KASPERSKY lab

CONSUMER SECURITY RISKS SURVEY 2014: MULTI-DEVICE THREATS IN A MULTI-DEVICE WORLD

July, 2014

Contents

Introduction

The spread of the Internet to even the farthest corners of the Earth means that today, every third inhabitant of the planet is a global network user. However, just as in the real world, the virtual world has its advantages and its disadvantages. And crime is among those disadvantages.

The Internet is a source of cyber threats, which may affect both individual users and large corporations. Some criminals systematically attack large "targets", others prefer the "carpet bombing" approach, making just a small amount of profit but from a large number of victims. However, they focus their efforts on various popular operating systems. The more popular the platform, the more attention it attracts from criminals.

Attackers normally carefully monitor trends in information technology and quickly create new ways of accessing other people's data illegally, taking into account both changing user habits and new methods and devices for accessing the Internet.

In order to evaluate how Internet users react to online threats and how prepared they are for these, Kaspersky Lab, together with the independent company B2B International, regularly conducts global statistical studies. As part of these studies, users from different countries answer questions about their knowledge of current cyber threats and about incidents they may have encountered.

This year special attention has been paid to the needs of modern Internet users, such as the protection of digital identity and privacy, valuable financial and personal data, as well as multiplatform protection. Kaspersky Lab set itself the aim of finding out what worries Internet users most today and what actions they are taking or plan to take to protect themselves.

See this link for the report from the previous study.

Main findings

Multi-device is becoming the leading trend:

- 77% of respondents use multiple devices on different platforms
- 27% prefer to access the Internet on mobile devices
- Most users (92%) store sensitive information on all of their devices, including mobile devices

Users trust devices with data about their personal lives and this worries them:

- 58% of respondents are concerned that their personal data may be stolen
- 60% of users worry that they may be being spied on via their devices, including being looked at through a webcam
- 38% of respondents store highly sensitive information on their devices and are afraid that someone will see it

Financial threats are becoming more and more frequent:

- 80% of users carry out financial transactions of which 40% use mobile devices for this
- 43% of respondents have come across some kind of online financial threat with users of Apple devices being the most commonly affected
- 75% of respondents believe that banks, payment systems and online stores should provide them with special solutions for secure transactions on their endpoints

Children are the most vulnerable Internet users, which is also a danger for parents:

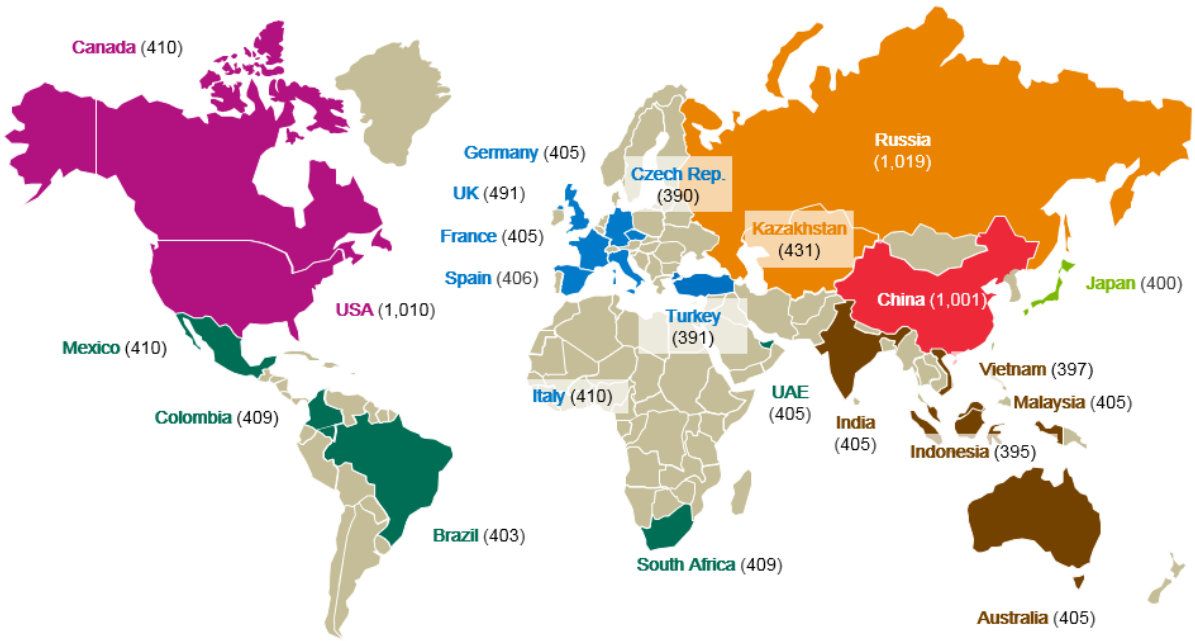
- 40% of adults believe that the number of online threats to their children is growing, while 22% feel that they cannot control what their child sees or does online
- Over the past 12 months, children of 21% of the respondents faced some kind of cyber threat on the web, and 20% lost adults' data or money

Users are worried about cyber threats but do little to protect themselves:

- Just over half of computers on the OS X operating system and mobile devices on the Android platform were equipped with security solutions
- Less than 80% of computers on OS X and Windows were password protected, and only 67% of smartphones and 57% of Android tablets had passwords
- Only 38% of respondents take precautions when using free public Wi-Fi networks

