KASPERSKY lab

CONSUMER SECURITY RISKS SURVEY 2016

CONNECTED BUT NOT PROTECTED

Contents

Introduction	2
Main findings	3
Methodology	4
Section one: Our devices and how we protect them	5
Section two: What we do with our time online	7
Section three: What we love to store on our devices	10
Section four: Cyberthreats and their consequences	13
Section five: Protecting what matters	17
Section six: Looking after our children	20
Conclusion	22

Copyright © 2016 Kaspersky Lab. All rights reserved.

INTRODUCTION

The Internet brings with it a myriad of opportunities. It makes the world smaller; allowing people to communicate in new and exciting ways, at any time and wherever they are. It makes information constantly accessible to people, which in turn is adjusting how they live their day–to–day lives, how they travel from A to B, and what they choose to remember. It's an attractive prospect, and it's easy to see why 40% of the world's population has an Internet connection.

Yet the Internet also offers opportunities to criminals. Some malicious parties are out to harm. Some are seeking financial reward. Others intend to steal identities, data, or even disrupt the lives of children and older relatives. To better understand the threats people face online, and how they protect what matters most to them, Kaspersky Lab, together with B2B International, has undertaken this global study. We have collected data from thousands of Internet users across the globe to assess how users behave online, what their concerns are, what issues they face and how they defend themselves against possible threats.

A bird's–eye view of consumer security

In conjunction with the study, this year we are launching the Kaspersky Cybersecurity Index, the first index to monitor and track the security status of consumers on a global scale, and make this information available to Internet users 24/7.

The Index analyses the consumer security data across three key indicators: the 'Concerned Indicator,' which shows the percentage of people who believe they may be targeted by a cyberattack, the 'Affected Indicator,' which identifies how many people have actually fallen victim to cyberattacks during the reporting period, and the 'Protected Indicator,' which shows the number of users who have installed security solutions on all devices they use to access the Internet. We plan to measure these indicators every six months, to provide the information needed to monitor the degree of risk to the average Internet user.

Our findings indicate that besides being aware of the threats online, people are failing to install security solutions on their devices, and they are behaving carelessly. This makes them easy targets for cybercriminals, and as a result, 29% have been affected by online threats.

Our goal is to help users understand the risks they are exposed to. Ultimately, we hope that our insights will help users protect what matters most to them as they become ever more connected.

See this link to find out more about the Kaspersky Cybersecurity Index.

Copyright © 2016 Kaspersky Lab. All rights reserved.

MAIN FINDINGS

Consumers are concerned about online threats to the people and things that matter most

- **70%** are aware and concerned about online hacking
- **64%** of people are worried about online banking fraud
- **44%** say the data stored on their devices is so sensitive that they wouldn't want anyone else to see it
- Yet only one–in–five **(21%)** consumers believe they are a target for cyberattacks

The dangers online can have severe consequences for people's data

- Overall, **29%** of people have been affected by online threats
- Malware is the biggest threat faced by consumers. **42%** have faced malware, with **22%** of them suffering from devices infected with malware as a result
- **17%** of people online have faced a ransomware threat, with **6%** becoming infected as a result. One–in–five users that pay a ransom don't get their files back

And children are also exposed to online threats

- Their kids seeing inappropriate content **(37%)** communicating with dangerous strangers **(36%)** and becoming victims of cyberbullying **(34%)** online, are top worries for parents
- **14%** of parents believe their children are addicted to the Internet
- **12%** believe their children are seeing inappropriate/ explicit content online
- Compared to last year, more parents feel they do not have any control over what their children see and do online

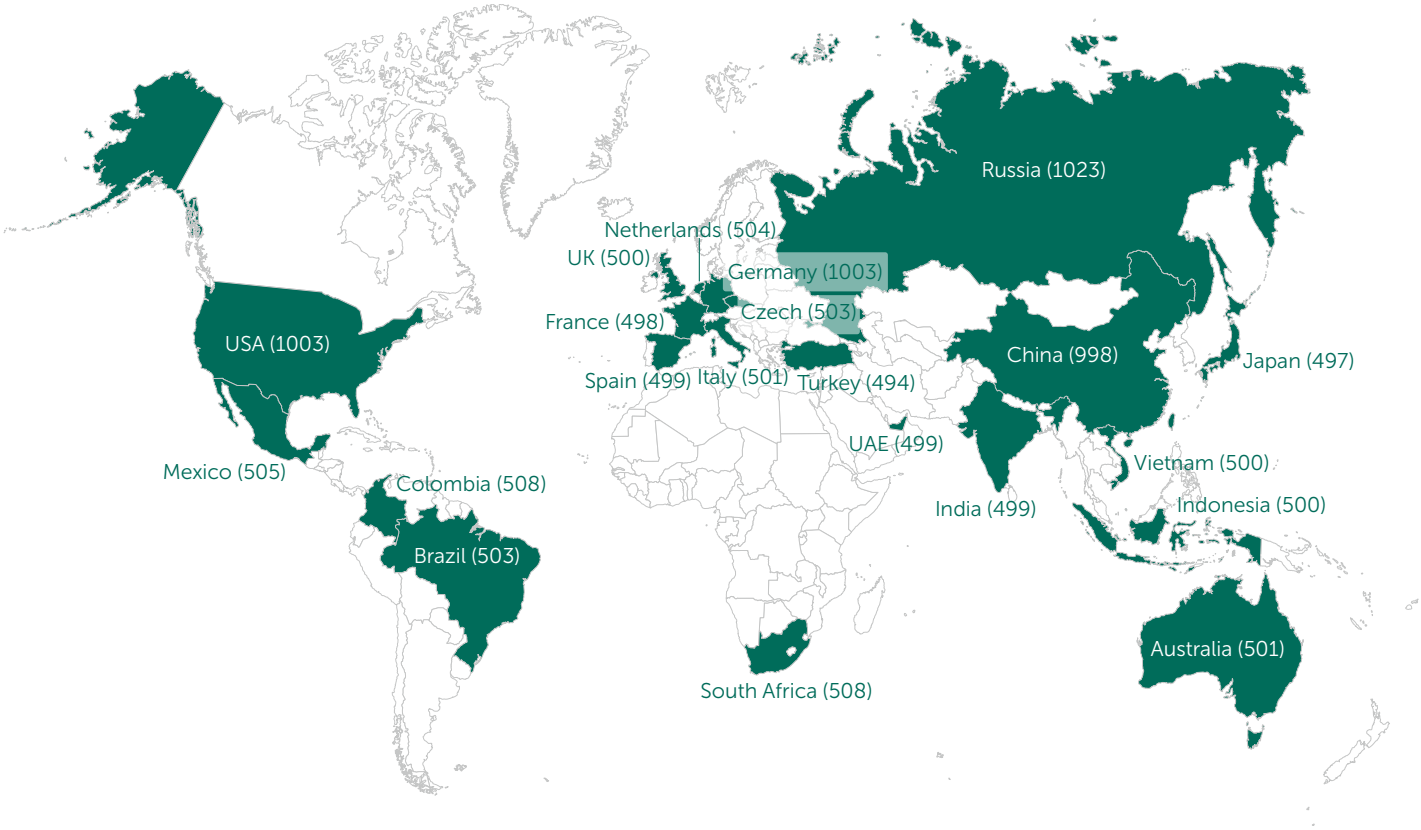
People should be more cyber savvy — and protect what matters most — when they are online

- Only **60%** use a security solution on every connected device they own
- **71%** use insecure public Wi–Fi in cafés, bars and fast food restaurants, with **15%** using it to shop, bank, or make payments online
- **51%** use insecure methods to remember passwords
- **22%** have accidentally disclosed confidential data or personal information to someone online
- Around a quarter **(23%)** believe security solutions are just a gimmick

Copyright © 2016 Kaspersky Lab. All rights reserved.

METHODOLOGY

The study was conducted online by B2B International in August, 2016. Users from 21 countries were surveyed online.



A total of 12,546 people, aged 16 and over, split equally between men and women, were surveyed.

28% were aged under 24, 26% were aged between 25 and 34, 19% were aged 35 to 44, 14% were aged 45 to 54. 13% of those surveyed were over 55s, with 7% aged 55 to 64, and 6% aged 65 or older.

