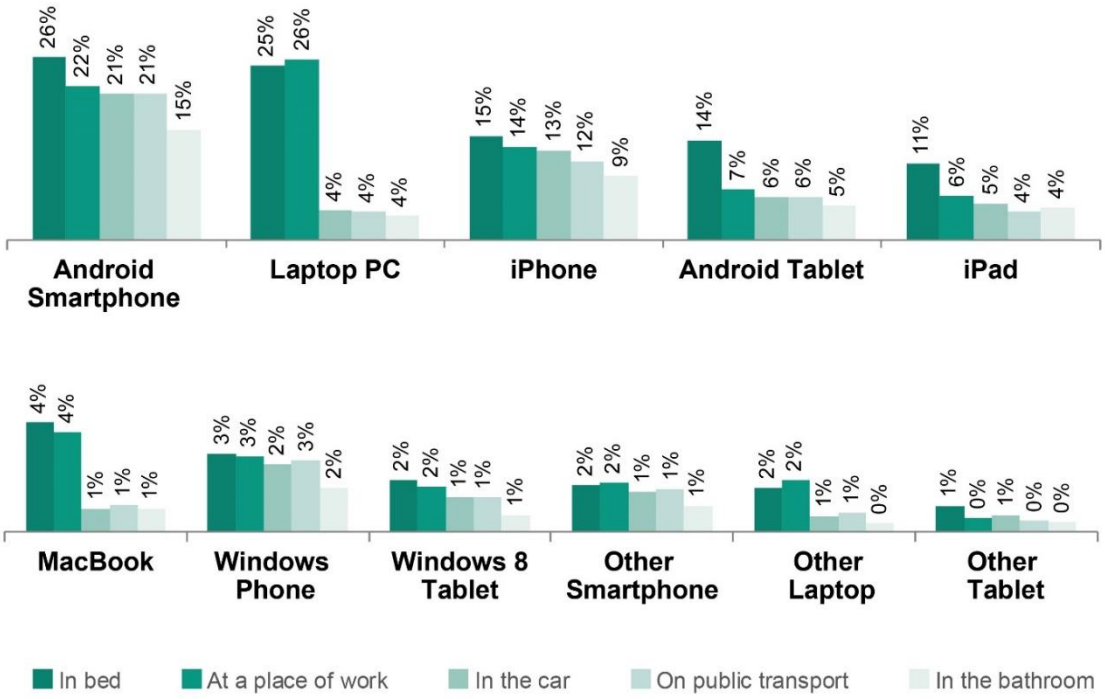
However, traditional devices and operating systems retain a dominant presence, even among multi-device users. PCs make up 89% of desktops and laptops used, while Apple computers make up just 10%.

When it comes to tablets, the field is more even with Apple iPads accounting for 42% and Android-based tablets for 48% of the tablets used globally. Six in ten (59%) smartphones used to access the Internet are Android devices, while a third (33%) is iPhones.



The growing use of mobile and portable Internet-enabled devices, as well as the spread of next-generation networks, makes it ever easier for consumers to go online anytime and anywhere; and they are embracing the opportunity to do so. A quarter (26%) spends over four hours a day online – rising to 30% of 16-24 year olds – and one in six (15%) manages six hours. The median time spent online is 18 hours a week:

This Internet activity is taking place in bed, at work, while travelling on public transport, in the car and even in the bathroom.



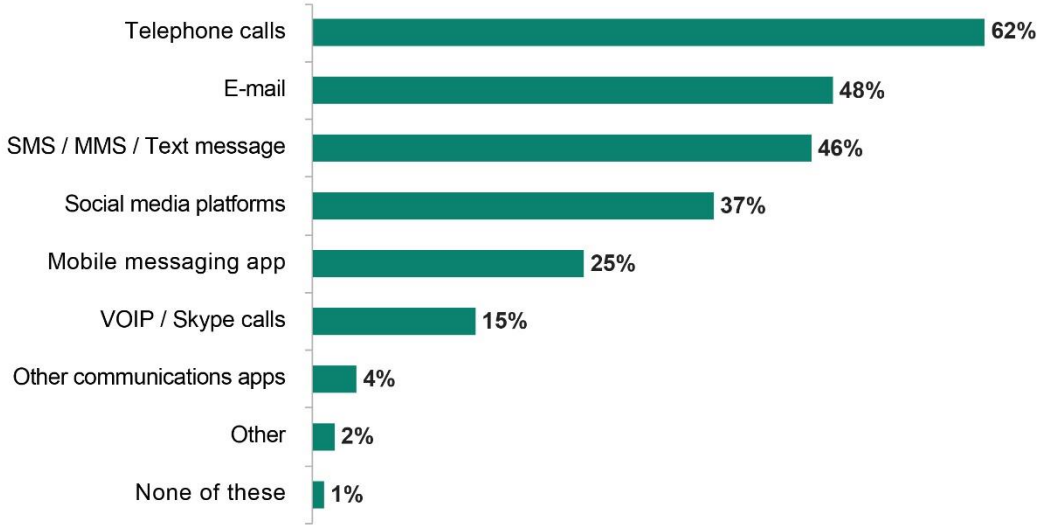
One in six (15%) Android device users take their phone into the bathroom, as do 9% of iPhone users and a surprising 4% of laptop (and tablet) users. Those aged 16 to 34 are, at 39%, 2.5 times are as likely as those over 45 to take their device into the bathroom.

Section 2. Online and on the move: Internet activity

Consumers' primary online activities include email, online shopping, news, social media, banking and entertainment such as films and gaming – although devices are also used for payment transactions, education and even online dating.

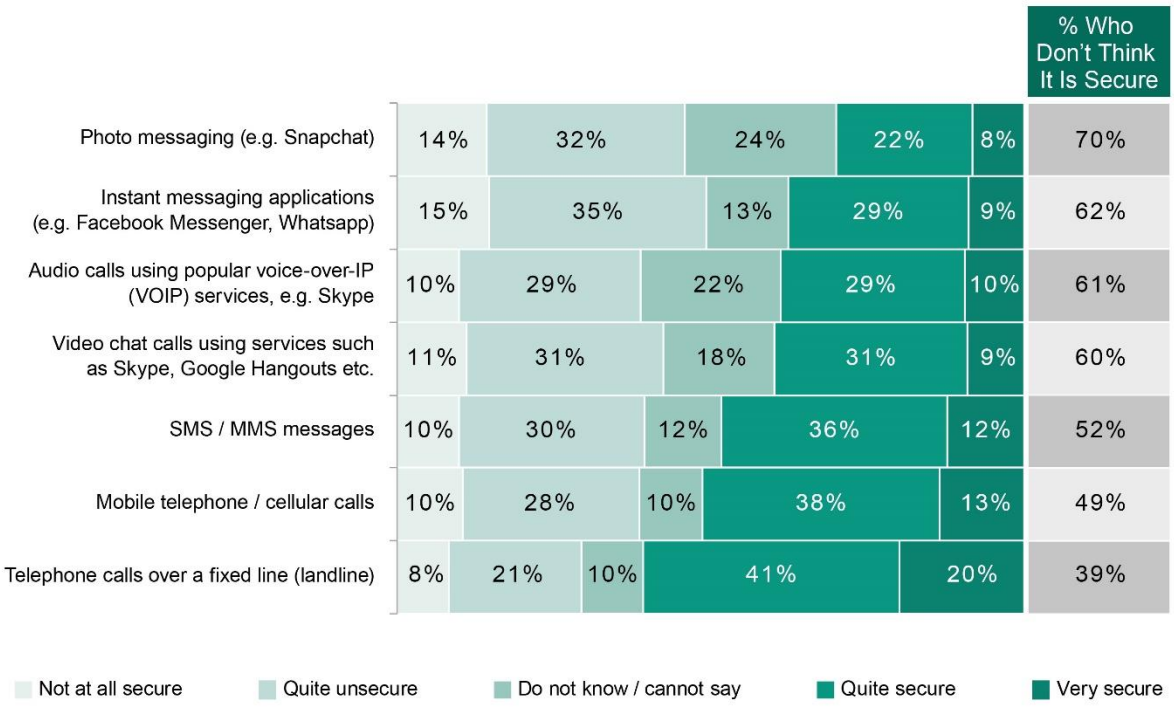
Activity	Any Device	Desktop / Laptop Computer	Tablet	Smartphone
E-mail	**85%**	86%	77%	83%
Working	**73%**	76%	63%	58%
Using social media sites	**67%**	65%	61%	70%
Online shopping	**66%**	70%	48%	41%
Reading news, articles, books, etc.	**66%**	66%	62%	62%
Online banking	**60%**	61%	42%	44%
Watching movies / videos online	**54%**	54%	51%	37%
Downloading software/ applications	**51%**	49%	42%	50%
Instant messaging / video calling	**48%**	44%	44%	51%
Education / learning	**44%**	46%	43%	29%
Using online payment systems / wallets	**42%**	44%	28%	27%
Online gaming	**40%**	37%	39%	37%
Uploading / Sharing media	**37%**	36%	32%	33%
Online data storage	**35%**	35%	33%	27%
Visiting online dating websites	**13%**	12%	15%	9%
Other activities	**1%**	1%	1%	1%

The communications methods used range from the well-established such as telephone calls, email and text messaging to social media, mobile message and VOIP:

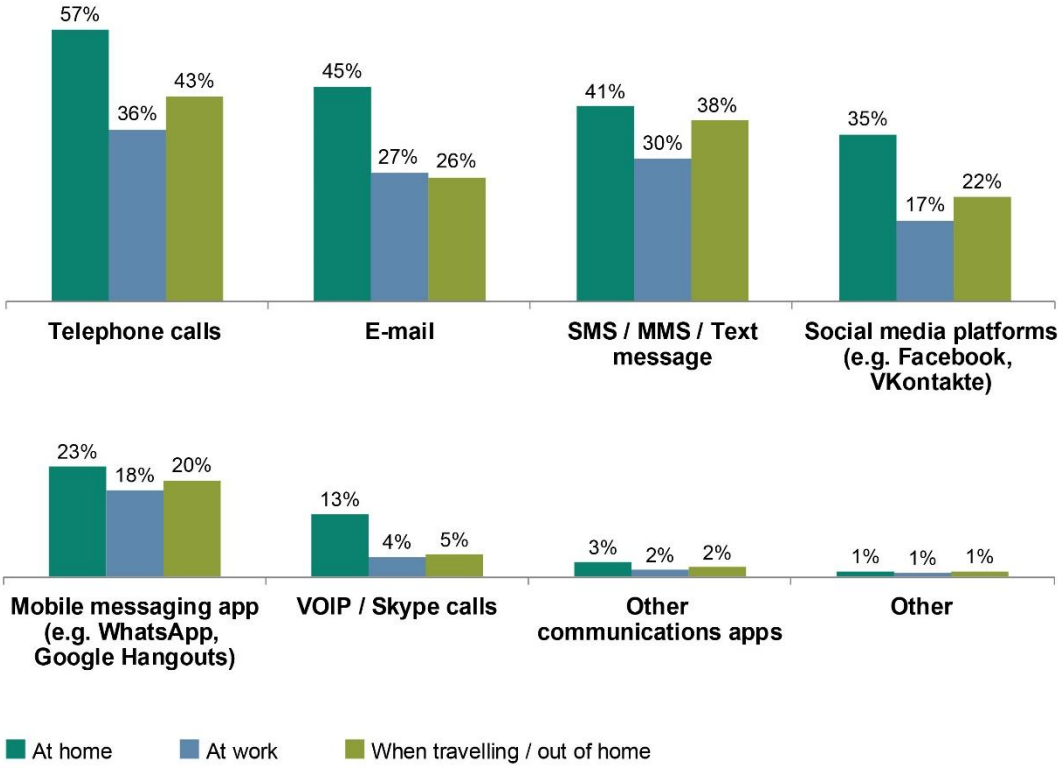


The study found that concerns about the security of some online communications channels do not prevent consumers from using them. For example, a quarter uses messaging apps such as WhatsApp and Facebook messenger, even though 50% regards them as insecure.