Methodology

The study was conducted via an online survey from May to June 2014 with users from 23 countries:



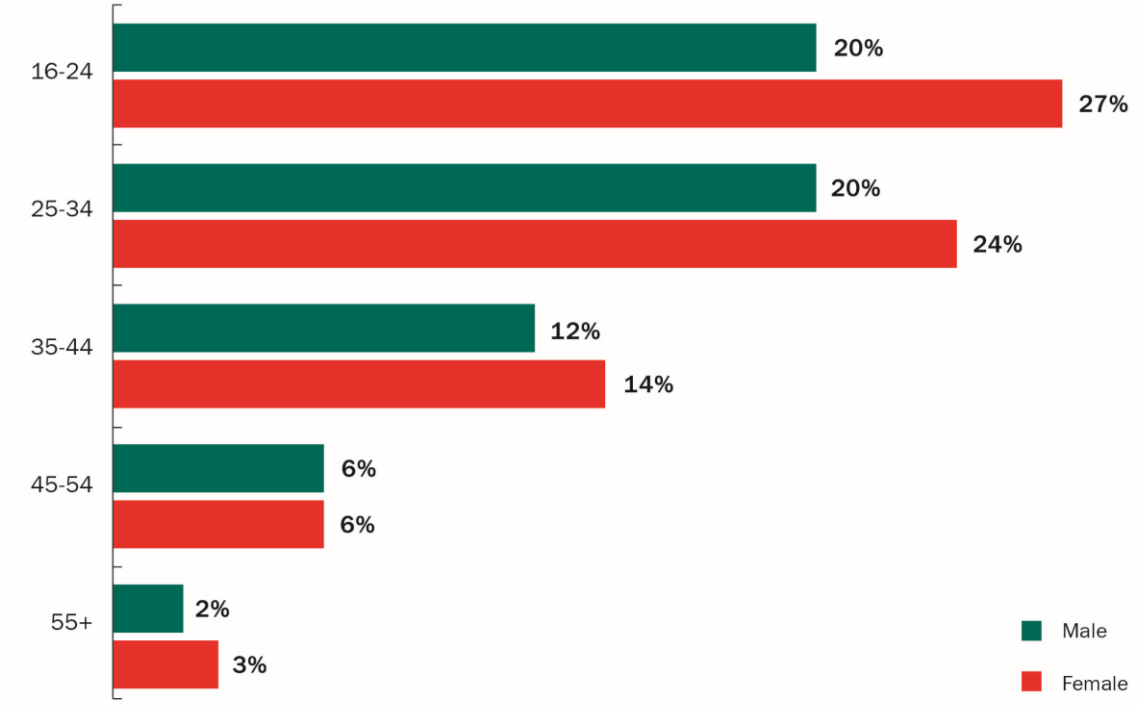
A total of 11,135 people aged 16 and over were surveyed. 51% were men and 49% were women. A quarter of respondents were young people aged under 24, 27% of users reported their age as between 25 and 34, 21% between 35 and 44 and 15% between 45 and 54. The older generation (55 or older) represented 12% of respondents.

It is important to note that the Internet in the People's Republic of China is very different due to state guidelines. The results from China were therefore excluded from the general worldwide data statistics in most cases.

Section 1. The use of different devices to access the Internet

First of all, participants in the survey mentioned the devices they use to go online. It was found that **77% of respondents use multiple devices on different platforms at the same time.** If we look at the devices they use to go online *most of the time*, we can see that 73% prefer traditional desktop and laptop computers, 16% smartphones and 11% tablets.

The highest numbers of study participants choosing a smartphone as their main gateway to the Internet live in the Middle East, Latin America and Asia (up to 27% of respondents from these countries most frequently go online from their smartphone). If we take a look at the demographic aspect, the highest number of people choosing a mobile format were young women aged between 16 and 34:

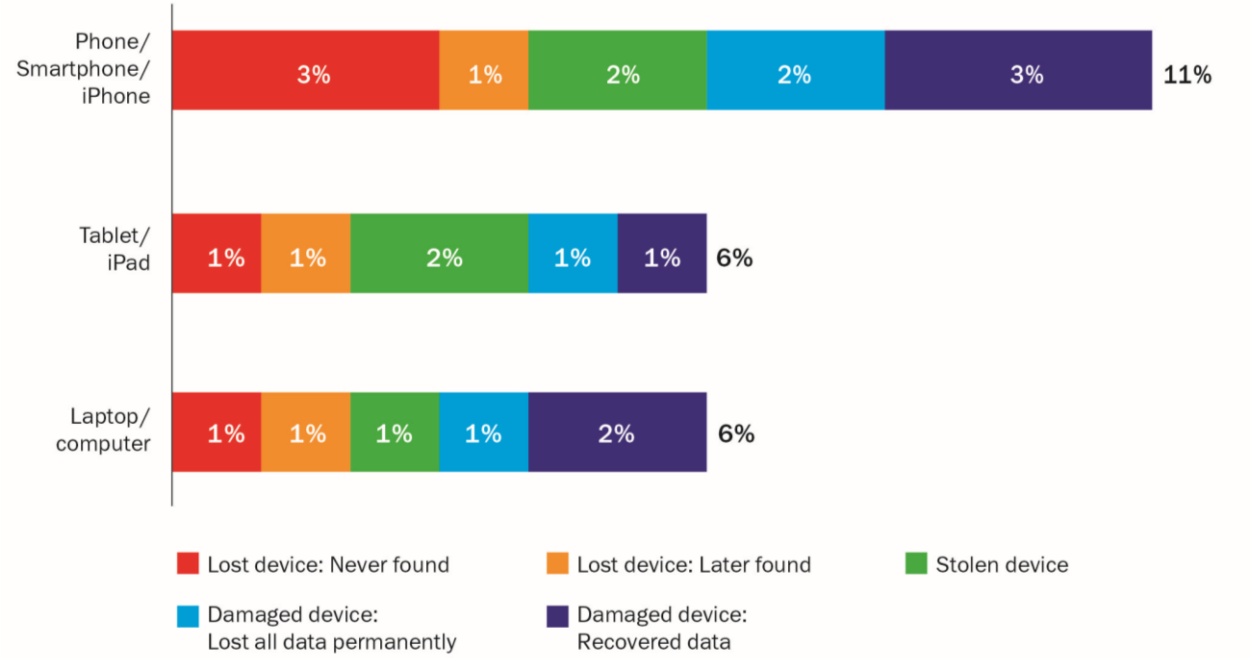


The study also showed that while users choose different devices to access the Internet, they don't worry about protecting themselves against online threats in the same way for all of these devices. For instance, 92% of users have installed a security solution for their Windows computer, but the proportion of protected desktop computers on OS X did not even reach 60%, and only 47% of respondents said that they had protection for their MacBook. Users of mobile devices are similarly unconcerned – **only 63% of tablets and 58% of Android smartphones are protected against cyber threats using special security solutions.**

But Windows OS is no longer the sole target of intruders. According to data from the Kaspersky Security Network, about 20,000 new malware samples for the Android OS are

detected every month in 2014, and a short while ago a network of Flashback bots on over 700,000 computers on OS X was disabled. Moreover, we must not forget about cross-platform threats, such as the semi-legal cyber espionage network Hacking Team, which has used spyware modules for iOS and Android.

However, it is not only cyber criminals who pose a threat to the data stored on users' devices. According to the survey, 12% of respondents reported their devices were lost, stolen or broken over the past year. The highest number of victims are young people aged between 16 and 24 (18%), and inhabitants of the Asia-Pacific region, China and emerging markets (28%, 27% and 25% respectively).



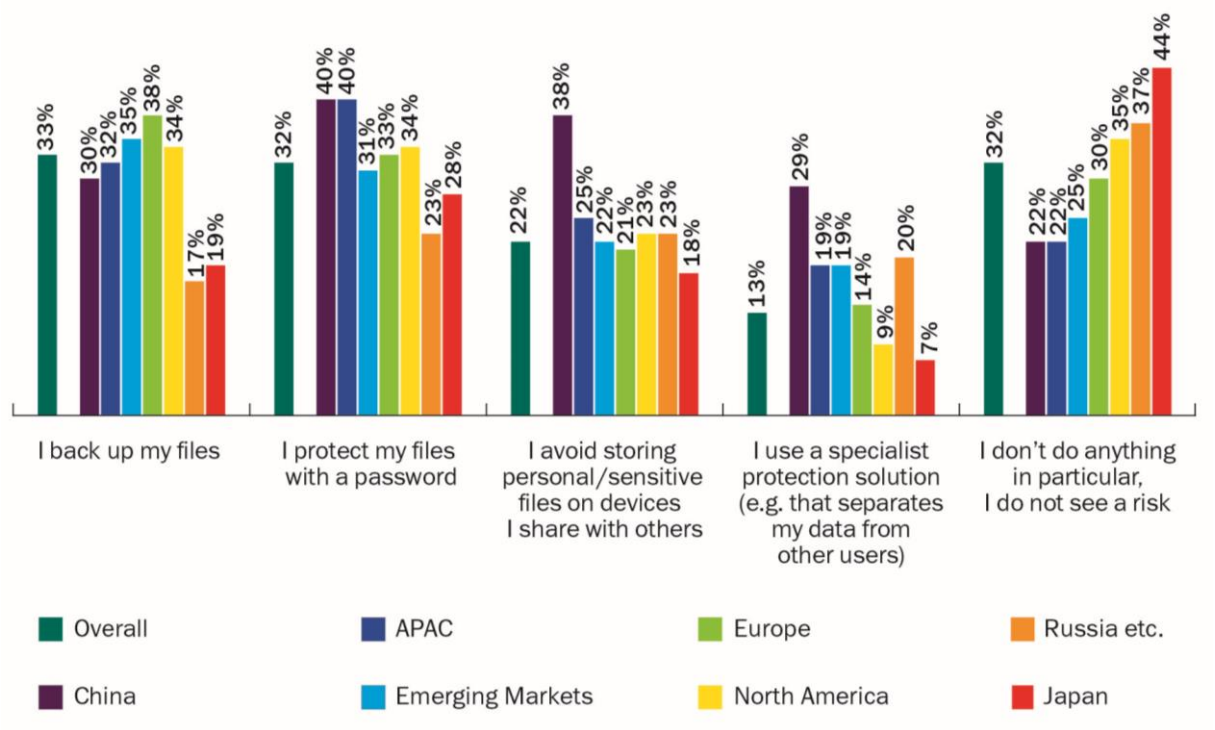
These kinds of incidents most commonly involve smartphones (11%), and less frequently tablets and laptops (6%). They are usually accompanied by the complete or partial loss of the data stored on them. Moreover, according to the respondents, **15% of the information stored on their devices is unique and, if lost, they would never be able to recover it.**

52% of users surveyed admitted that they value the data on the device more than the device itself. And **38% of respondents said that some of the information stored on their device is so confidential that they are afraid that someone might see it.** Most of these respondents live in Russia and China: 69% and 64%.