Data was weighted to be globally representative and consistent. The 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.

Copyright © 2016 Kaspersky Lab. All rights reserved.

SECTION ONE: OUR DEVICES AND HOW WE PROTECT THEM

Relying on multiple devices to stay connected

Internet users go online with several devices, and every household has on average six connected devices. Almost all (98%) of respondents have computers at home (96% has Windows computers and 20% Mac computers). Slightly fewer (92%) people have mobile devices (88% has smartphones and 67% tablets).

Computers still remain the most popular method of going online, with 90% regularly using computers to go on the Internet. Smartphones (61%) are the next most popular devices used to go online, with Android smartphones (41%) used more regularly than iPhones (20%).

Devices tend to be owned and used by the same person, with 71% saying the device they mainly go online with, is only used by them. 25% share their device with other adults in the family and only 4% share their device with their children.

Failing to protect all of these devices sufficiently

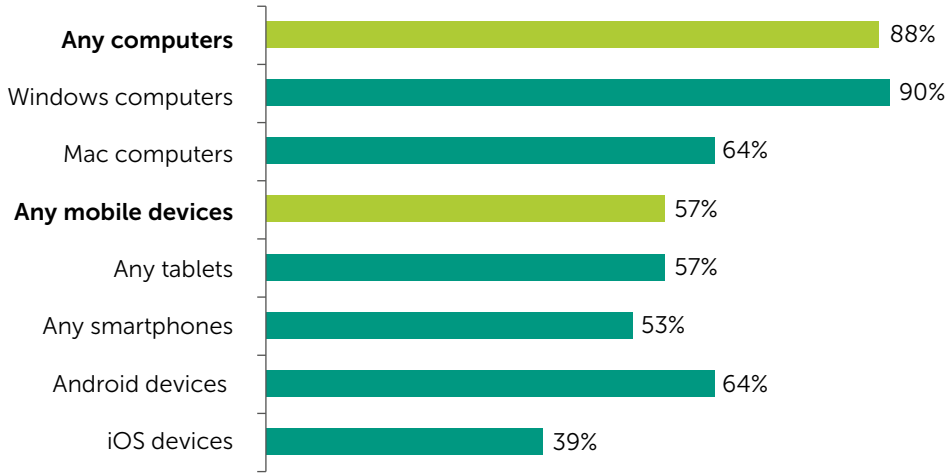
To measure and monitor Internet protection, the study asked respondents questions about the security solutions they have installed on their various connected devices.

86% use a security solution on at least one of their devices, but despite the fact that every device is vulnerable to threats, and can share threats with other connected devices, users are still failing to protect all of their end–points. Only 60% said they use a security solution on every device they own.

In particular, it is the mobile devices that are left least protected against online dangers. Only 53% of users have protected their smartphones with security software, 57% have protected their tablets, and 88% have protected their computers in this way.

Only 55% said they think their desktops and laptops definitely need IT security software for their protection, 42% feel the same about smartphones and tablets, and 32% about smart devices.

Devices used to regularly access the Internet that have antivirus / Internet security software installed



Copyright © 2016 Kaspersky Lab. All rights reserved.

The study also highlights a number of other methods users are taking to protect themselves online. For example, around a quarter (24%) said they cover their webcam to prevent people from hijacking it to spy on them, and 17% avoid using popular websites like Facebook and Google, because they are concerned these site gather information about them.

Using passwords in an attempt to protect devices

When it comes to protecting our devices with passwords or other authorization means, there is also room for improvement. Only 71% of respondents said they protect all of their connected devices with a password, and a worrying 22% said they don't protect any of their devices in this way, leaving their data open and vulnerable should any of their devices be lost or stolen.

It is encouraging to see that 81% have protected their computers with passwords and almost the same number have protected their smartphones. However, only 77% have protected their tablets with passwords.

Only 46% of users have protected their devices with both a password and a security solution, with just 67% of users protecting their computers in this way. The number is even lower for tablets and smartphones, with only half of these devices (46% and 45% respectively) being protected with the recommended combination of password and security software.

With so many people owning connected devices, and using these devices to go online, there is still a long way to go before all devices are protected effectively.

A combination of passwords and comprehensive security solutions is necessary to protect every device that's used to go online. When consumers don't protect every end point, they leave themselves vulnerable to cyberthreat.

Copyright © 2016 Kaspersky Lab. All rights reserved.

SECTION TWO: WHAT WE DO WITH OUR TIME ONLINE

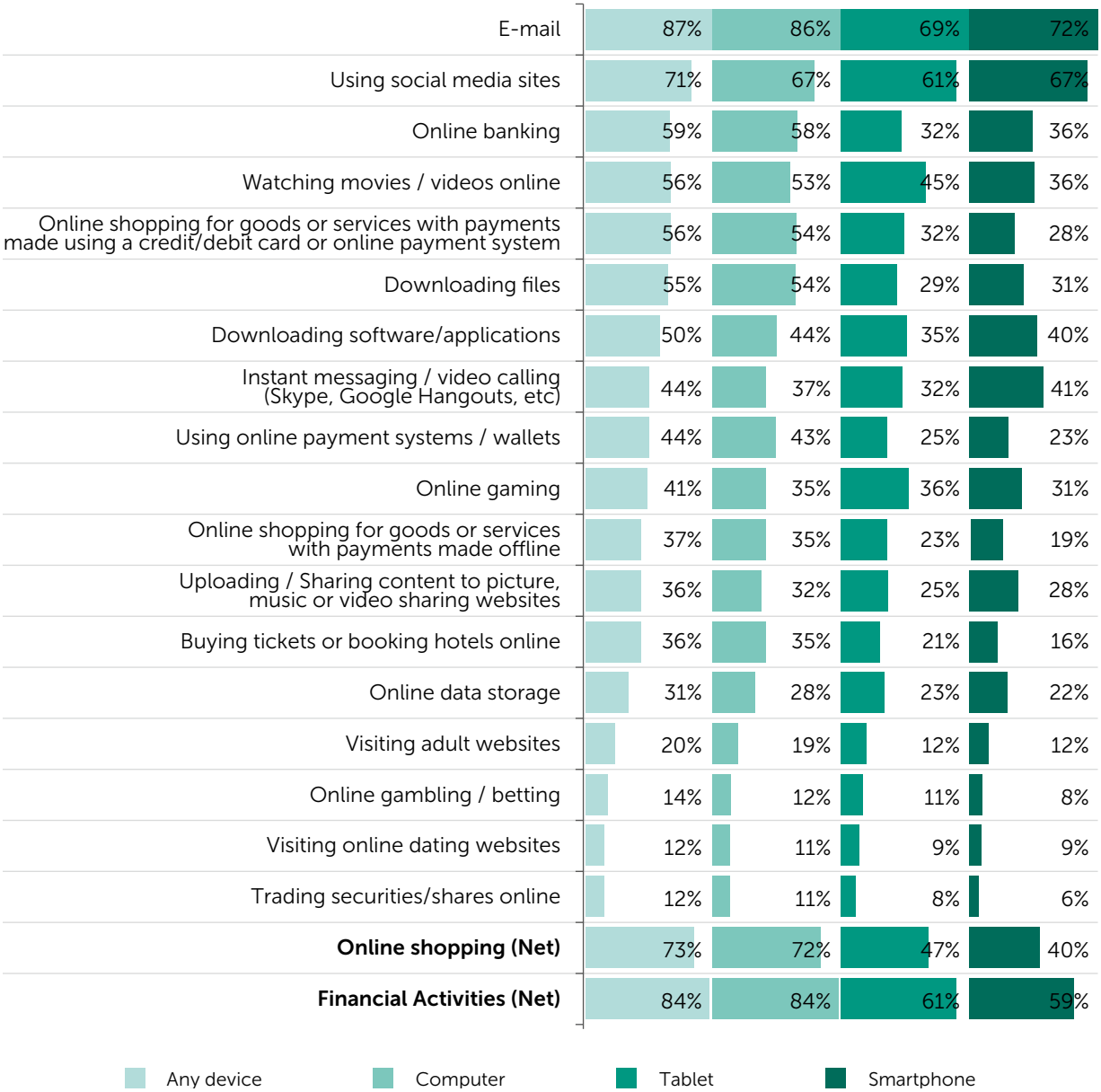
Spending time online

Consumers' primary online activities include emailing and social media. In addition to this, people tend to use their computers for banking and shopping more, but pick up their mobile devices for watching videos. Tablets meanwhile are most used for gaming, while smartphones are popular for instant messaging.