The communications methods used most by consumers to stay in touch tend to be the most well-established ones: phone calls (used by 62% of respondents), SMS/MMS text messaging (46%), and email (45%). These are also perceived as the most secure.



Most online communications activity takes place when users are at home. Outside the home environment, users see little difference between work, travelling, shopping or socialising. For example, 20% communicate via mobile messaging while on the move and 18% do so while at work.

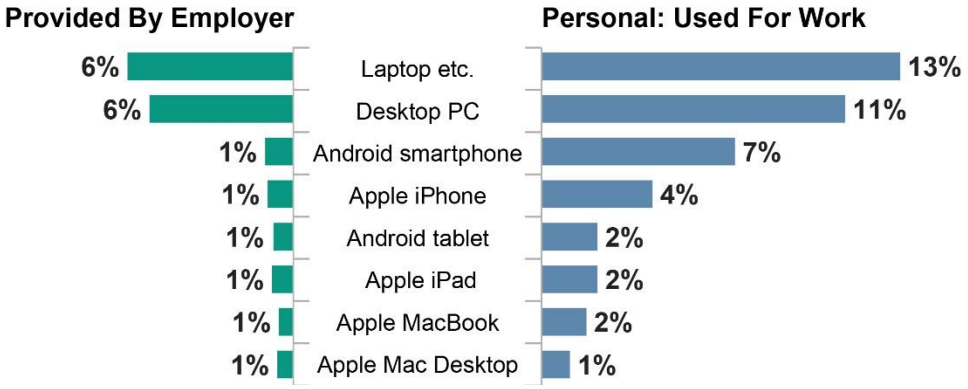


Women prefer to communicate via social media (41%, compared to 35% of men), while men are more likely to prefer VOIP/Skype (17% compared to 14% for women.)

Those aged 45 and over prefer the more traditional channels of phone (68%) and email (67%); leaving texting (52%), social media (45%) and mobile messaging (34%) to be dominated by those aged 16-34 and smartphone users.

The work-life balance of devices

The study shows the extent to which consumers are using personal devices for work and devices owned or provided by work for personal activity. The boundaries between work and personal device use are blurring, and study reveals some of the potential security risks associated with this.



Around one in seven (13%) respondents uses a personal laptop for work, and 6% uses a work-provided one for personal activities. Similarly, 7% uses their own Android smartphone and 4% their own iPhone for work.

Work device users tend to be more active overall. For example, 41% of those with smartphones that are used for or provided by work use their device for online shopping, compared to 32% of general smartphone owners. Similarly, online payments are undertaken on 27% of work smartphones compared to 20% of general ones.

Perhaps more surprising is the popularity of online dating websites among those who use their devices for work – 15% of work tablet users visit online dating websites, compared to 8% of general tablet users.

Activity	Any Device	Desktop / Laptop Computer	Tablet	Smartphone
E-mail	**85%**	86%	77%	83%
Working	**73%**	76%	63%	58%
Using social media sites	**67%**	65%	61%	70%
Online shopping	**66%**	70%	48%	41%
Reading news, articles, books, etc.	**66%**	66%	62%	62%
Online banking	**60%**	61%	42%	44%
Watching movies / videos online	**54%**	54%	51%	37%
Downloading software/ applications	**51%**	49%	42%	50%
Instant messaging / video calling	**48%**	44%	44%	51%
Education / learning	**44%**	46%	43%	29%
Using online payment systems / wallets	**42%**	44%	28%	27%
Online gaming	**40%**	37%	39%	37%
Uploading / Sharing media	**37%**	36%	32%	33%
Online data storage	**35%**	35%	33%	27%
Visiting online dating websites	**13%**	12%	15%	9%
Other activities	**1%**	1%	1%	1%

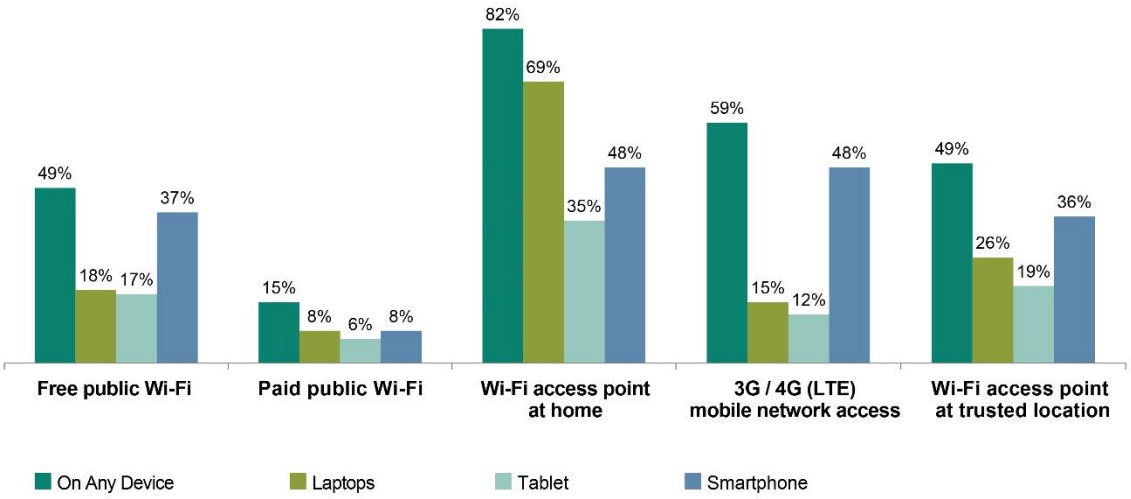
The security implications of this are clear. Consumers who use their connected devices for work, use them more for everything. This does not just increase their own exposure to risk, but often that of their employer too.

Wireless without a safety net

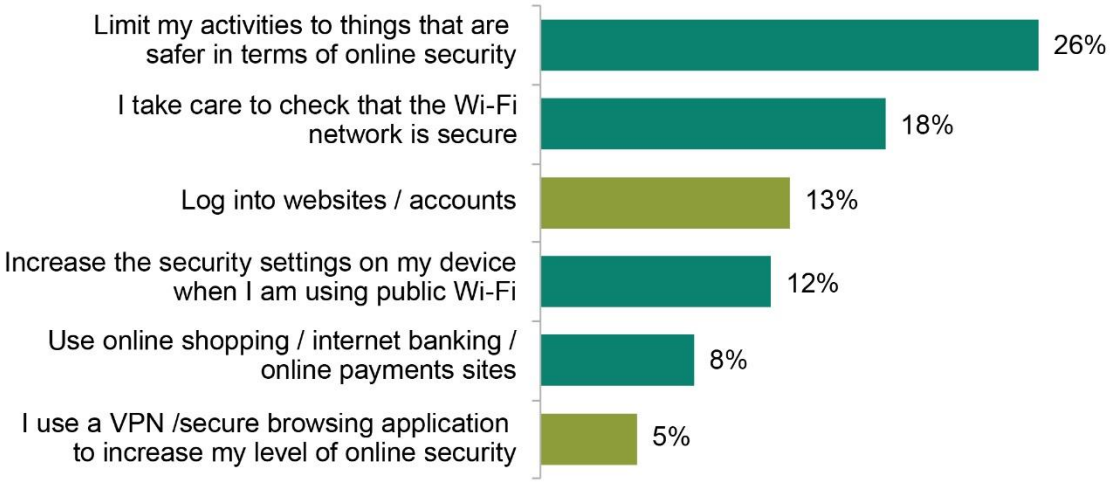
The study found that for all device users wireless networks play a key role in enabling online activity both at home and while out and about. Eight in ten (82%) have a Wi-Fi access point

installed at home. Laptop users are most likely to connect over Wi-Fi at home (69%), as are tablet users (35%), with far fewer using Wi-Fi, 3G or 4G/LTE networks while out and about.

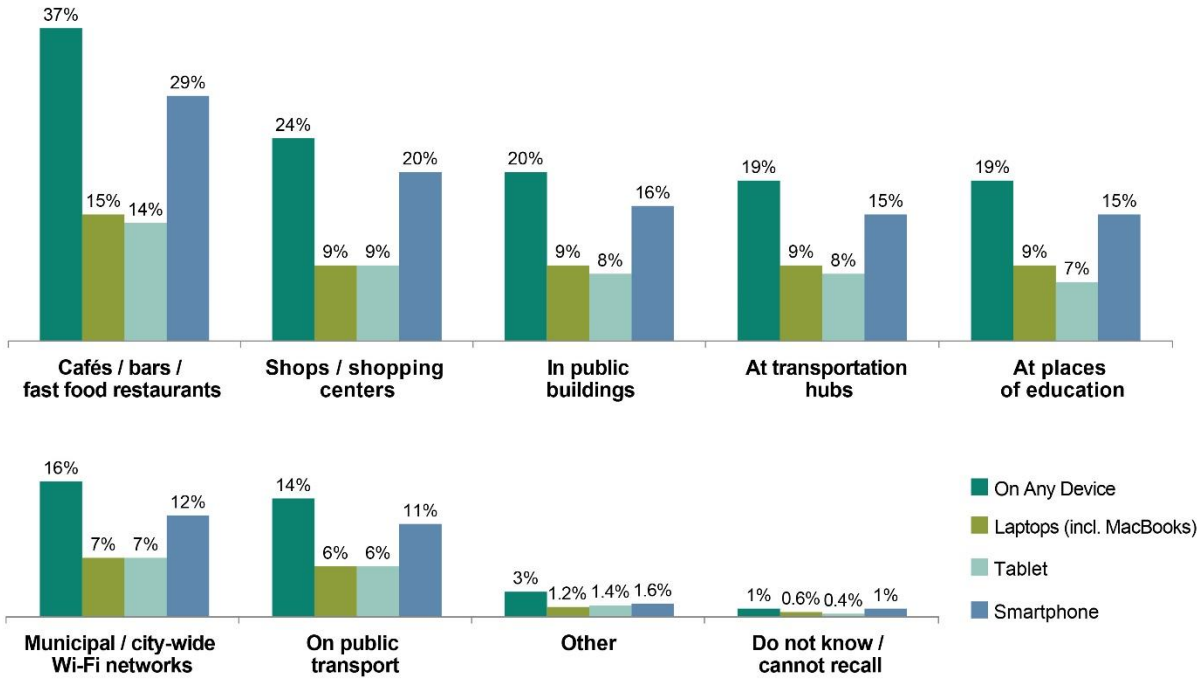
Not surprisingly, highly portable smartphones are widely used to connect to the Internet at home and elsewhere. 48% connects over home Wi-Fi networks and the same proportion goes online over 3G and next generation 4G/LTE networks. A third uses a Wi-Fi access point at a trusted location (36%) and free public Wi-Fi (37%).



A worrying 13% of consumers use public Wi-Fi to log onto websites and accounts, and 8% uses them to shop or bank online. Just one in four (26%) says that when using public Wi-Fi they limit their activities to things that are safer.