In this respect, the respondents were asked whether they protect their gadgets, for example, with a password (including graphical passwords). Only 80% of survey participants who used a computer on OS X use this simple protection method. The figure was even lower among Windows users – 76%. **The least careful respondents were Android smartphone and tablet users; 67% and 57% use passwords respectively.**

Furthermore, according to the survey, every third respondent shares their personal device with other people, for example family members, including their children, colleagues and

friends. 32% of these users do not take any further action to protect the device and/or the data stored on it as they do not see the risk. The highest number of unsuspecting users are found in Japan (44%), while the most cautious live in China and Asia-Pacific (in both regions, only 22% don't take protective measures).



However, sharing devices involves further dangers; the owner cannot be 100% sure of the computer literacy level of their children, family members or friends. What may seem to be an elementary precaution to some people may not even occur to others. A shared device can therefore make several users vulnerable.

Thus, the survey shows that the vast majority of respondents prefer to access the Internet on a variety of devices on different operating systems, but that they do not really worry about protection. Such carelessness puts the safety of their data and money at risk because, as we will see in the following sections, people put a lot of trust in their devices.

Section 2. Online user activity

Respondents were asked to indicate what they often do online and which devices they use. This year's list of options has been extended to cover as many user interests as possible. The proportion of some activities decreased as a result compared with last year's survey; this does not mean that users are now less likely to perform these actions, but it shows which activities are performed most often and therefore come to mind first. In general, the responses were as follows:

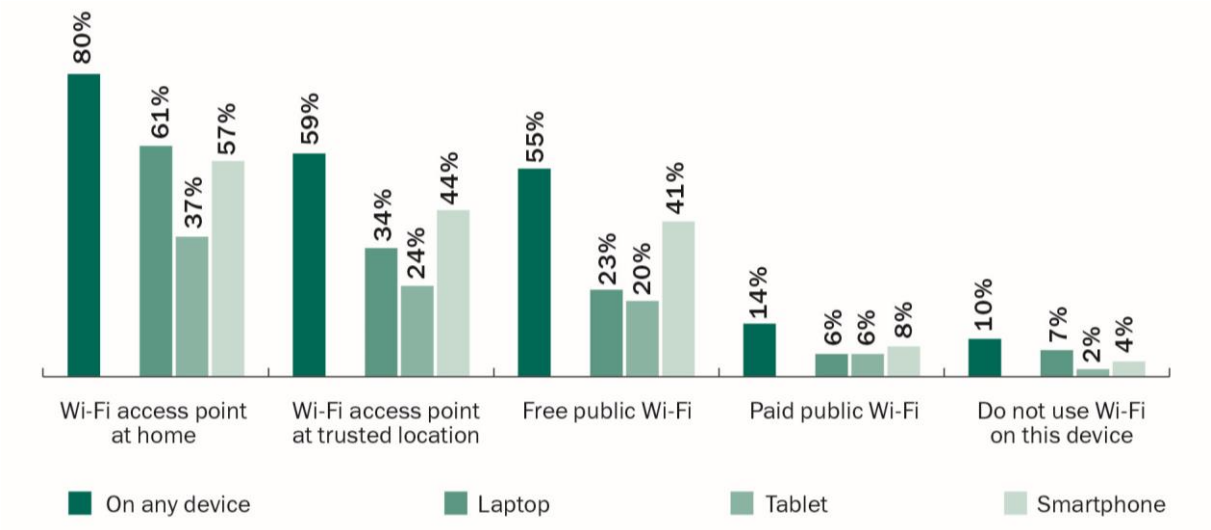
Activity	Any device	Desktop/ laptop	Tablet	Smart-phone	Any mobile device
Online shopping	66%	61%	16%	17%	27%
Online banking	62%	57%	13%	21%	27%
Online gaming	30%	22%	10%	12%	17%
Online gambling/betting	7%	5%	2%	2%	4%
Using social media sites	66%	57%	23%	40%	47%
Downloading software/applications	42%	32%	11%	20%	24%
Downloading media	45%	38%	10%	15%	21%
Online data storage	26%	22%	7%	10%	14%
Sharing content/data	42%	34%	10%	19%	24%
Instant messaging/video calling	45%	33%	13%	24%	30%
Visiting adult websites	15%	12%	3%	4%	6%
Using online payment systems	35%	31%	7%	9%	13%
Visiting online dating websites	8%	6%	2%	3%	4%
Watching movies/videos online	46%	38%	15%	13%	24%
Listening to music/radio	55%	42%	15%	30%	36%
Email	90%	83%	29%	51%	60%
Education/learning	36%	31%	10%	10%	16%
Working	48%	44%	9%	13%	18%
Reading news, articles, books, etc.	68%	57%	23%	30%	42%
Any financial activity	**80%**	**75%**	**22%**	**30%**	**40%**
Any activity	**98%**	**94%**	**40%**	**64%**	**73%**

As can be seen from the table, email has not lost popularity among Internet users – 90% regularly check and send emails from their devices. Second place goes to reading (68%), and third place was shared between online shopping and social networking (66%). Social network activity on mobile devices was higher, coming in second place after emails while reading came third.