Men are more likely to watch videos/movies online than women (58% vs 54%) and men are also more likely to spend time gaming (45% vs 37%). However, women are more likely than men to communicate via social media online (75% vs 68%).

Assessing how people communicate online, both men and women are more likely to email, with 87% of respondents overall saying they regularly email online. Emailing is particularly popular with older generations. Almost all (94%) of the older Internet users surveyed said they communicate via email online, whereas social media sites are most popular with younger respondents 16–24 (79%).

Regular personal online activities by device type



Copyright © 2016 Kaspersky Lab. All rights reserved.

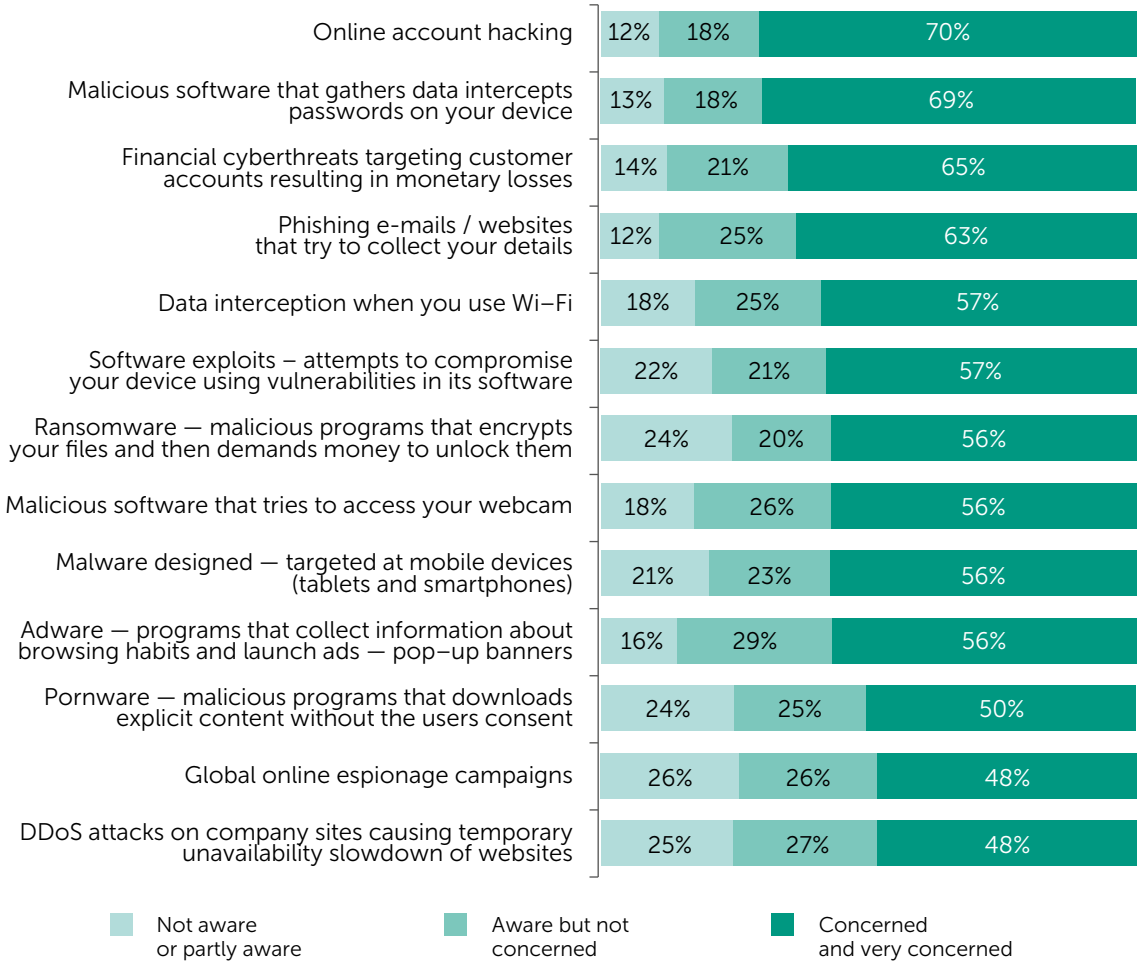
With the gap narrowing between people's work and consumer lives, the study shows consumers are continuing to use their work devices for their own online activities, exposing themselves, and their employers, to risk. For example, 17% use their work device for online dating services. Different generations use their work devices for different personal activities. The use of work devices for online shopping, using a credit or debit card, increases with the age of consumers (41% of 16–24 year olds do this, compared to 62% of 55 + year olds).

Aware and worried about threats

Questioning consumers about their online–woes unearthed a number of significant concerns, with only one–in–five (21%) consumers believing they are a target for cyberattack.

When asked what they know about online hacking, 70% of consumers said they know about it and it concerned them. Hacking therefore, is the threat that the largest number of respondents said they are aware and have concerns about. Regarding threats to their privacy, half (56%) said they were aware and concerned about the risk of someone watching them on their device's camera or webcam without them knowing.

Awareness and concerns about online threats



65% of Internet users are concerned about the risk of personal data being stolen online, a point that is especially important to, considering that for 44%, some of the data stored on their devices is so sensitive that they wouldn't want anyone else to see it, and for 51%, the value of the contents of their digital device (s) (e.g. photos, music, videos etc.) is worth far more than the device itself.

With the introduction of new connected technologies on the horizon, the cybersecurity industry should be aware of a consumer skepticism about smart devices such as connected cars and smart TVs. 51% of consumers said they are

Copyright © 2016 Kaspersky Lab. All rights reserved.

worried about the effects these developments will have on their privacy. This may be partly to blame for the fact that half (52%) of consumers feel the number of threats to their security online is significantly increasing.

Despite all of these concerns, consumers are leading these lives without making use of the security software that could alleviate their worries. Indeed, around a quarter (23%) even believe security solutions are just a gimmick.

But staying connected at any cost

Even though consumers are concerned about the safety of their data and the privacy of their lives online, they are happy to continue engaging with the online world at every opportunity, with 42% using free — but potentially insecure — public Wi–Fi to do so, and only 13% using a secure VPN connection.

People are connecting to public Wi–Fi in multiple locations. 71% of those surveyed, for example, admitted they make the most of public Wi–Fi in cafés, bars and fast food restaurants. However, it's not just the locations that's concerning, it's what they are doing when they are connected in this way. 13% of the consumers questioned said they use public Wi–Fi to access/use online data storage, 15% use it to shop, bank, or make payments online, 23% log onto websites and accounts without additional precautions, and a third use online messengers or make video calls (30%), or send and receive files (31%). These are sensitive activities and, without the appropriate protection, users could potentially be watched, monitored or intercepted by cybercriminals operating on the same Wi–Fi.