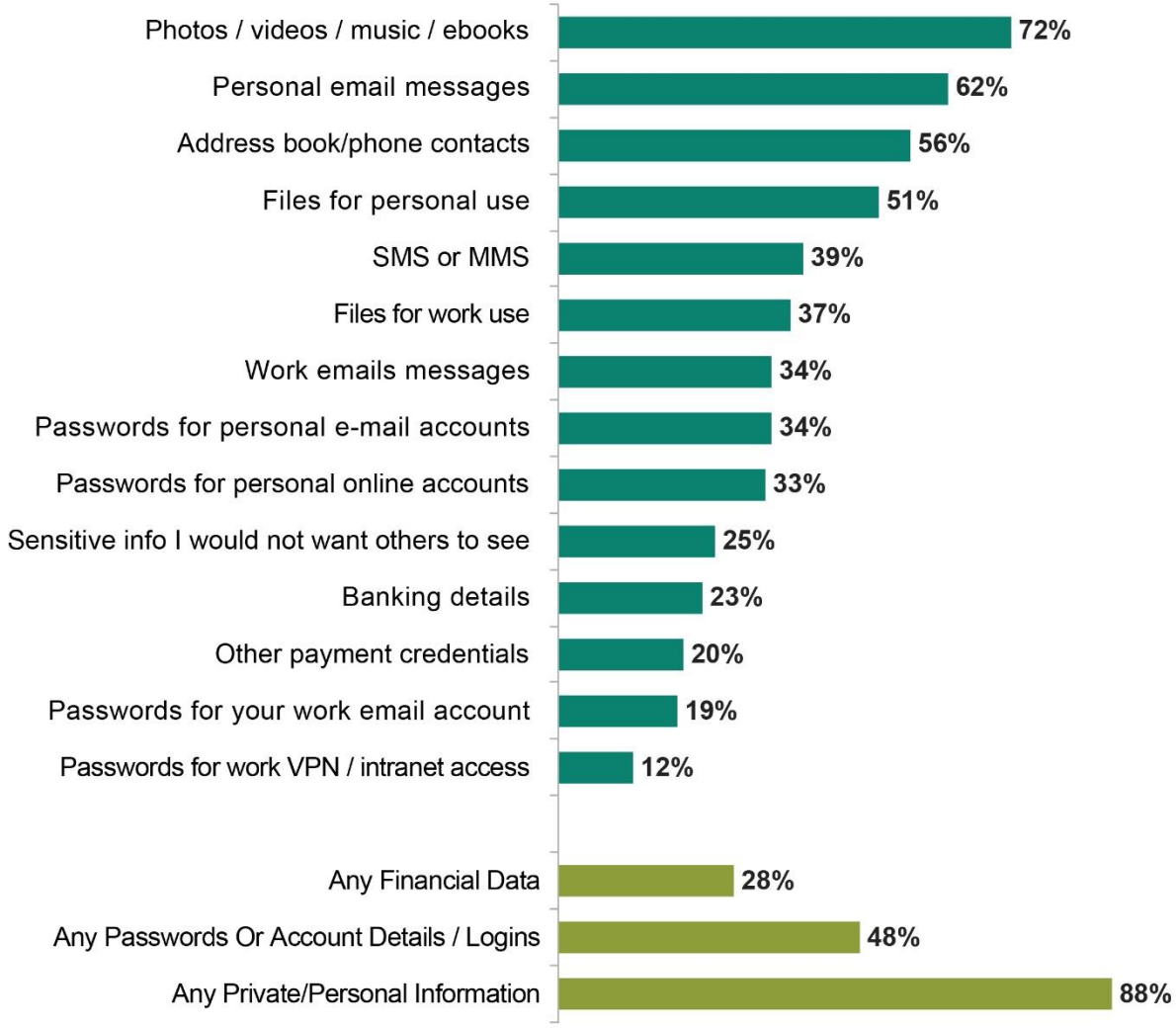


The use of insecure Wi-Fi networks is likely to reflect their convenience, cost-effectiveness and generally fast download speeds – all highly attractive to today's connected, mobile consumer. A third (37%) of all device owners connect to the Internet over public Wi-Fi while in a café or restaurant and 24% connects in shops and shopping centres. Smartphone users are most likely to connect in cafés/restaurants (29%) and shops (20%).


37%
15%
14%
29%
24%
9%
9%
20%
20%
9%
8%
16%
19%
9%
8%
15%
19%
9%
7%
15%
Cafés / bars / fast food restaurants
Shops / shopping centers
In public buildings
At transportation hubs
At places of education
16%
7%
7%
12%
14%
6%
6%
11%
3%
1.2%
1.4%
1.6%
1%
0.6%
0.4%
1%
Municipal / city-wide Wi-Fi networks
On public transport
Other
Do not know / cannot recall
On Any Device
Laptops (incl. MacBooks)
Tablet
Smartphone

Section 3. The connected treasure chest: what is stored on devices

The study explored the potential risks facing the personal data increasingly stored on Internet-enabled devices. It found that 88% of respondents store some form of private or personal information on their digital devices. Around half (48%) store passwords or account login details and 28% stores financial data - information that could be of immense value to criminals.



Many of those surveyed now understand this: around half says that the most worrying information cybercriminals could get hold of are their account passwords (47%) and financial assets (46%), followed by details of where they live (34%) and private pictures and videos (24%).

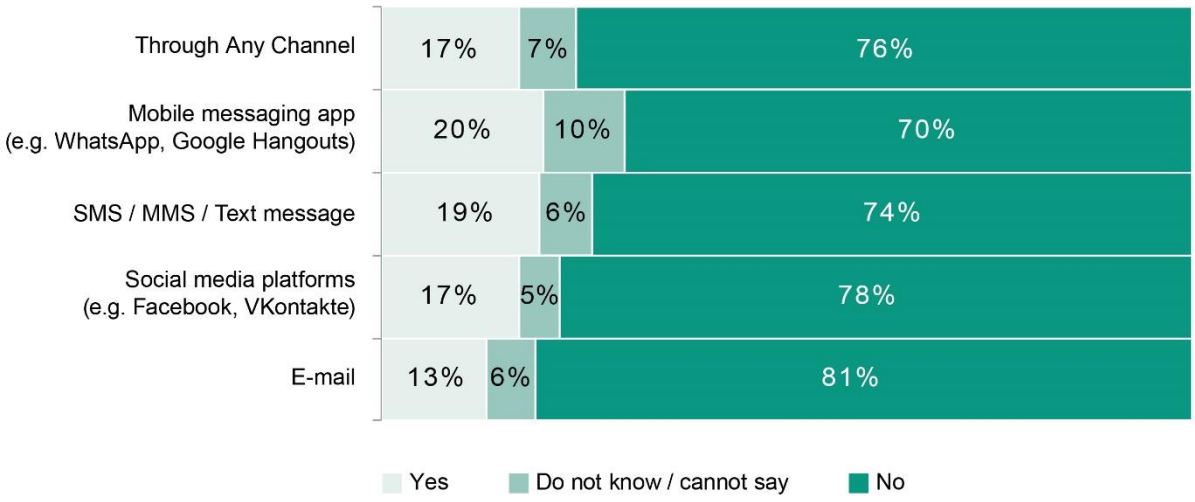
The loss of information stored on a device can have financial as well as emotional and practical consequences. The study found that the estimated median value of replacing all digital assets stored on devices is $682.

The study also found that personal information and images are being shared freely from Internet-enabled devices – not just about the users themselves, but about other people.

For example, while 45% has shared a picture of themselves, 36% has shared an image and 16% a video of someone they know. One in ten (9%) has shared a document containing private or personal information about someone else, compared to 14% doing the same with their own information. Nearly half of those surveyed (42%) has shared their own contact details and 30% has revealed their date of birth or address.

Much of this information is shared only with friends and family, but colleagues and others account for a small but significant share. For example, 16% have shared personal contact details with colleagues and 4% has made public a photo of someone they know.

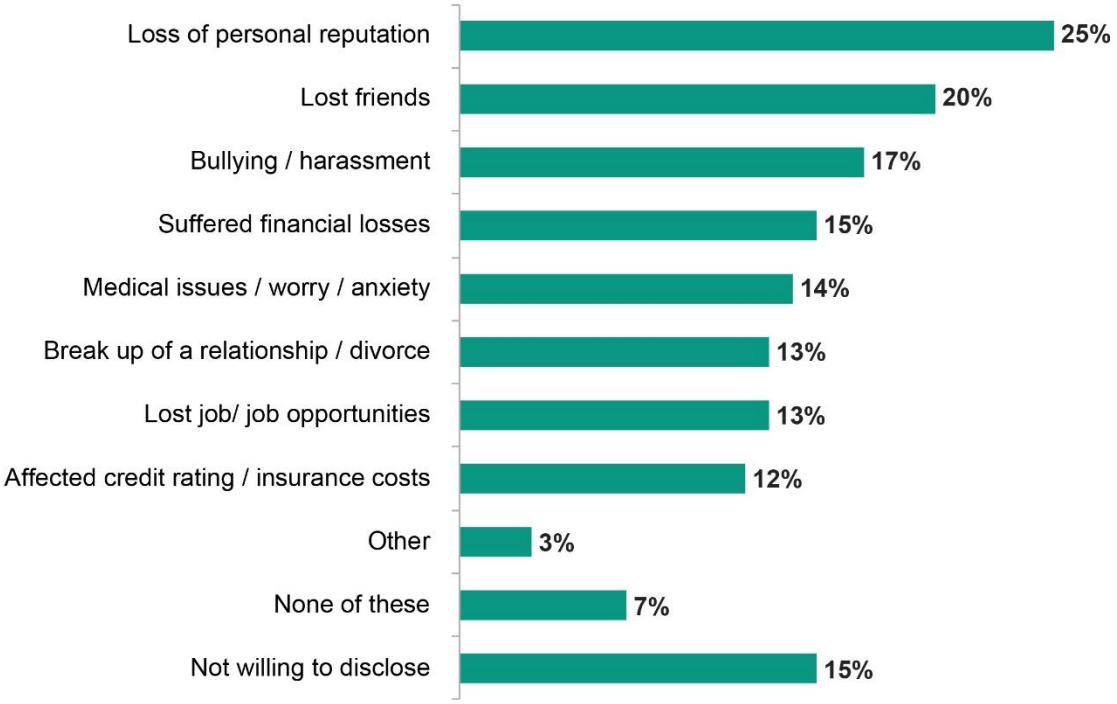
Up to a fifth of consumers have shared explicit content – with 20% sharing through a mobile messaging app, 19% by text and 17% through social media; despite their clear concerns about the security of such platforms.



This contradiction between what people fear and what they do regardless of those fears can also be seen elsewhere. Half (54%) worries that sharing information will result in a secret being exposed, 49% worries about identity theft, and a third worries about embarrassing or offending someone and the risk of damaging personal relationships. Yet just 36% of

respondents have implemented strong privacy settings to ensure only trusted people can see, and 19% takes no special action to protect their privacy and keep personal information safe.