80% of users used their devices to make financial transactions (electronic payments, online purchases, etc.), with 40% using mobile Internet for this. Cyber criminals also pay attention to mobile platforms: according to Kaspersky Security Network, which receives

information about cyber threats from around the world, the number of malicious programs designed to steal financial data from Android devices increased by 14 times last year.

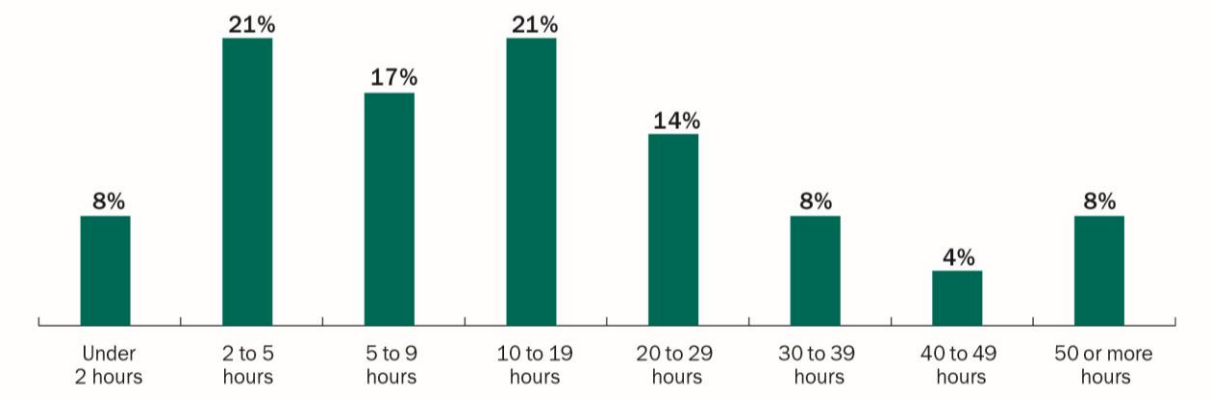
Due to the fact that most modern devices are equipped with wireless modules and, according to ABI Research, more than 4 million free Wi-Fi zones appeared in 2013 alone, it would also be interesting to know how people use Wi-Fi connections to do things online. The survey confirmed that the vast majority of respondents (90%) use Wi-Fi networks, and this percentage is even higher for tablets and smartphones: 98% and 96% respectively.



Half of the respondents (55%) regularly use free public Wi-Fi networks and smartphone users are most active in this respect (41%). For comparison purposes, only 23% of respondents connect to the access points from their laptops, and 20% from their tablets. This may be due to two factors. Firstly, it is much faster and easier to connect to any free Wi-Fi network from your smartphone on the go, while tablets or laptops require more time to be used as a spontaneous workplace. Another factor may be the users understanding of the risks associated with accessing free Wi-Fi. In order to confirm or refute this hypothesis, respondents were asked whether they have used any additional security measures in these circumstances.

It was found that only a third of users limit their online activity when connected to free Wi-Fi, even fewer (8%) increase the device's protection settings. At the same time, **12% of public Wi-Fi users log in to social networks, email and other sites, and another 6% make financial transactions or purchases online, thus endangering their data and money.**

The survey participants also reported how much time they spend on the Internet *at home*: 38% of users spend between 2 and 9 hours per week on the Internet (approximately one hour per day), 35% spend between 10 and 29 hours per week online and 20% spend more than 30 hours online (more than 4 hours per day).



Young people aged between 16 and 24 spend the most time online: 12% of them spend more than 50 hours a week on the Internet. Residents of Russia and the emerging markets spend the most time on the Internet (18% and 11% selected this option respectively).

With such active use of the Internet and its many services, the users' devices inevitably contain data, some of which can be classified as critical to security, which will be discussed in the next section.