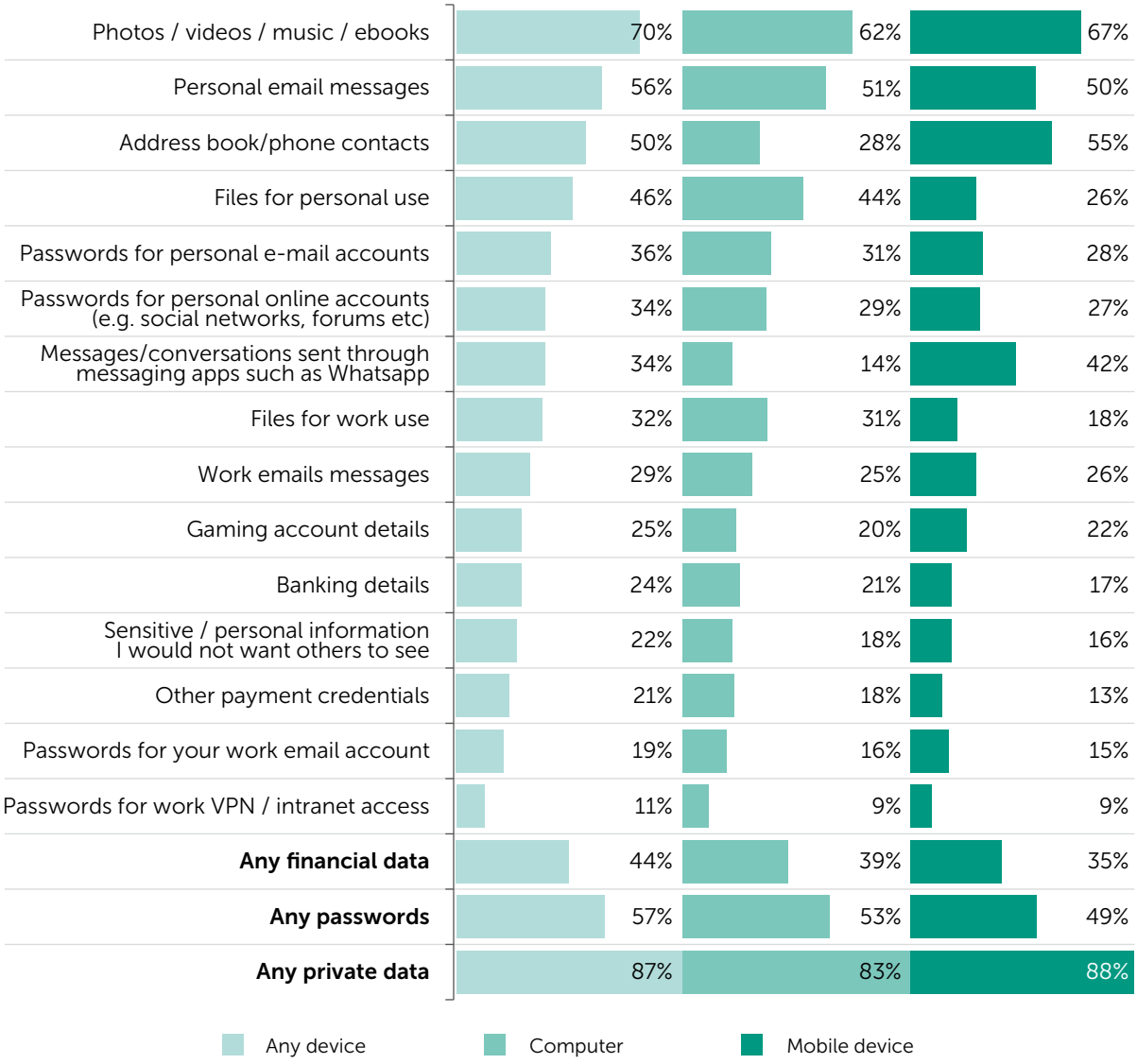
Copyright © 2016 Kaspersky Lab. All rights reserved.

SECTION THREE: WHAT WE LOVE TO STORE ON OUR DEVICES

Devices as the gateway to important and valuable information

With people using their devices for almost every aspect of their lives, the study demonstrates the variety of different data stored on the digital devices of consumers. We see that 9 in 10 users store some kind of private data on their devices, with 27% doing this on devices without a security solution and 17% without authorization in place.

The data consumers store on different devices

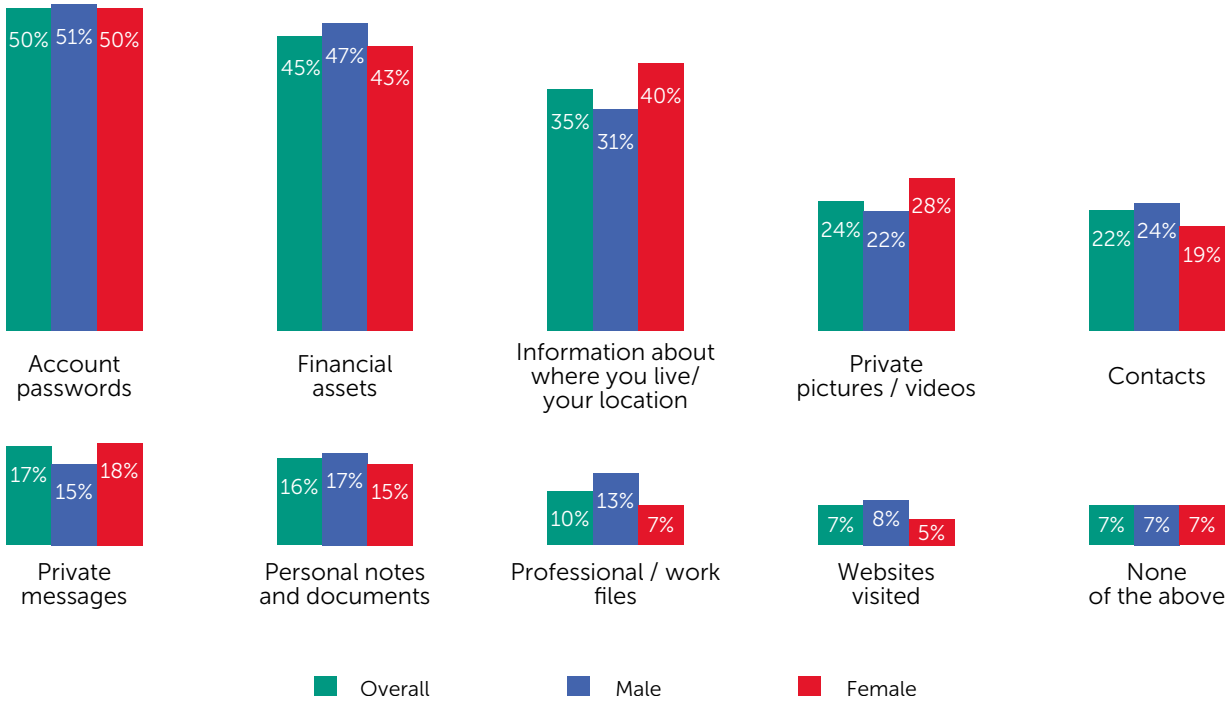


People place importance on the data their devices hold, putting particular emphasis on their photos, videos, music and eBooks — 45% of users said these were the most important things stored on their devices. Personal files are also considered to be important, with 20% of consumers saying that their personal documents, spreadsheets, to–do lists and materials related to their hobbies and interests were the most important information held on their devices. This is swiftly followed by files for work use, and banking details (both 17%).

Users said they were most worried about their account passwords being accessed by cybercriminals (50%), with this even coming ahead of financial assets (45%).

Copyright © 2016 Kaspersky Lab. All rights reserved.

The information consumers would be most concerned about cybercriminals accessing



The difficulties of recovering information

Consumers will find some information hard, or indeed impossible to replace, with consumers admitting that 13% of their files would be completely irreplaceable. 16% would never be able to replace the files they keep for personal use, and a worryingly high 27% would never be able to replace their photos, videos, music and eBooks.

Over half (56%) of consumers said they would be able to recover their banking information immediately, although for one–in–three (33%) this would take a few days. In addition, people are less confident about recovering sensitive or personal information than work–related data. 44% said they would be able to recover work files immediately, dropping to 40% for personal files.

The monetary value of information is also evident in the study. A calculation of the responses suggests that, on average, it would cost a consumer $674 to replace their digital assets if lost. If this happened, for example through the theft or hacking of their digital device, one–in–three consumers questioned (29%) couldn't be sure how much it would cost to replace their digital assets. It is a difficult figure to calculate but it is clear the value consumers place on their digital assets is high.

Sharing habits putting valuable data in danger

Despite consumers' love for their data, and a degree of anxiety existing around its potential theft, the study suggests there is a strong trend of people sharing their personal digital information through potentially insecure channels online.

Two–fifths of consumers have shared contact details online and a quarter (24%) have shared more detailed personal information. This habit also stretches to the sharing of anything private or secret (16%), data that contains personal information (15%), or financial details (9%).