22% has accidentally disclosed confidential information, and for around half of them there have been consequences:



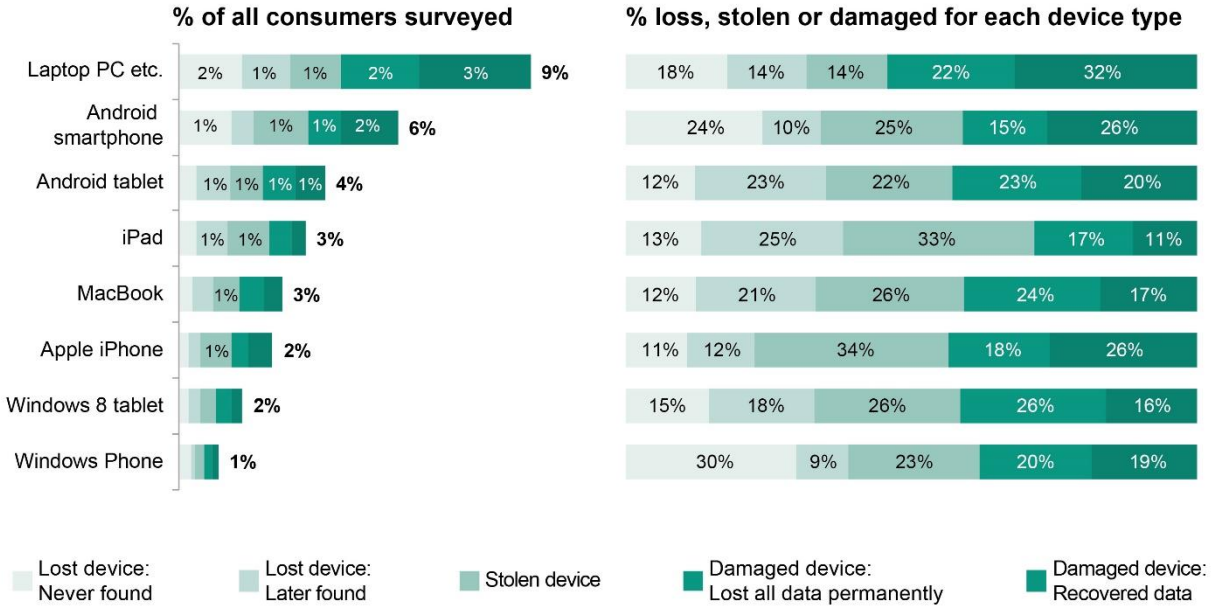
Sharing doesn't stop at information; consumers also share their devices with others. Around a quarter is happy to let people they live with go online using their primary device. Security for shared devices is varied and includes protecting files with passwords (used by 30%), setting up separate user accounts (25%) or a specialist protection solution (11%). Over a quarter (28%) believes there is no risk, so doesn't do anything.

Section 4. Risk: damage, loss or the theft of devices

In the last 12 months, one in seven (14%) respondents has lost a connected device or had it stolen, and 12% has damaged a device. 15% of the data lost was never recovered,

Younger respondents were the most affected, with 17% of those aged under 24 losing a device and 13% having it stolen – around twice as many as older age groups.

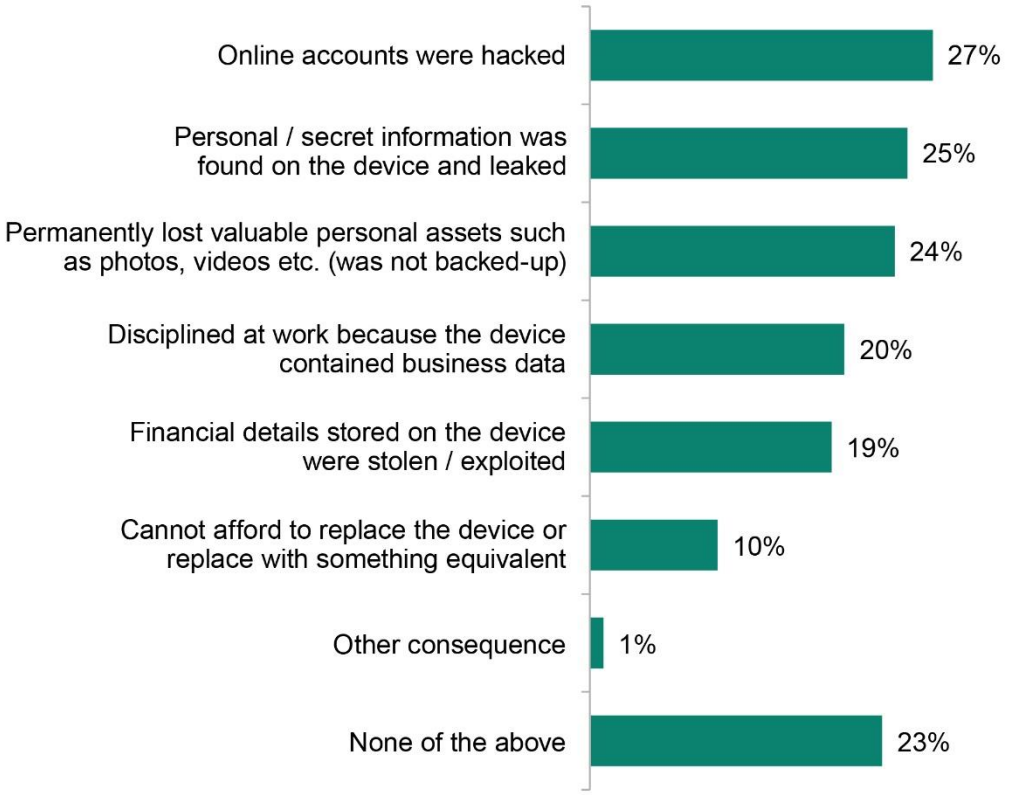
Laptop PCs and Android mobiles were the most affected devices:



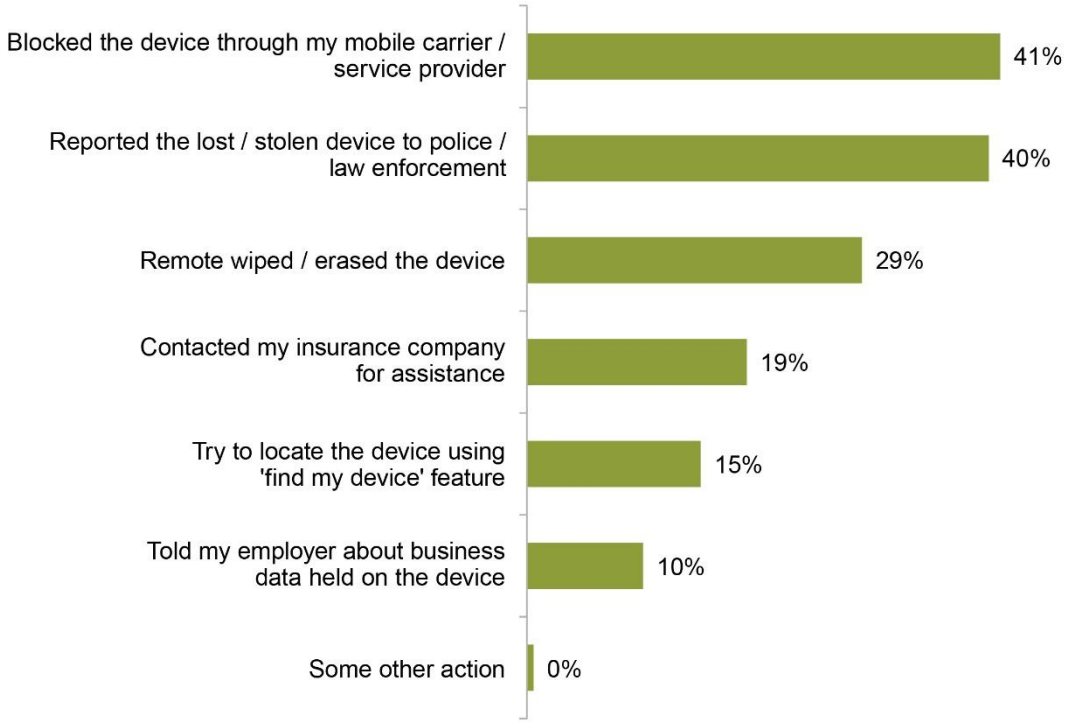
For three quarters (77%) of respondents the loss or theft of a device turned out to have far-reaching consequences.

As result, a quarter (27%) found their online accounts hacked into - rising to 32% of those aged under 24. 25% discovered that personal or secret information had been leaked, 24% permanently lost valuable personal information such as photos that had not been backed-up and 19% realized that financial details stored on the device had been stolen and used.

The study also found that one in five (20%) of those who had suffered a consequence had been disciplined at work because the missing or damaged device contained business data.



Consumers reacted to the loss or theft of a device in a number of ways: 41% of respondents asked their service provider or mobile network operator to block the device, 40% reported its disappearance to the authorities, 29% undertook a remote data wipe and 15% tried to locate the device. Around 11% took no action.

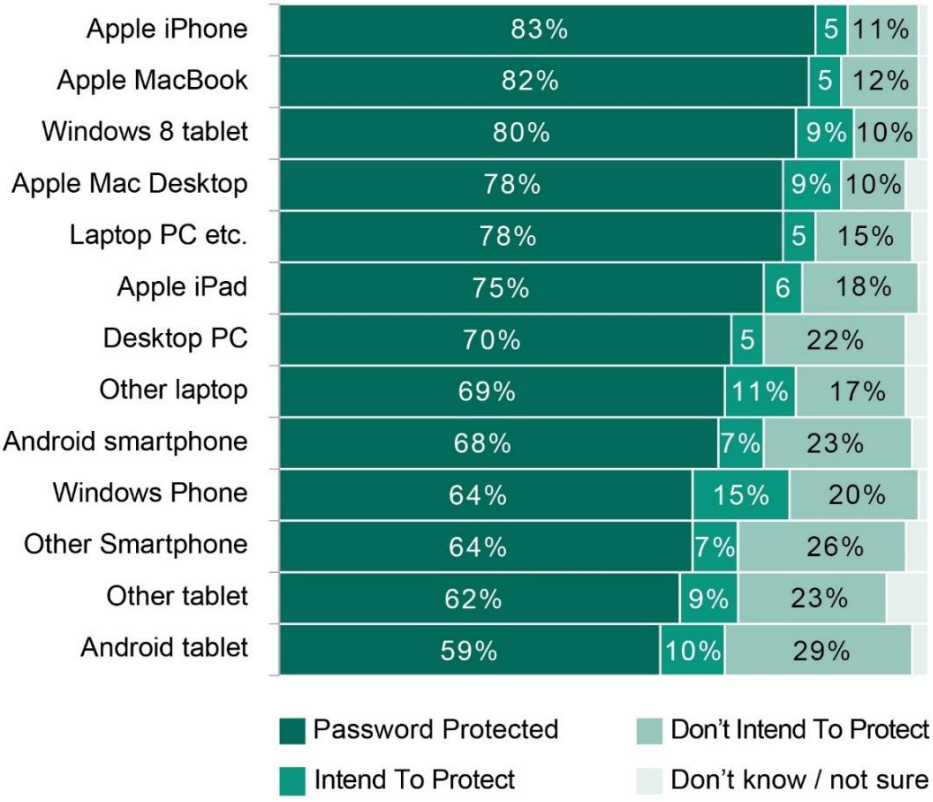


Section 5. Device protection

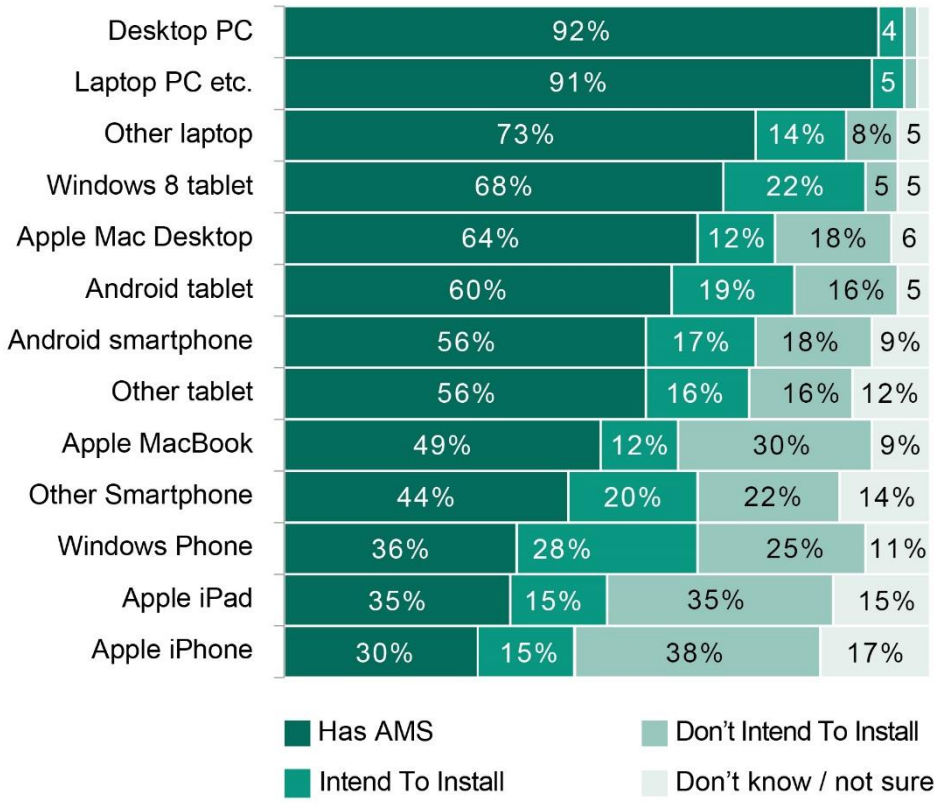
The 2015 study shows that high levels of connected device ownership and use, as well as a growing awareness of risk are not matched by an equally high level of protection. Just 58% of device users protect all their devices with passwords, and a worrying 16% doesn't password-protect any.