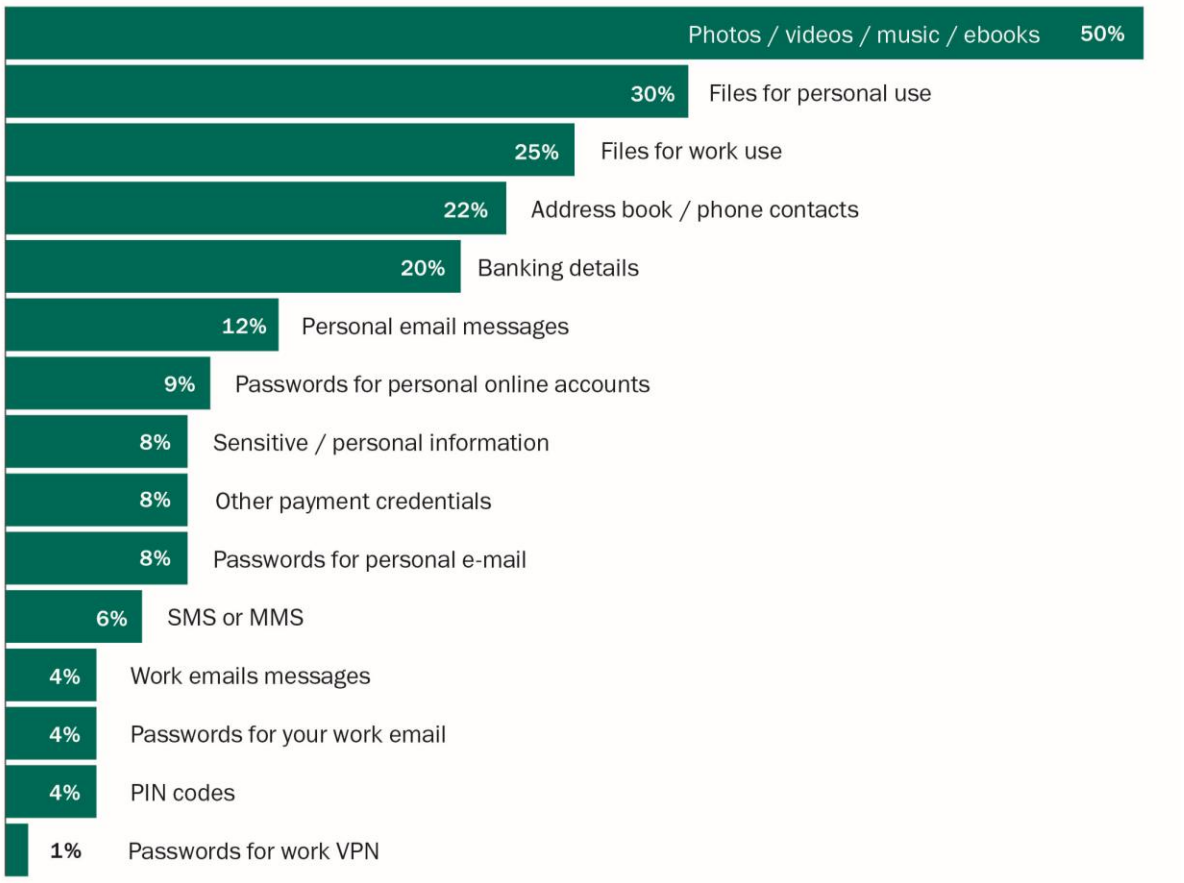
Section 3. Data stored on devices and attitudes towards this data

The study showed that **92% of users store private information on their devices,** the theft or loss of which may pose a serious risk. A third of respondents store financial data (bank or payment details, PIN codes), and 43% store login details and passwords for accessing email, social networks and other profiles:

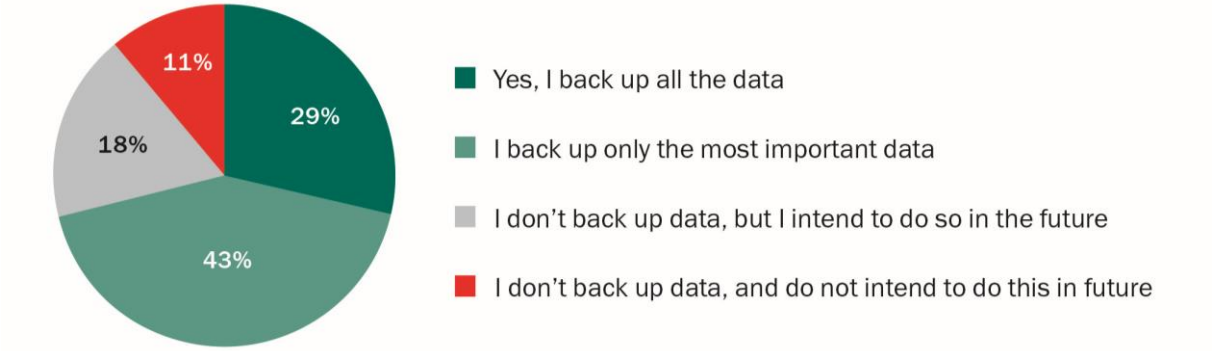
Data	Any device	Tablet	Smart-phone	Desktop/ laptop
Photos/videos/music created by you	79%	60%	68%	71%
Personal email messages	68%	49%	55%	61%
Address book/phone contacts	61%	36%	69%	36%
Files for personal use	61%	27%	23%	59%
Files for work use	46%	18%	12%	45%
SMS or MMS	42%	21%	60%	0%
Work email messages	38%	23%	28%	34%
Passwords for personal email accounts	31%	16%	18%	26%
Passwords for personal online accounts	28%	14%	17%	23%
Sensitive/personal information	27%	11%	13%	23%
Other banking details	22%	10%	11%	18%
Passwords for your work email account	17%	9%	9%	14%
Other payment credentials	16%	7%	7%	14%
PIN codes for online banking/payment systems	15%	7%	11%	10%
Passwords for work via VPN/intranet access	9%	4%	4%	7%
Any financial data	**30%**	**15%**	**19%**	**25%**
Any passwords or account logins	**43%**	**25%**	**30%**	**38%**
Any private/personal data	**92%**	**80%**	**91%**	**88%**

It is worth noting that financial data, login details and passwords were more frequently used on traditional computers, while personal files were used on smartphones, which may be explained by the fact that phones now serve as a convergent device with rich functionality including, for example, a camera. However, the percentage of users storing information of interest to cyber criminals (financial data and passwords to their accounts) on mobile devices is also quite high. At the same time, smartphones are more likely to be vulnerable to attacks, as shown in previous sections.