The tendency to share important and personal data doesn't just put individual consumers at risk. One–in–ten (10%) said they have shared personal information about someone online and one–fifth (19%) have shared potentially compromising explicit information. Work–related data is also regularly put at risk, with a fifth (21%) of consumers admitting that they have shared workplace or commercial information.

Copyright © 2016 Kaspersky Lab. All rights reserved.

When sharing information online, consumers put a number of procedures in place, although not all of these methods are effective at securing data as it is shared from one user to the next — for example, the study shows that people attempt to reduce the risks involved with data sharing by keeping interactions with close family and friends separate from the interactions they have with other people, and by double–checking messages for personal information before they are sent.

The precautions taken by consumers, when communicating and sharing information online

Methods	Overall	16 to 24	25 to 34	35 to 44	45 to 54	55 or older
I keep interactions with close family / friends separate from other people	**40%**	40%	38%	38%	42%	43%
I double–check messages / posts before sending	**39%**	44%	41%	37%	34%	35%
I use high privacy settings to ensure only trusted people can see information	**35%**	39%	38%	34%	31%	28%
I delete my Internet history after sharing / sending information	**29%**	27%	30%	29%	31%	30%
I do not sign up to social networks / messengers if I think my personal data is at risk	**28%**	29%	25%	25%	27%	36%
I avoid sharing information when I am tired or under the influence of alcohol	**25%**	31%	25%	25%	23%	16%
None of these	**16%**	13%	14%	16%	17%	20%

People share their data online with a variety of other Internet users. Users are most likely to share personal data with friends (72%) and family (67%). Much fewer (34%) would share data with their colleagues but a surprisingly high one–fifth of users (22%) share their personal information in the public domain, exposing themselves to the whole online community.

When data sharing goes wrong, the consequences are far–reaching

22% of respondents in the study admitted that they have accidentally disclosed confidential data or personal information to someone online and the results vary from embarrassment to much more sever repercussions, such as lost jobs or damaged relationships.

The major consequences of having unintentionally shared information online

Consequences	Overall	16 to 24	25 to 34	35 to 44	45 to 54	55 or older
I embarrassed / offended someone	**27%**	30%	27%	27%	19%	23%
My personal / secret information became public knowledge	**23%**	18%	25%	25%	28%	30%
My relationships with a friend /family member was damaged	**21%**	20%	21%	31%	13%	9%
My financial details were stolen and I lost money	**19%**	10%	24%	20%	27%	26%
My relationship with my partner was damaged / we split up / got divorced	**16%**	14%	18%	20%	8%	10%
I damaged my employment opportunities / lost my job	**14%**	8%	20%	14%	12%	2%

Because of the personal importance of the data users store on their devices, sharing this data can get consumers into trouble. In order to avoid criminals or unwanted third–parties from accessing this private information, consumers need to ensure that when they do share data, it is shared securely, safely, and with consideration to the effect it may have on others.

Copyright © 2016 Kaspersky Lab. All rights reserved.

SECTION FOUR: CYBERTHREATS AND THEIR CONSEQUENCES

As we have already discussed, only 21% of consumers feel targeted by cyberattacks, and only around half are afraid of other risks — such as privacy breaches. Yet, 29% have fallen victim to cyberthreats, demonstrating that consumers are not concerned enough about the dangers they are faced with online. Certainly there's work to be done to encourage more people to use comprehensive security solutions and to behave safely online. With this in mind, it's important to assess the threats consumers face, and the impact of these threats.

The threat and consequences of malware

Malware has become the biggest threat faced by consumers. 42% have come across, or been targeted by malware online, with 22% of them falling victim to it as a result.

The source of malware infections vary for different consumers, with the highest number of infections originating from consumers visiting suspicious websites (42%). After infection, only 77% of malware sufferers have been able to remove malware completely and 36% have faced financial consequences, averaging at $121 as a result.

The source of malware issues

Sources of infection	Overall	16 to 24	25 to 34	35 to 44	45 to 54	55 or older
Visiting a suspicious website	**42%**	46%	45%	44%	39%	30%
Virus appeared on the device. Not sure how it got there	**29%**	26%	21%	24%	38%	48%
Fake app or piece of software	**22%**	28%	27%	22%	15%	9%
USB stick	**20%**	24%	26%	22%	11%	3%
An email or some other message from someone I don't know	**18%**	13%	17%	23%	21%	22%
Trusted website that had been hacked	**16%**	14%	20%	19%	15%	10%
From another infected device	**16%**	17%	23%	17%	11%	5%
An email or some other message from someone I know	**16%**	11%	18%	23%	14%	13%
Other	**2%**	1%	1%	1%	3%	5%

The effects of malware aren't just financial. As a result of infection consumers suffer from a variety of issues such as their devices slowing down (34%), and receiving suspicious e–mails (14%). For some users their devices are even more severely affected — for 13% their device stopped working completely.

The threat and consequences of ransomware

Ransomware should be taken more seriously by consumers. 17% have come across, or been targeted by ransomware online, with 6% of them falling victim to it as a result.

A quarter (24%) of users don't know about ransomware, and may therefore be ill–prepared to mitigate its risks. This is concerning because when their devices are infected with ransomware, 47% of Internet users have had all of their files encrypted and 26% have had a significant number of files encrypted. As a result, 18% lost almost all of their data and only 28% has been able to recover all of their files.

With ransomware there is a strong incentive to pay money to criminals — victims are locked out of their data and told that if they pay a ransom, they will get their data back. The study shows that 36% of ransomware victims do give in

Copyright © 2016 Kaspersky Lab. All rights reserved.

and pay the ransom, despite the fact that it is never guaranteed that they will get their data back. Indeed, 17% do not succeed in getting their files back, even after paying the ransom.

The data desires of cybercriminals

When it comes to accessing consumers' personal information, criminals use several methods to trick consumers into letting them in, with phishing remaining popular and effective for cybercriminals. Overall 20% of consumers have experienced a cybercriminal attempting to trick them into sharing personal or sensitive data, with 6% being successfully tricked by cybercriminals.

For 58% of consumers that have had their personal details shared, the root cause of their problems has been a fake email. 29% have first been contacted by a fake social media message, 28% have visited a fake website, 25% have received a fake phone call and 22% have received a fake instant message.

As a result, consumers have had private information, from payment details to account logins shared.

Details requested by cybercriminals

Details affected	Overall	16 to 24	25 to 34	35 to 44	45 to 54	55 or older
Payment Information	**34%**	29%	36%	35%	30%	43%
Online banking logins	**32%**	22%	30%	40%	39%	36%
Private, personal information such as your address/date of birth	**30%**	34%	27%	29%	34%	27%
E–mail account logins	**27%**	28%	28%	34%	22%	18%
Social network logins	**24%**	24%	27%	30%	18%	9%
Shopping site logins	**17%**	17%	22%	19%	12%	9%
Instant messaging / communication account logins	**15%**	15%	18%	21%	12%	2%
Some other type of private / sensitive information	**15%**	16%	15%	12%	11%	19%
Gaming account logins	**14%**	15%	18%	15%	8%	2%

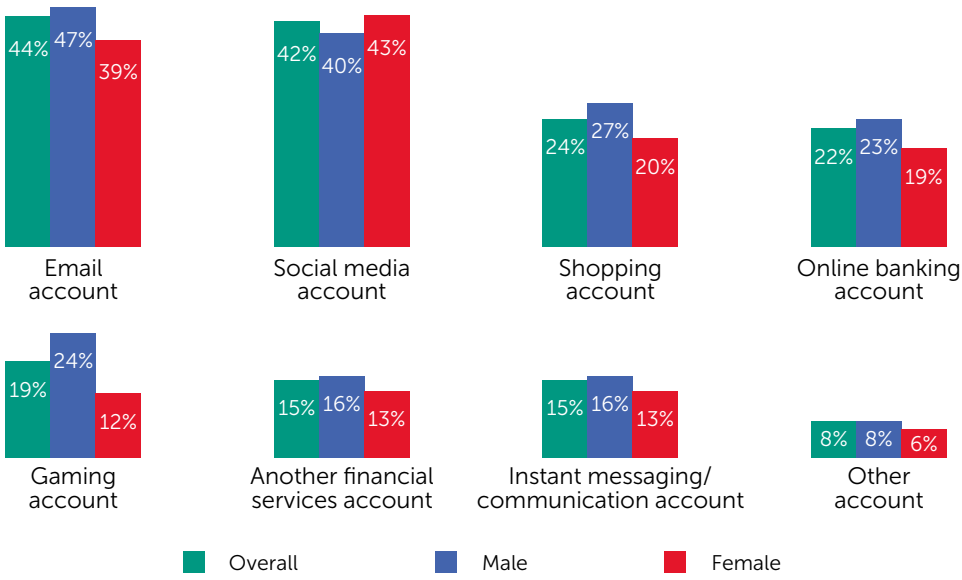
Hacking consumer online accounts

18% of consumers have experienced cybercriminals attempting to hack into their accounts, with 8% actually falling victim to the attempt. Accounts have most often been hacked when cybercriminals have guessed the password of their victims (40%). Around a third (30%) of those suffering from hacked accounts have had their login details stolen by malware. Around a fifth (23%) were tricked into revealing their login details, or the company providing the account was hacked.