Around a third of those of with Android smartphones (30%) and tablets (39%), as well as 35% of Windows phone users fail to protect their device with a password, and up to a quarter say they have no intention of doing so.

In contrast, Apple iPhones, MacBooks and iPads are among the most password-protected, with 83%, 82% and 75% respectively setting a password – often prompted to do so by the device upon set-up; as well as 78% of all laptop users.

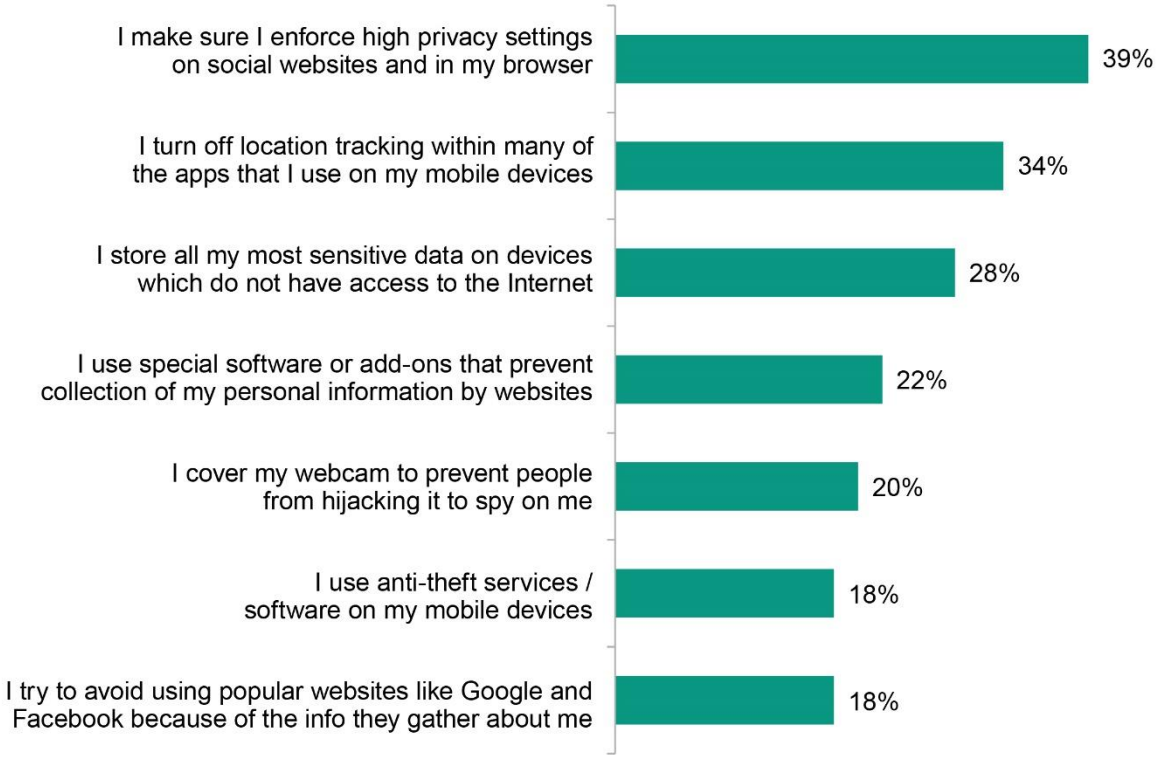


Further, a mere third (30% and 35% respectively), has installed an anti-malware solution on their Apple iPhone or iPad; while just 56% has done so for their Android smartphone. PCs and Macs are on the whole far better protected, with 92% installing anti-malware software on their PC and 64% doing so for their Mac. A fifth (21%) has not installed any security software on their main device.

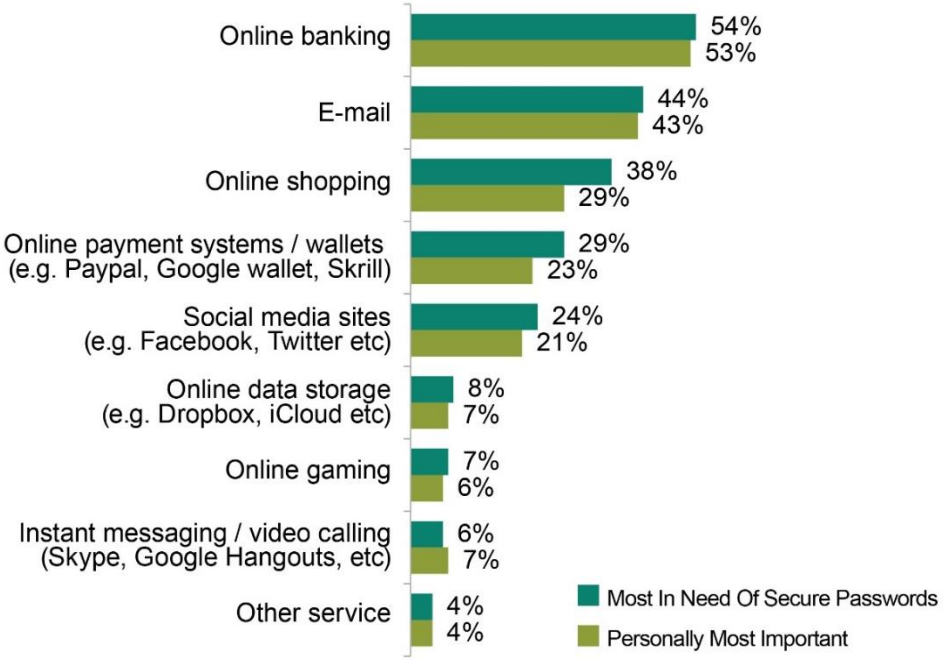


Only around half (53%) use the security functions that come with their devices, such as remote block/find-my-device capability – with smartphone (47%) and tablet (47%) users the most likely to do this. Similarly, only around a third (38%) set up separate users accounts for different users and purposes, with laptop (33%) and desktop (36%) users the most likely to do this. A third would run a scanning and disinfection solution if necessary, although just one in five would bother to do this for a tablet or smartphone.

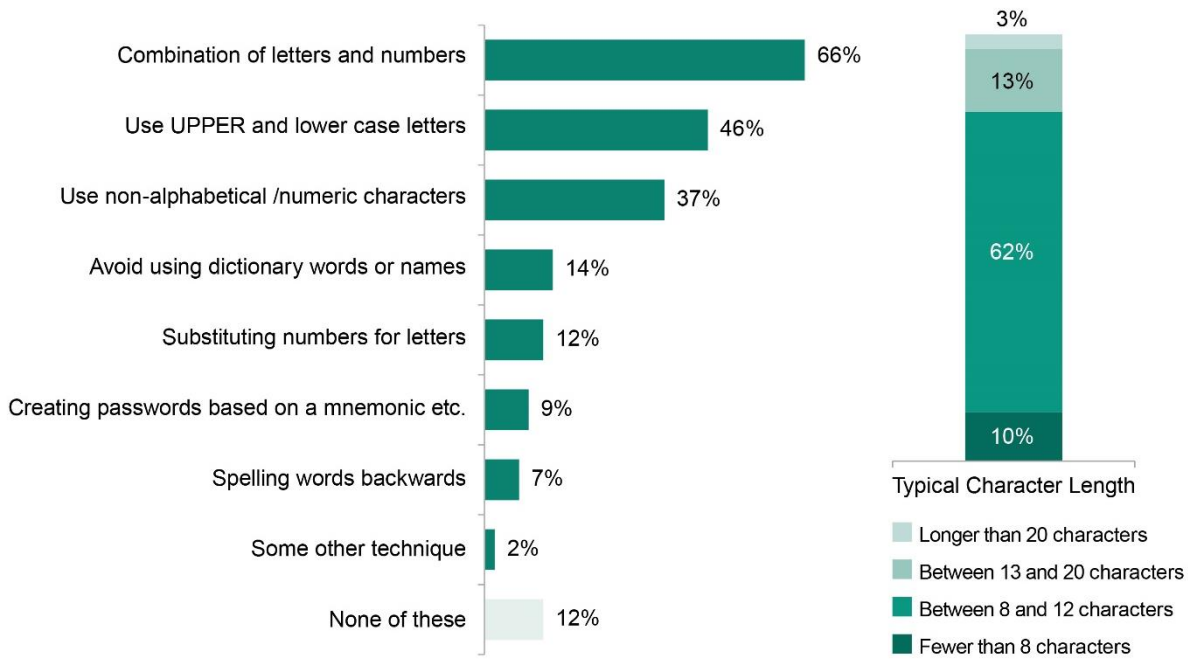
Other actions to protect devices and activity on devices include enforcing strong privacy settings on social media accounts and browsers (39%); turning off location-tracking (34%) and storing sensitive data on a device that is not internet-connected (28%). A fifth physically covers their webcam, and the same number avoids popular social media networks and websites.



When it comes to protecting online accounts, half of those surveyed believe online banking sites are most in need of a secure password (54%), followed by email at 44% and online shopping sites at 33%. Just 29% of respondents felt that secure passwords were a priority for online payments systems.

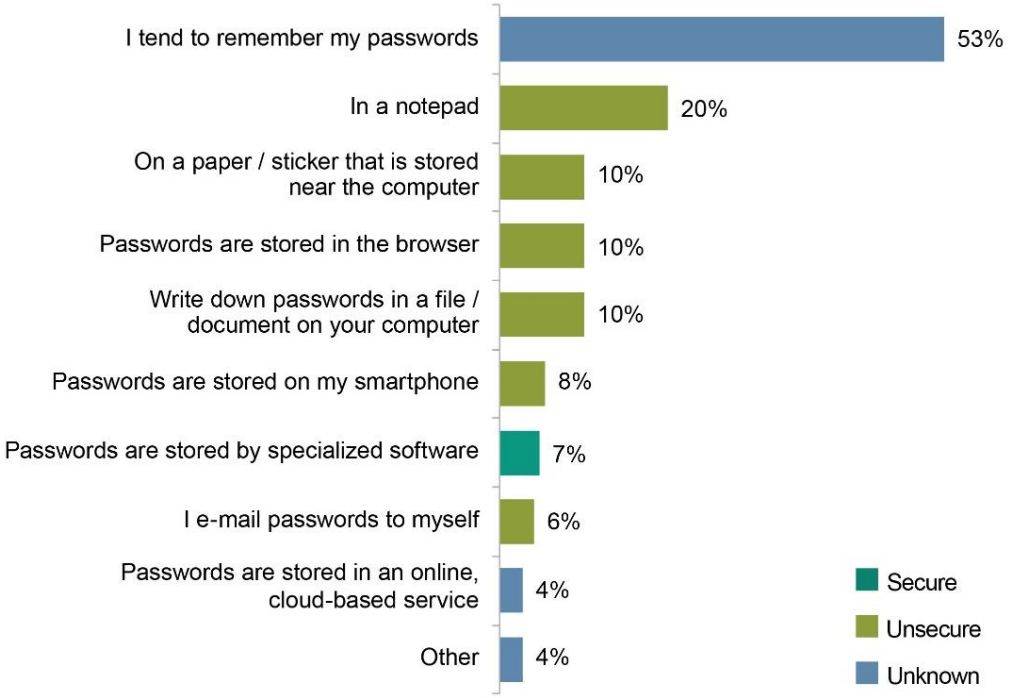


However there are signs that messages about the need for secure passwords, and what constitutes a secure password are starting to get through. For example, passwords are now generally longer and comprise a greater mix of lower and upper case letters and numbers.