According to the survey, users say that their media files are the most important for them (50% of respondents chose this option), with personal files (30%) and work documents (25%) coming second and third. Banking data only came fifth (20%), while only 9% of users selected passwords. These statistics suggest that most users value the importance of the data stored on their device from an emotional point of view rather than looking at how useful this data could be to cyber criminals.



Despite the fact that precious memories and the fruits of intellectual labour are priorities for the users, only 29% confirmed that they backed up all of their files. The smallest number of users doing so live in China (12%) and Russia (13%). In contrast, 11% of all respondents said that they do not back up and do not plan to do so in future, and in Russia the portion of such users was 22%.



87% of those who still back up their files use physical media such as external hard drives (79%), as well as CDs and DVDs (8%), with only 12% using cloud storage. 88% of those who use cloud storage also synchronise all or part of their devices using this method.

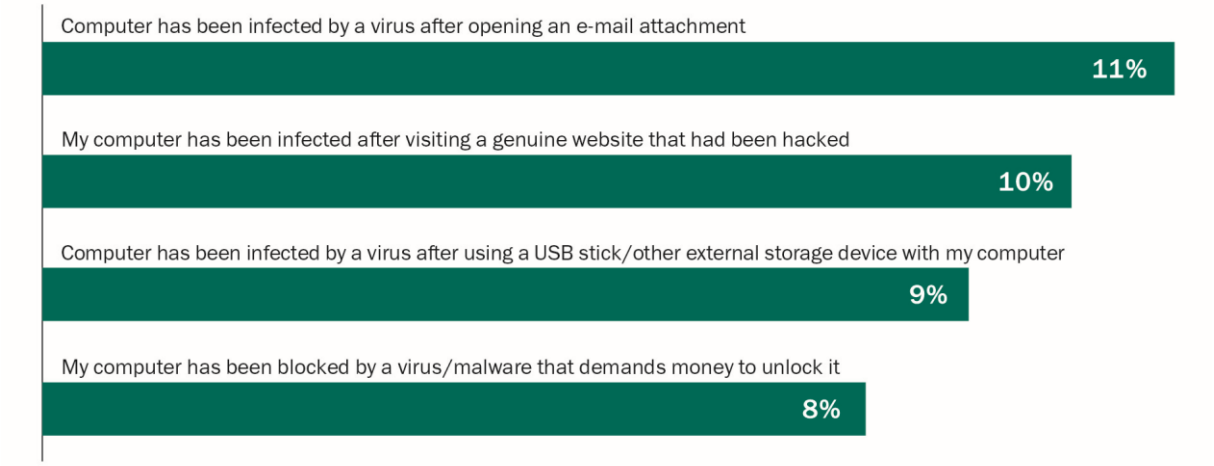
Significantly, **24% of respondents using physical media to back up lost their data at some point** because the media had been damaged (10%), stolen (3%), lost (10%) or had become unreadable (8%). However, despite the risks associated with physical media, many users do not trust cloud storage – 22% of respondents are not sure that their data will be safe, and another 31% would not save their most important files using cloud storage because they are scared of leaks.

The following section will describe the cyber threats that users currently face.

Section 4. Cyber threats faced by users and their implications

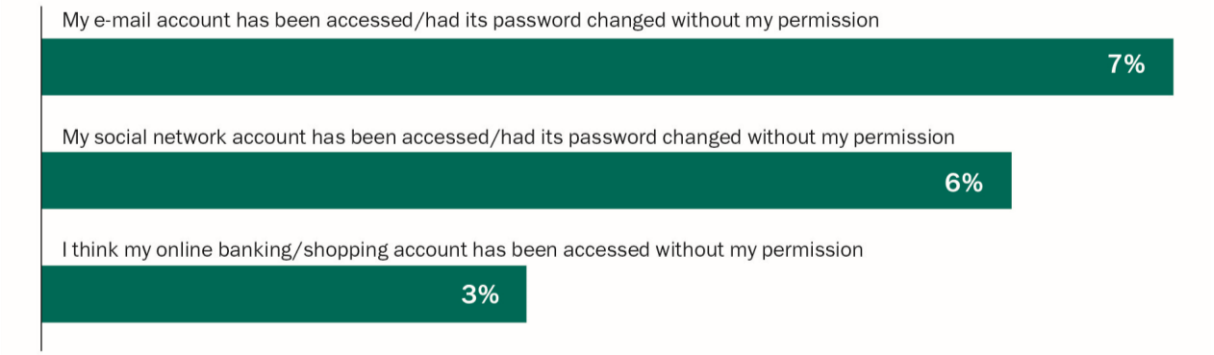
Respondents described the dangerous situations they had faced on the web over the last 12 months, and rated how negatively this had affected them. B2B International experts then calculated the average cost of "successful" cyber attacks for users.