A large number of different account types have been hacked, with the most commonly hacked being email and social media accounts. These accounts are almost twice as likely to be hacked as either shopping or online banking accounts.

Copyright © 2016 Kaspersky Lab. All rights reserved.

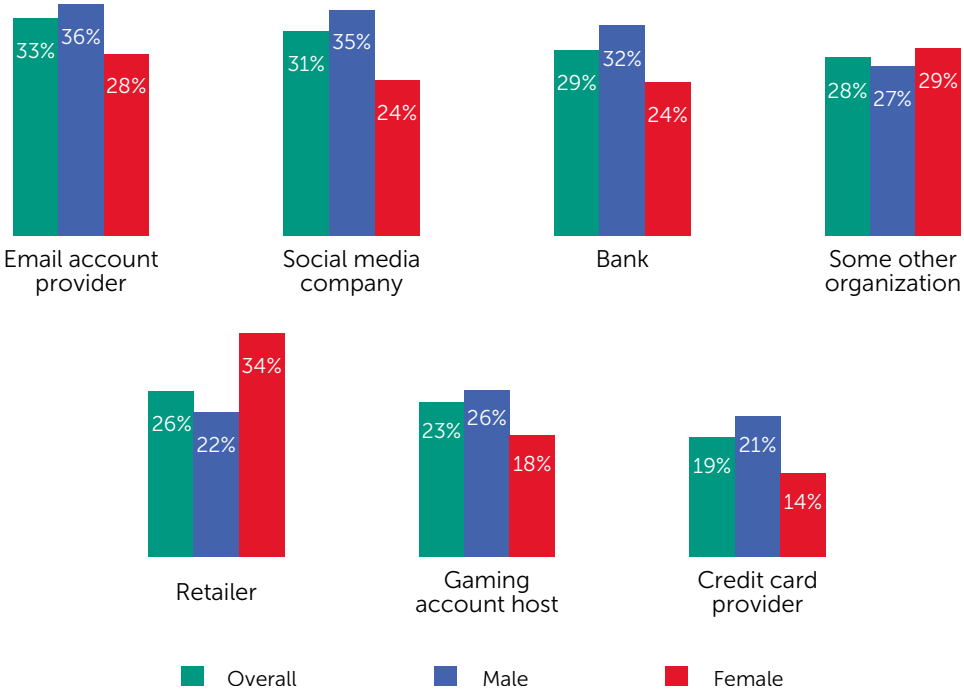
The consumer online accounts targeted in a hacking attempt



The threat of data leakage by third parties

Consumers have suffered data leakages from a number of different sources. 12% of people have experienced a third party attempting to leak or share their data inappropriately, and 5% have suffered from this. Email account providers are most likely to leak consumer data, but the rate of data leakage from institutions such as banks has been, for consumers, worryingly high.

Third parties that inappropriately shared/ leaked consumer data



Copyright © 2016 Kaspersky Lab. All rights reserved.

The inconvenience of online threats

Users have faced a number of inconveniences that have negatively impacted their experience of the online world in recent months, many of which, we believe are due to their lack of cyber–savviness.

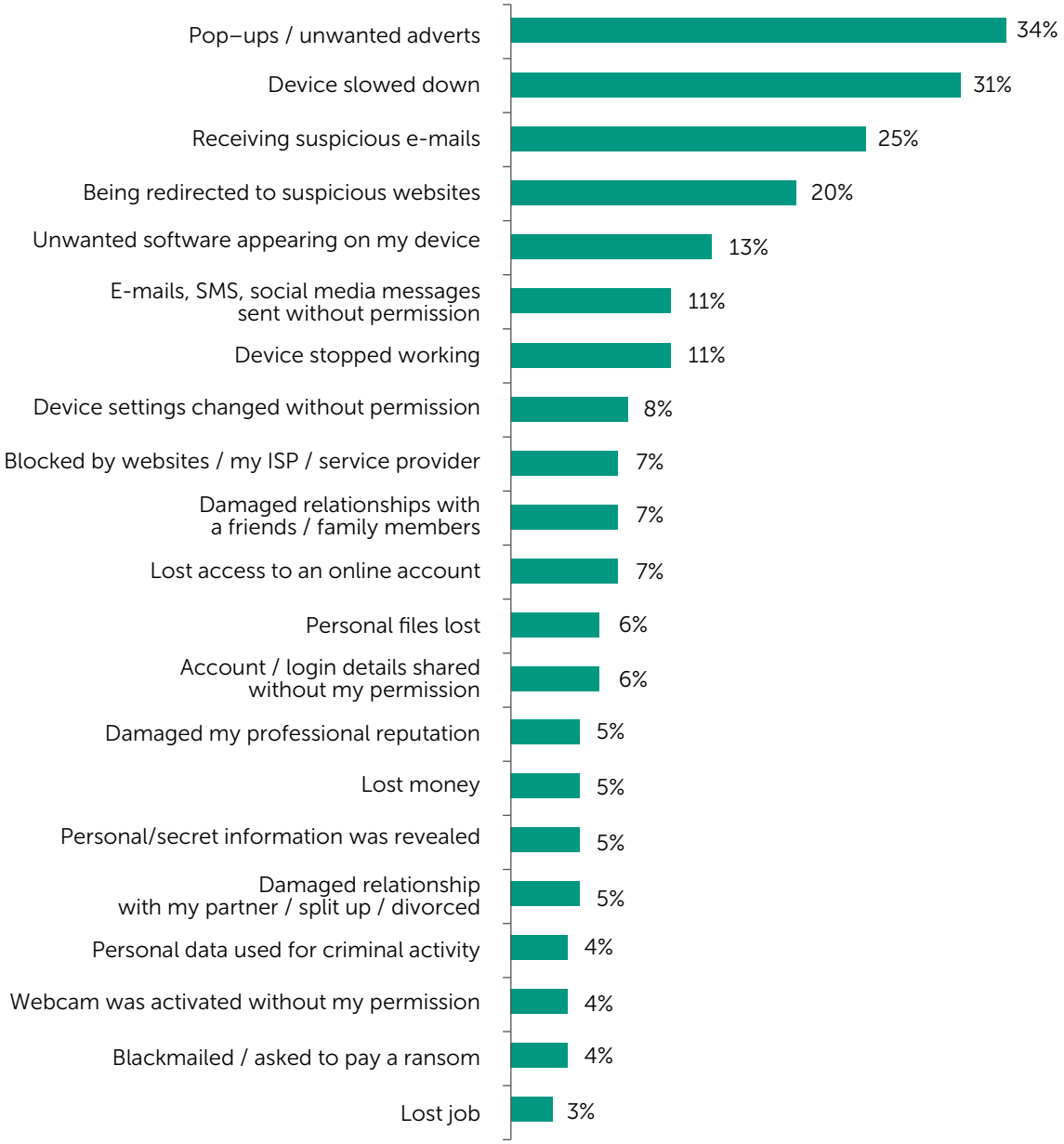
Adware, for example, has been playing a role here. 34% suffer from unwanted pop–ups and adverts, whilst 14% have experienced unwanted software appearing on their devices and 8% have had their device settings changed without their permission. Despite the issue affecting so many, 16% of users don't know what adware is.