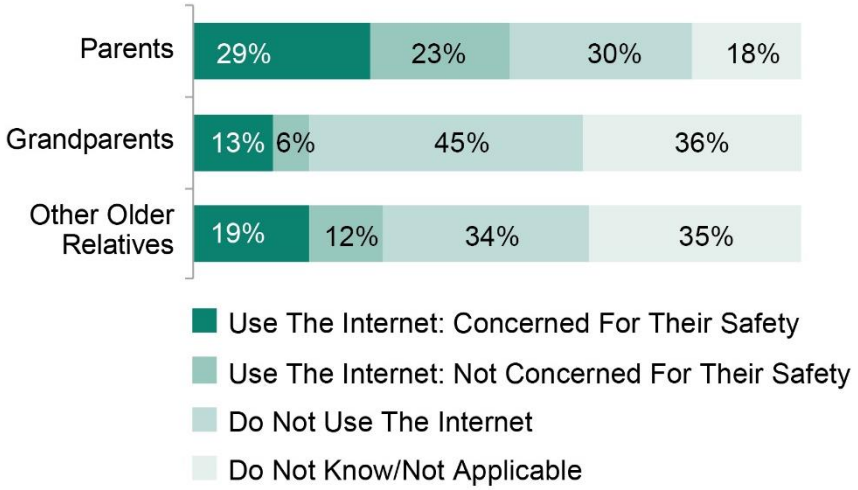
Despite this, 23% of respondents have no more than five passwords for up to 20 online accounts. This suggests that passwords are frequently re-used and rarely changed.

Further, a third of respondents are happy to share their password with family members and half (48%) store passwords insecurely: on notepads, sticky notes or on their device.

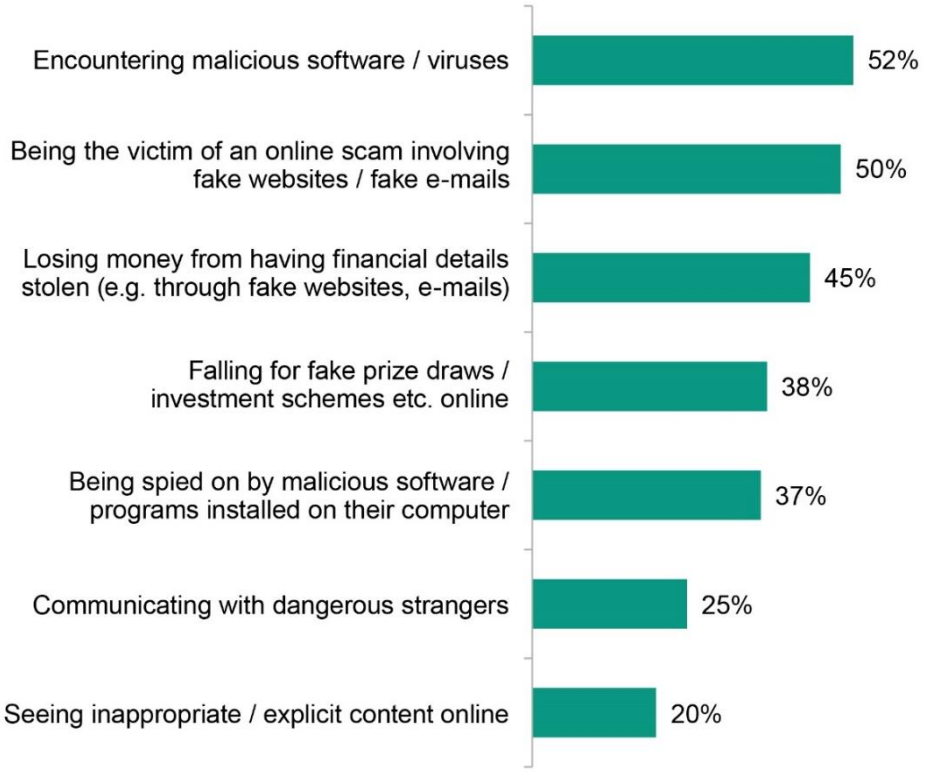


Section 6. Protecting other people

Up to two-thirds (61%) of those with older parents and grandparents who use the Internet worry about their relatives' safety online. Adults worry that older relatives may not know how to protect themselves from malware (52%), online scams (50%) or theft (45%); and 25% worries about their vulnerability in the face of contact from dangerous people they don't know and being exposed to explicit or inappropriate content.



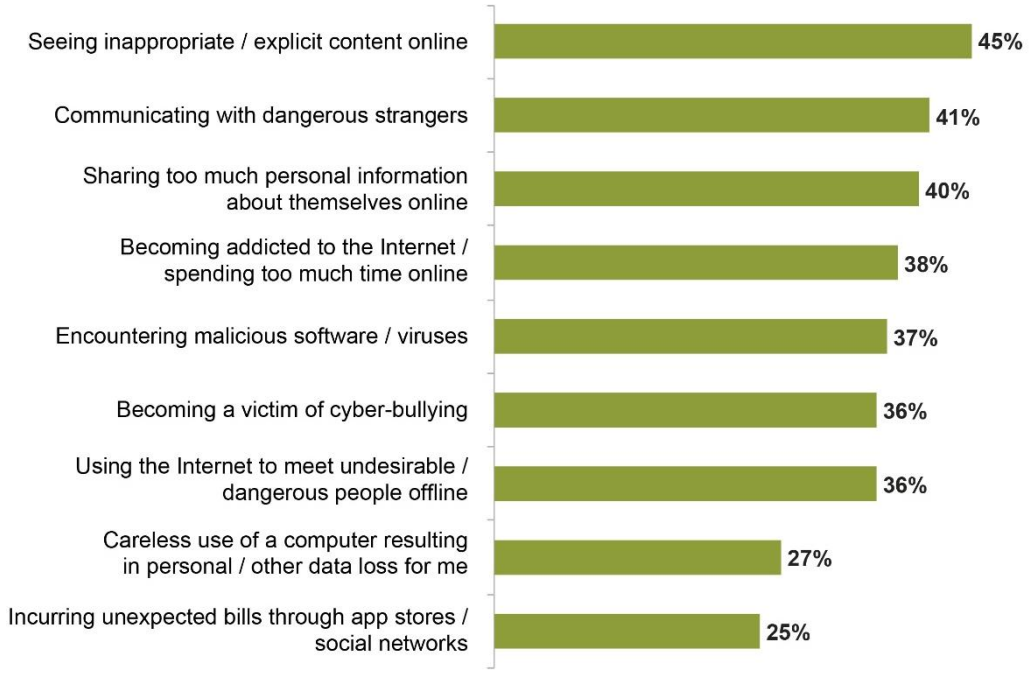
The main concerns are:



Half of parents believe that online threats to their children are increasing – but a fifth does nothing to keep them safe.

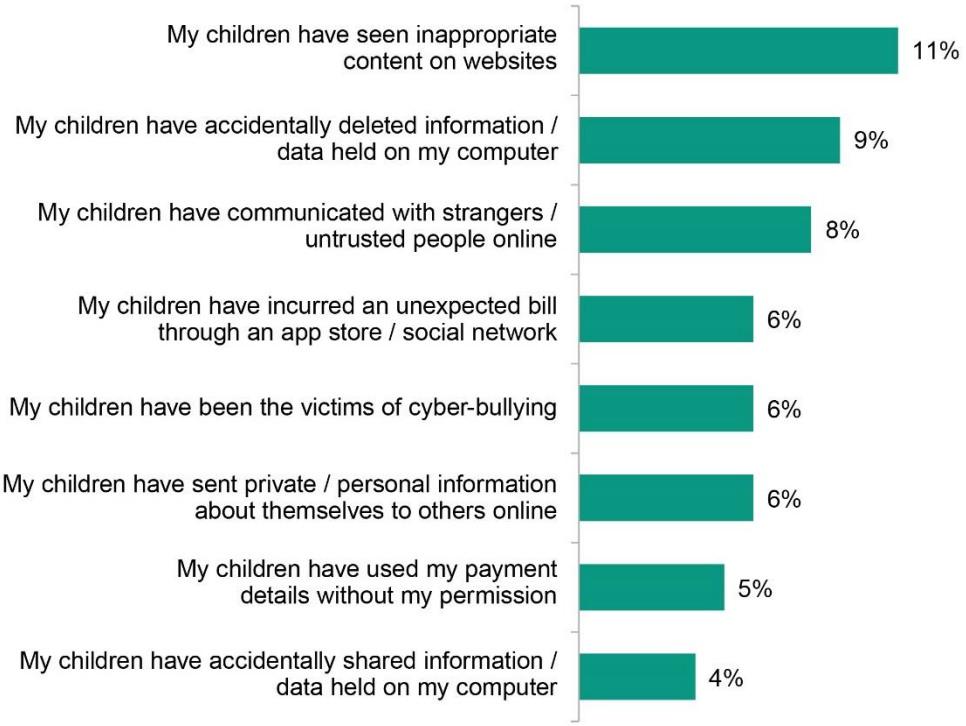
According to parents the greatest online threat facing children is exposure to inappropriate or explicit content: a worry for 45% of parents and experienced by 11% of children in the last 12 months. This is followed closely by concerns about contact with dangerous strangers (41%), experienced by 8% of children, and the over-sharing of personal information (40%), experienced by 6%. With the boundaries between the on- and offline world increasingly blurred for many young people, it is not surprising that a top concern for 36% of parents is that children might arrange to meet in the real world an unsuitable person they had met online.

A third (36%) worries that their children will become victims of cyber-bullying. Although just 6% believe that their children have been cyber-bullied in the last year, the real extent of cyberbullying may be far higher. Three in ten (31%) parents feel unable to control what their children see or do online, so could be unaware of any cyber-bullying affecting, or even perpetrated by their offspring.

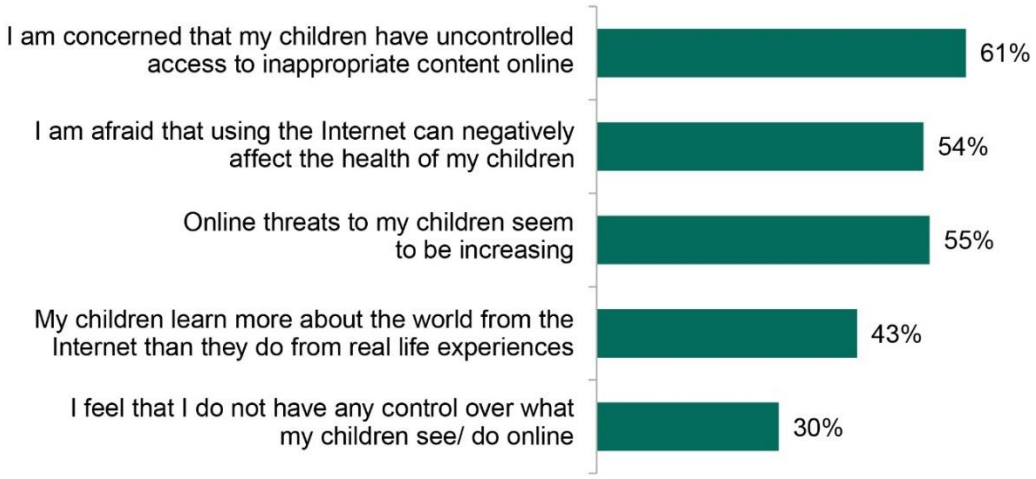


Nearly two thirds (61%) of parents with children aged under 18 living with them worry that their children have uncontrolled access to inappropriate content online – but three quarters (76%) of all parents have not installed parental control software that would help to mitigate such risks.

The study also found that young people can unintentionally expose their families to risk by inadvertently losing or sharing data or incurring costs, such as through in-app purchases. Around a quarter of parents worry about this and 20% have experienced it. By the parents' point of view, children experienced online for a 12 month period:



With a considerable amount of inappropriate, distressing and potentially harmful content accessible through the Internet, it is disheartening to see that just under half (42%) of parents believe their children learn more about the world from the Internet than they do from real-life experiences.



The survey shows that parents try to protect and support their children online by educating them about potential risks (39%), limiting the amount of time they spend online (37%), supervising their online activity (33%) and installing special software, among other things.

Supporters of parental control software welcome its ability to spot dangerous sites they might otherwise miss (43%) and the reduced need for constant supervision (37%). Others feel that it could discourage children from learning how to use the Internet safely (21%). One in ten believes their children will see inappropriate content whatever measures are taken.

Section 7. Risk: malware, identity theft and financial incidents

Malware

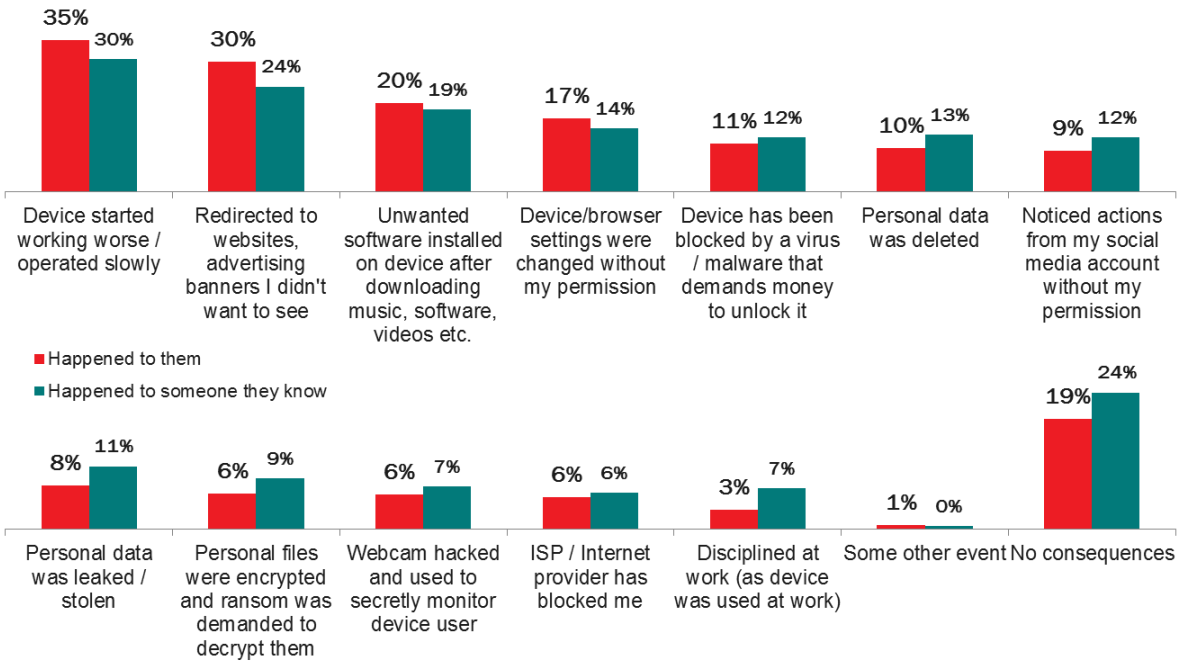
Of the Internet-users surveyed, 45% had suffered at least one malware incident in the last 12 months, and 44% say they know of others who have been affected. 13% of those who had been infected didn't know how. Others acknowledged that they had been hit following a visit to a suspicious or untrusted website or after installing a fake application.

One in six was infected through a message or storage device from someone they know and 6% became infected by visiting a genuine website that had been hacked. This highlights the extent to which attackers are willing and able to exploit trusted personal relationships and brands to spread their malicious software.

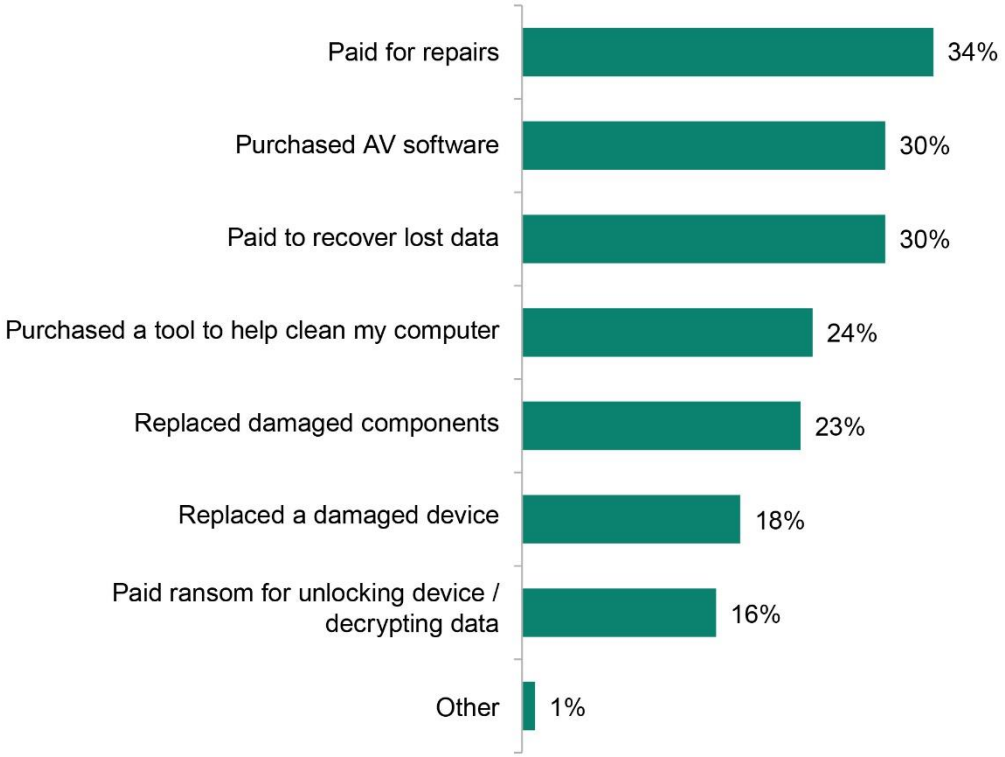
Threat experienced	Any Device	Windows PC	Android Device	iOS Device	Mac Desktop/ MacBook	Mobile Windows Device
Got virus / malware infection, but not sure of the method	13%	89%	5%	1%	3%	0%
Device infected after visiting suspicious / untrusted website	12%	81%	11%	6%	6%	2%
Device has been infected by a virus after using a USB stick etc. given to me by someone I know	8%	78%	14%	7%	7%	2%
Got malware infection due to it spreading from another infected device	7%	78%	16%	7%	7%	4%
Device infected after installing a fake application which posed as a legitimate one	7%	76%	19%	6%	7%	2%
Device has been infected by a virus after opening an e-mail etc. attachment from someone I know	7%	71%	18%	11%	7%	2%
Device has been infected by a virus after opening an e-mail etc. attachment from someone I do not know	7%	74%	17%	7%	6%	3%
Device has been infected after visiting a genuine website that had been hacked	6%	77%	14%	8%	9%	2%
Any malware incident	**45%**	**83%**	**13%**	**6%**	**6%**	**2%**

Different device types are vulnerable to different malware attacks. For example, 52% of laptop and 46% of desktop users were unable to determine how they were infected, compared to just 5% of smartphone users. In fact, infected fake apps were the top infection vector for smartphones, accounting for 22% of all malware incidents. The top threat for tablets appeared to be opening infected attachments from someone they know.

The most likely impact of a malware infection was reduced performance, with 35% saying the device slowed down or failed to function properly. One in three (30%) found themselves redirected to websites and advertising banners and 20% had unwanted software installed. Around one in ten was hit by a more severe impact, including data locking (11%), encryption and demands for a ransom (6%), the deletion of personal data (10%), fraudulent social media posts (9%) and hacked webcams (6%).



One in three (33%) of all potential malware incidents resulted in financial costs, with the most prevalent being the need for to pay for professional repairs, followed by the need to buy a replacement device. The estimated average cost incurred was $160 US. This estimate does not take into account the potential loss of valuable information, the risk of online accounts being compromised or financial details being stolen.



Intercepted identities

A third (36%) has been exposed to an identity threat and 25% say they know of others who have been affected. Identity theft takes many forms but the basic approach remains largely the same: pretending to be someone or something you're not in order to persuade people to reveal personal information such as names, addresses, account details, passwords and other credentials.

Threat experienced	Global	Windows PC	Android Device	iOS Device	Mac Desktop/ MacBook	Mobile Windows Device
Receiving anonymous/unsolicited email or social network messages with suspicious attachments/links	25%	79%	14%	9%	8%	2%
Receiving a suspicious e-mail claiming to be from a social network asking to send a password etc.	14%	75%	18%	12%	9%	3%
Being redirected to a suspicious web page asking to enter social media / e-mail / game credentials	11%	75%	19%	9%	8%	2%
Any identity threat	**36%**	**75%**	**16%**	**10%**	**8%**	**2%**

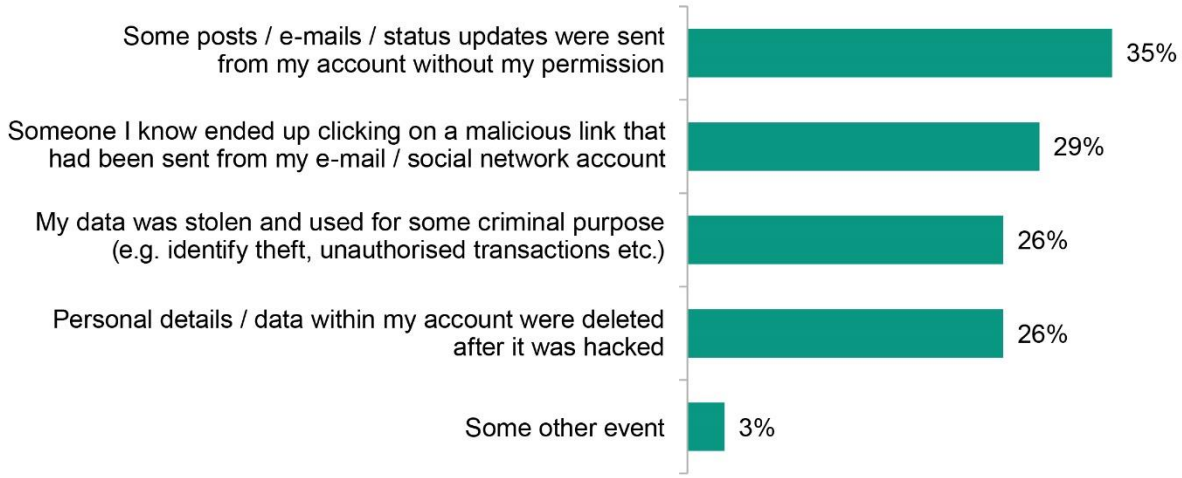
Traditional devices were more susceptible to identity theft approaches than mobile ones. Of those respondents who experienced a threat, most encountered it on a laptop (50%) or desktop (44%), with one in four being received on a smartphone. Around three quarters (75%) were experienced on the Windows PC platform and 16% on Android devices; with iOS devices accounting for 10% and Macs for 8%. The proportion of threats against Mobile Windows devices was negligible.