And the consequences don't stop with unwanted software and adware. There are other inconveniences faced by users online, all of which consumers should be aware, and wary of, in order to understand why it's so important to protect their devices.

Following unwanted adverts, the second most common inconvenience experienced by users online is their device slowing down, followed by receiving suspicious emails and being redirected to suspicious websites. Although only 4% have had their personal data used in criminal activities, this is rather more than just an 'inconvenience'.

Worryingly, because people are failing to install security software on their devices, they are putting themselves at risk of suffering from these consequences unnecessarily, especially as they continue to do more online than ever before.

Problems experienced as a consequence of using the Internet



Copyright © 2016 Kaspersky Lab. All rights reserved.

SECTION FIVE: PROTECTING WHAT MATTERS

Bad user password habits get people into trouble

As already mentioned, people are most aware and concerned about online account hacking and value the passwords for their accounts highly. We can see that consumers are using passwords to protect what is precious to them. Yet, with so much important information at stake, it is important for us to assess password habits, in order to help consumers understand how to improve their protection. The study tells us that only 30% of consumers create new passwords for different accounts, and 1–in–10 use the same password for all of their accounts. Needless to say, this is putting consumers at unnecessary risk. If a cybercriminal was to gain possession of one of their victims' passwords, it's likely they will be able to use it to access several of that victim's accounts.

Taking a closer look at the passwords used by victims, the most popular option is to create passwords out of a combination of letters and numbers, with 64% of consumers using this tactic. However, the safest method, of using specialized software, is only used by 4% of Internet users.

Techniques used by consumers when creating new passwords

Techniques	Overall	16 to 24	25 to 34	35 to 44	45 to 54	55 or older
Combination of letters and numbers	**64%**	61%	60%	60%	68%	73%
Use UPPER and lower case letters	**47%**	47%	45%	44%	47%	52%
Use non–alphabetical / numeric characters	**37%**	33%	36%	38%	40%	39%
Avoid using dictionary words or names	**13%**	14%	13%	12%	13%	13%
Substituting numbers for letters	**11%**	12%	13%	9%	8%	10%
Creating passwords based on a mnemonic / acronym of a phrase	**8%**	10%	9%	7%	7%	7%
Spelling words backwards	**6%**	8%	9%	7%	5%	2%
Passwords are generated by specialist software	**4%**	5%	4%	4%	3%	4%
Some other technique	**2%**	2%	1%	1%	3%	2%
None of these	**12%**	12%	12%	12%	13%	13%

To understand their password decisions, we asked consumers about the password choices they make for different online activities. The majority agreed that online banking should have the strongest passwords, and less than 10% of people felt that online data storage, online gaming, online dating sites, and instant messaging/ video calling should have the strongest passwords.

Copyright © 2016 Kaspersky Lab. All rights reserved.

The online services that consumers think most need a strong password for

Accounts	Overall	16 to 24	25 to 34	35 to 44	45 to 54	55 or older
Online banking	**51%**	33%	51%	55%	60%	65%
E–mail	**39%**	44%	39%	39%	36%	35%
Online shopping	**37%**	28%	34%	35%	45%	49%
Online payment systems / wallets	**33%**	28%	34%	33%	38%	37%
Social media sites	**28%**	43%	28%	25%	21%	17%
Online data storage	**9%**	13%	10%	9%	7%	5%
Online gaming	**7%**	11%	8%	6%	4%	1%
Instant messaging / video calling	**6%**	10%	6%	7%	4%	3%
Online dating websites	**2%**	3%	3%	3%	1%	1%
Other service	**4%**	4%	4%	4%	5%	5%

Users are not as protective of their passwords as they should be, with many sharing them with others, and noting them down in inappropriate and insecure places. Just under a third (28%) has shared a password with a family member and one–in–ten (11%) has shared a password with friends.

This tendency to share passwords with others puts them at risk of being intercepted, or falling into the wrong hands. And bad habits are also evident in how people remember their passwords — with over half (51%) relying on insecure methods to do so.

Methods used by consumers to store passwords / password reminders

Methods	Overall	16 to 24	25 to 34	35 to 44	45 to 54	55 or older
I tend to remember my passwords	**53%**	59%	56%	52%	52%	41%
In a notepad	**22%**	20%	21%	20%	25%	29%
On a paper / sticker that is stored near the computer	**11%**	10%	11%	10%	12%	16%
Passwords are stored in the browser	**11%**	13%	12%	11%	10%	8%
Write down passwords in a file / document on your computer	**10%**	10%	11%	10%	9%	9%
Passwords are stored on my smartphone	**9%**	13%	10%	10%	5%	2%
Passwords are stored by specialized software	**7%**	6%	8%	7%	5%	7%
I e–mail passwords to myself	**6%**	7%	9%	7%	4%	2%
Passwords are stored in an online, cloud–based service	**4%**	6%	4%	5%	4%	2%
Other	**4%**	2%	2%	3%	5%	9%
Don't know	**7%**	8%	8%	8%	6%	7%

Copyright © 2016 Kaspersky Lab. All rights reserved.

Concerns don't stop people making financial transactions online

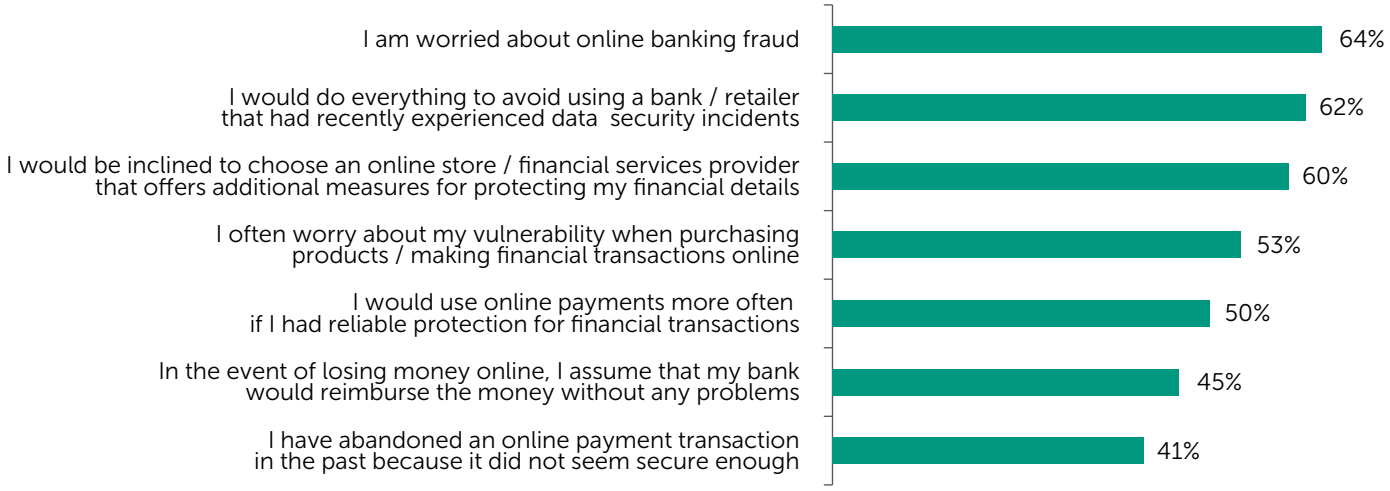
84% of consumers conduct financial operations — such as banking or shopping — on their connected devices, with 64% on their mobile devices.

Comparing results with last year's study, it is possible to see a shift in behavior when it comes to online transactions. Connected consumers are increasingly using smartphones, tablets and official banking and payment apps, with these overtaking computers browsers for making online transactions.

With people's banking lives becoming ever more connected, the security of banking log in details, passwords and data is essential. As we have already seen, half (51%) of consumers accept that their bank accounts require the strongest password in their password repertoire. But that priority needs to translate to other aspects of banking security too, especially as 44% of consumers admit that they keep financial data on their devices.