Account hacking

A quarter (25%) of respondents experienced some form of account hacking in the previous 12 months and 32% say they are know of others who have been affected. Respondents whose main device was an Android- smartphone or tablet were the most likely to be affected.

One in ten (11%) respondents discovered that their email or social media account had been accessed or had the password changed without their permission, and 7% noticed that someone else had obtained access to their online banking or shopping accounts.

In terms of impact, a third of those whose account had been hacked saw that unauthorized messages had been sent from the affected account. Around a quarter found their accounts being used for the distribution of malware through infected attachments (29%), or realized that information had been deleted or stolen for some criminal purpose (26%).



Financial Attacks

The number and range of financial threats is huge. As for identify theft, the attackers often disguise themselves as a reputable organisation and rely on people's trust and lack of awareness.

48% have experienced a financial threat in the last 12 months, and 42% know of friends, colleagues or family members who have been affected

Just under a quarter (22%) had received an email claiming to be from a bank and asking them to reveal personal or payment credentials, and 15% has received the same from an apparent shopping site. 11% were redirected to websites asking for such information.75% of those who experienced a financial threat encountered it on a Windows PC, while 18% of Android device users were affected. Financial threats made through smartphones mainly involved a direct approach by phone or email (30%).

Threat experienced	Global	Windows PC	Android Device	iOS Device	Mac Desktop/ MacBook	Mobile Windows Device
Receiving a suspicious e-mail claiming to be from a bank asking to send a password/other details	22%	81%	12%	10%	10%	2%
Receiving a suspicious e-mail claiming to be from a shopping site asking to send a password	15%	79%	15%	9%	8%	1%
Being redirected to a suspicious web page asking to enter online financial account details	11%	79%	16%	7%	6%	3%
Approached by a suspicious person over the phone / by e-mail trying to obtain financial data	12%	62%	23%	9%	7%	2%
A victim of some kind of online scam / fraud and had money stolen	6%	65%	15%	11%	6%	2%
Lost money on payment cards as a result of a retailer having their security compromised	4%	56%	16%	14%	10%	4%
Entered details on a fake banking/ payment website	4%	66%	20%	13%	12%	4%
Victim of data leakage / loss by financial organization	5%	54%	11%	12%	8%	3%
Had cryptocurrency (e.g. BitCoin) / e-money stolen	3%	64%	17%	10%	4%	5%
Other incident involving potential money loss (please state)	2%	52%	7%	5%	3%	0%
Any financial incident	**48%**	**75%**	**18%**	**11%**	**8%**	**3%**

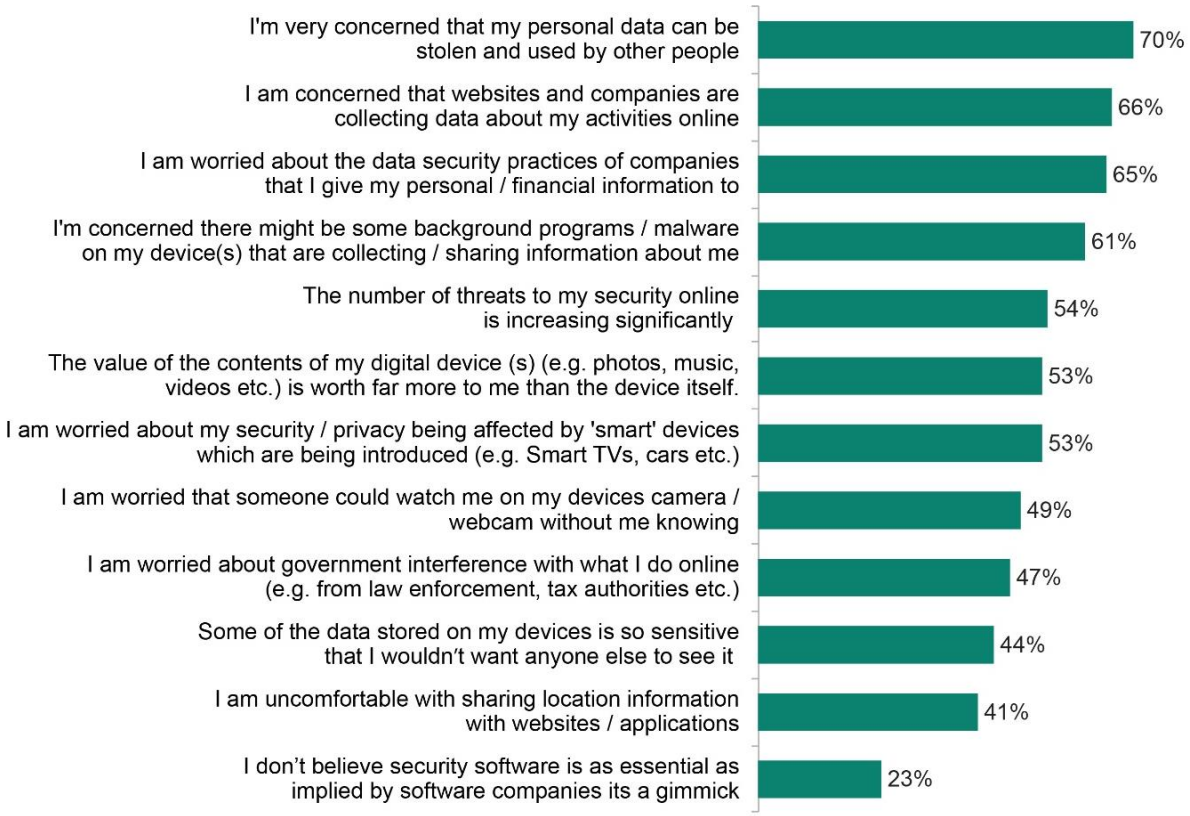
Those whose money was stolen online suffered an estimated median loss of $283. Globally, only around half (54%) of those affected managed to recover all their stolen funds, and a quarter (23%) didn't get any of it back.

Section 8. Awareness of risk

Half (46%) of consumers believe they are not a target for cyberattack; and only 55% is convinced that the number of threats to their online security is increasing significantly.

The study explored how consumers feel about their own cyber-safety. It found that despite the fact that many people feel they are not of interest to cybercriminals, nearly three-quarters (71%) are concerned that their personal data could be stolen and used by others. Two thirds worry about the extent of online data collection, the data protection offered by organisations they share their details with and the possibility of background malware collecting and sharing information direct from their devices.

The data collection and privacy risks of new ‘smart’ technologies are an emerging concern for 53% of respondents. Other concerns included the collection of location-based data, the vulnerability of data stored on devices or being spied on.



Awareness of current security risks

Of those aware of the top security issues, 68% worry about malicious software that can gather data or passwords from a device and about online account hacking. This is followed by concerns about financial threats targeting bank accounts (62%) and ‘phishing’ emails (61%). Adware annoys 54%. The same proportion is worried about software exploits

attacking vulnerabilities in their devices' software, although 24% admits to not really knowing what a software exploit is.

Other possible security concerns explored by the study include malicious software trying to access a device's webcam, a worry for 52% of respondents; ransomware – malicious programs that encrypt files and demands money to unlock them (a concern for 51%), malware targeting mobile devices (51%), and pornware - malicious programs that download explicit content without the user's consent (48%).

Not everyone is worried, however. Between a fifth and a quarter of respondents who say they are aware of each of the top security issues facing consumers today believe that there is nothing to be concerned about.

Threat	Not aware or partly aware	Aware but not concerned	Concerned and very concerned
Adware' Programs that collect information about browsing habits and launch ads - pop-up banners	17%	28%	54%
Malicious software that tries to access your webcam	20%	28%	52%
Global online espionage campaigns	27%	27%	45%
Denial-of-service (DDoS) attacks on company government sites causing temporary unavailability slowdown of websites	29%	27%	44%
Pornware' Malicious programs that downloads explicit content without the user's consent	26%	26%	48%
Data interception when you use Wi-Fi	20%	26%	54%
Phishing e-mails / websites that try to collect your details	14%	26%	60%
Malware designed - targeted at mobile devices (tablets — smartphones)	25%	24%	51%
Software exploits Attempts to compromise your device using vulnerabilities in its software	25%	22%	54%
Ransomware' Malicious programs that encrypts your files and then demands money to unlock them	28%	21%	51%
Financial cyber-threats targeting customer accounts resulting in monetary losses	17%	21%	63%
Online account hacking	14%	19%	68%
Malicious software that gathers data intercepts passwords on your device	14%	18%	68%

A significant number of consumers are aware of large scale business- and political threats such as global cyberespionage campaigns and denial-of-service (DDoS) attacks. This could be due to an increase in media coverage of such incidents. Even though the risk and impact of these threats may be far removed from consumers' everyday lives, they are a matter of concern to just under half of respondents (45% and 44% for cyberespionage and DDoS respectively). Having said that, 28% were not entirely sure what global cyberespionage was all about and 29% were unsure about DDoS attacks.

Worries about financial threats

People the world over worry about financial threats online and many respond with caution when visiting banking and shopping websites they are unsure of. Two-thirds (65%) worry about financial fraud, as well as their vulnerability when making payments online (54%).

This is leading many to look for evidence of additional security (59%), to avoid those sites that have recently experienced a security incident (58%), and even to abandon an online payment (43%). However, a significant and vulnerable proportion either takes no action (31%) or assumes it's the responsibility of their bank to recover any stolen funds (42%).

Just under half (48%) of consumers believe that the burden of online financial security is shared between them and their bank, while a quarter (27%) feels it's their own responsibility to keep their money safe online. However, most respondents agree that they would like to see greater security in online transaction and banking channels.

Three quarters (72%) of those who conduct financial transactions online do so through a web browser – and over half (52%) would welcome greater protection, as would a third (32%) of the one in three consumers that now rely on mobile banking applications.

Conclusion

The Consumer Security Risk Survey 2015 reveals the extent to which Internet-enabled devices and online activities have become integral to the lives of consumers across the world. However, the study also reveals a deep contradiction between what connected consumers understand and fear and what they do regardless of those fears.

Many consumers underestimate how vulnerable they can be and behave accordingly: failing to properly protect devices and data from theft or loss, or their families from online risks. Too many people still don't know how to spot a fake or compromised website or a fraudulent approach for payment credentials.

Addressing this must be a priority. We need to educate and support consumers so that they can fully appreciate how valuable their identity, information, and the data trail left by everything they do online is to others, including criminals – and the responsibility they have to protect this through passwords, anti-malware solutions, sensible online access and behaviours.

To help achieve this important goal, this year's study and report has focused not just on the main Internet activities and security risks, but on the very real consequences of exposure, loss, attack or infection, as experienced in the last 12 months by consumers across the world.

Kaspersky Lab is committed to helping people protect what matters most to them. Not just through its leading consumer security solutions, but through awareness and communication; empowering people to make informed decisions about their own safety and that of the people they care about. Together we can save not just *the* world, but *your* world.