Consumers harbour several concerns about the security of their finances, with online fraud topping the list for 64% of people. Although it doesn't stop them, consumers feel vulnerable when they are making transactions online, and they seek ways to avoid putting themselves in danger by avoiding using banks and retailers that have recently experienced security incidents (62%) and abandoning online payments if they don't seem secure (41%).

Consumer concerns about security whilst completing financial transactions online



Consumer concerns about financial security are well–founded. 5% of consumers have lost money online as a result of scams or fraud, with the average sum lost reaching $476. Of those that have suffered, only 48% have succeeded in getting all of their stolen money back.

Copyright © 2016 Kaspersky Lab. All rights reserved.

SECTION SIX: LOOKING AFTER OUR CHILDREN

Parents lack control of their children's online safety

The Internet, as any parent knows, presents a wealth of opportunities for children. It allows them to communicate, learn develop, and discover new and interesting resources. The study shows us that around half (48%) of parents feel their children learn more about the world online than offline.

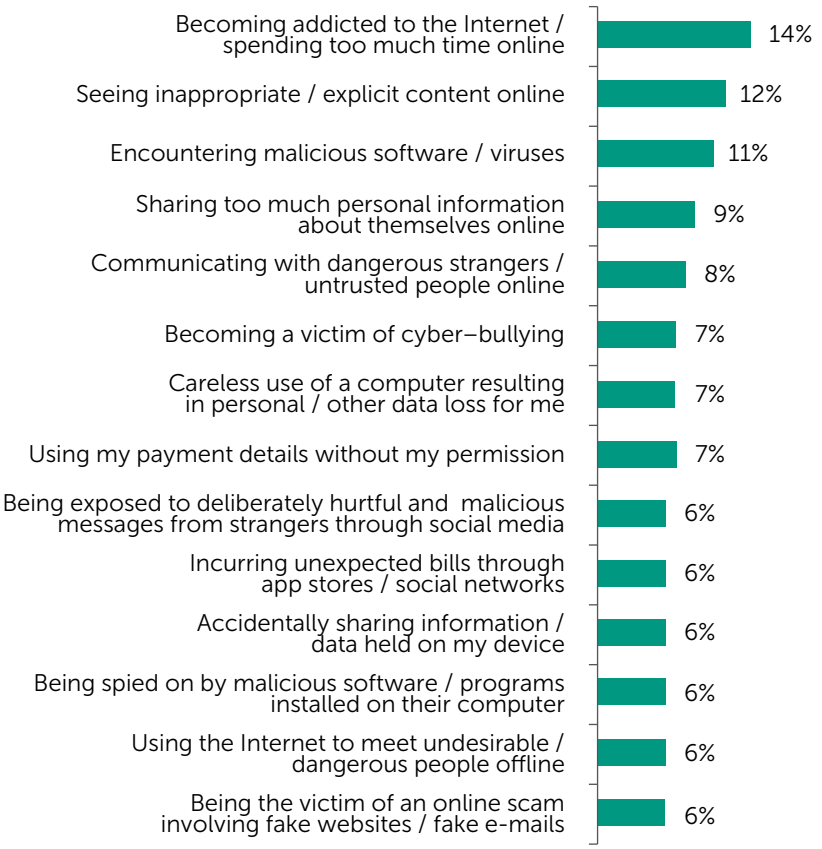
Yet the Internet is also concerning for parents, who worry about their children encountering the many dangers it contains, from seeing inappropriate, or explicit content, to accidently sharing data. The study also shows us that a third of parents (34%) feel that they do not have any control over what their children see or do online.

Parent concerns for their children online

These dangers are wide–ranging and naturally have varied consequences. Whilst accidentally sharing data can lead to parents' private or personal details being exposed, seeing inappropriate content or becoming the victim of cyberbullying can be severely damaging to a child's health — online and in the physical world.

Copyright © 2016 Kaspersky Lab. All rights reserved.

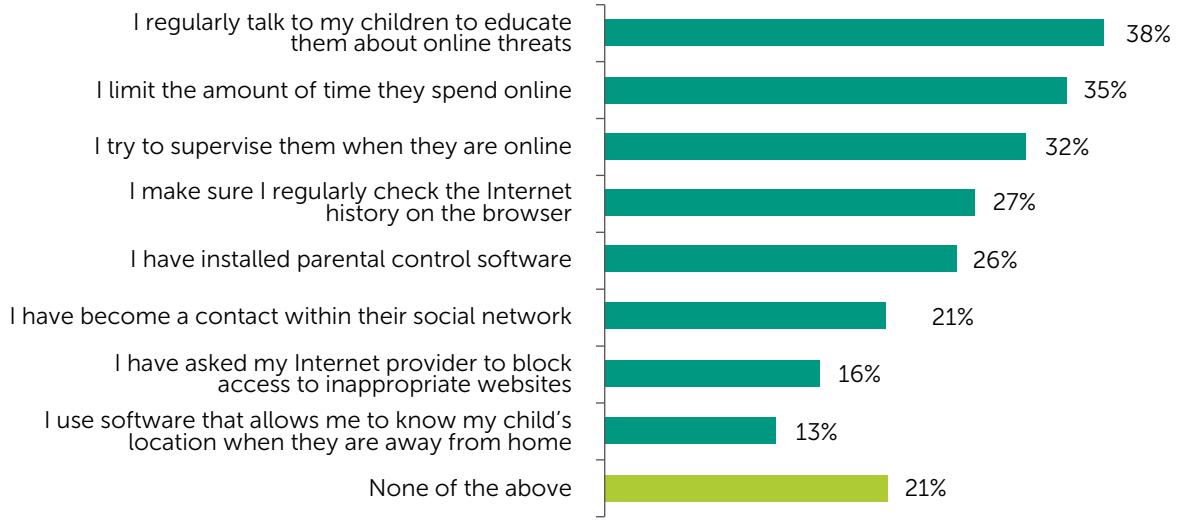
Threats and incidents that have happened to children online (according to parents)



But parents still aren't doing enough to protect their children online

Parents are taking a variety of steps to protect their children, although only a quarter (26%) use parental control software to help them in the process. Parents are more likely to regularly talk to their children (38%) about the dangers of the online world, bringing the Internet into family conversation and opening up forums for discussion. But even this is not enough. More parents need to be acting to protect their children from online threats, helping them to be cyber–savvy, and putting protection methods in place to keep them safe online, as they would in the physical world.

How parents protect their children from online threats



A horrifying 21% of parents not using parental control prefer to leave kids to just get on with their online lives themselves, and discover how to behave online independently, treating it as part of life outside the family home, away from parental supervision.

Copyright © 2016 Kaspersky Lab. All rights reserved.

CONCLUSION

This study, combined with the launch of the Kaspersky Cybersecurity Index, has come at a time when people are using their devices to connect all aspects of their lives. It shows us that people's concerns about the security of their devices are disproportionately low, considering the severe dangers posed by the online world and the high value people place on their devices. Indeed, the Kaspersky Cybersecurity Index has found that overall, a staggering 29% of people have been affected by online threats, yet only one–in–five (21%) of consumers believe they are a target for cyberattack.

These findings demonstrate a clear gap in people's understanding of the risks they are exposing themselves to online, and how they can effectively protect themselves, their data and their loved ones from harm; something that is particularly concerning when people value their devices and the data stored on them so highly.

Time and again, the report illustrates a lack of cyber–savviness among consumers. This is putting their valuable data at risk. Consumers share data insecurely, they conduct important transactions on public Wi–Fi and they treat their passwords irresponsibly. And whilst these habits persist, only 60% of consumers are protecting themselves with a security solution on every device they own.

These behaviors present multiple opportunities for cybercriminals to exploit precious data, target loved ones and seek financial or intellectual gain from their victims' losses.

At Kaspersky Lab, we are committed to helping people protect what matters most to them. That means building awareness, educating online users across the world, and helping them to move away from the Internet habits that endanger them, to live safer online lives. We develop leading security solutions to give people peace of mind, empowering them to enjoy every aspect of their connected lives without the worry.

Copyright © 2016 Kaspersky Lab. All rights reserved.