- **31% of respondents admitted that their device had been infected by malware**:

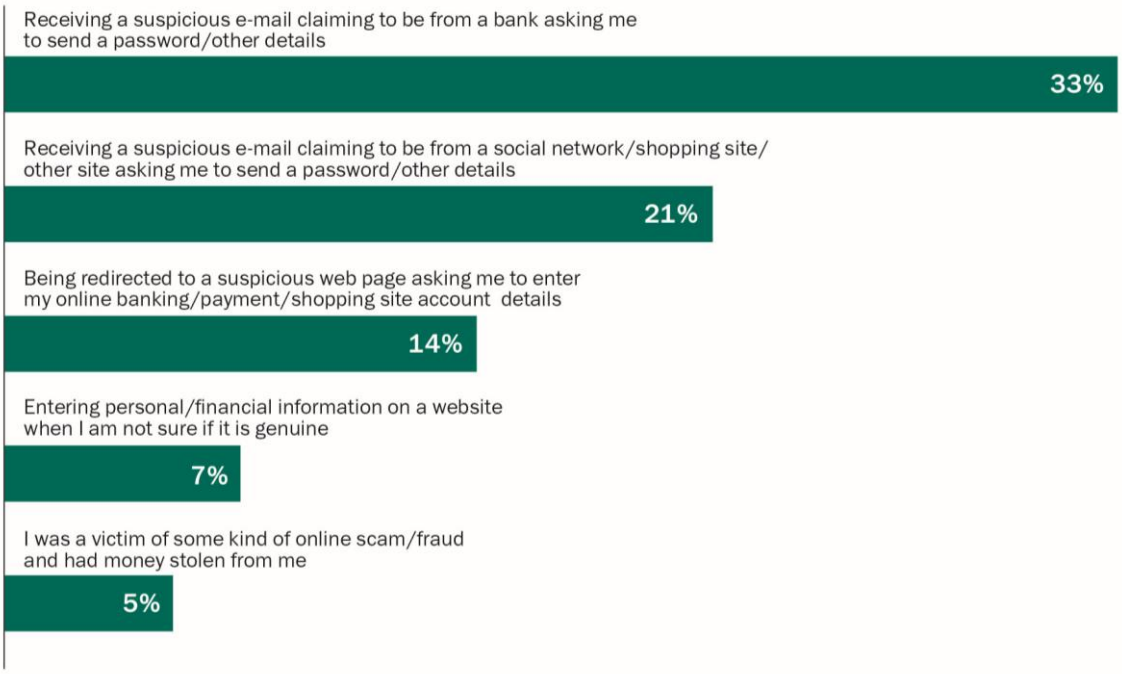


Users who were most affected by this cyber threat live in the Asia-Pacific region (61%), emerging markets (59%) and China (52%). An interesting point was that Windows users were not the most affected by malware over the 12 month period in question. Those who prefer to access the Internet via smartphones and Android tablets were actually the most common victims, 41% and 36% respectively.

- **14% of users reported that their account for social networks, email or payment systems had been attacked** (30% in the Asia-Pacific region and 26% in China and Russia):



- **43% faced various online threats that aimed to access the users' money:**



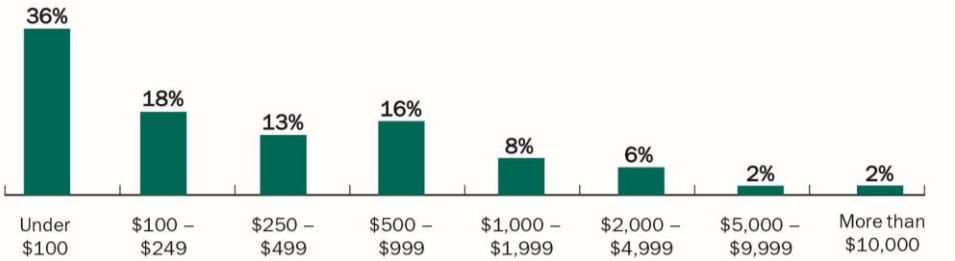
According to statistics, financial threats are most common for fans of Apple devices (52% on the iPad, 51% on desktop computers, 49% on the MacBook) and Android tablet users (50%). It is interesting to note that respondents who spend more time online using tablets are more likely to face attempts to access their finances.

Moreover, **9% of Android tablet owners reported that money had been stolen from them as a result of online fraud. The average for all devices was 5%.** This may be due to the fact that Android devices are the most vulnerable according to the survey.

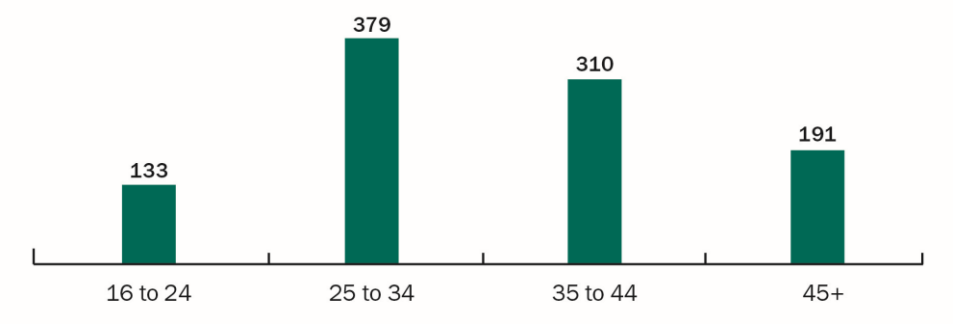
If we calculate the direct and indirect financial losses users faced due to various cyber threats, we get the figures given below.

As a result of infection by malware or an account being hacked, a fifth (21% of respondents) incurred costs in buying special software, paying an IT specialist, replacing device components, etc. In this respect, the average "price" of this type of attack over the past 12 months was $161. The most "expensive" malware incidents occurred in countries of the Asia-Pacific region – $212.

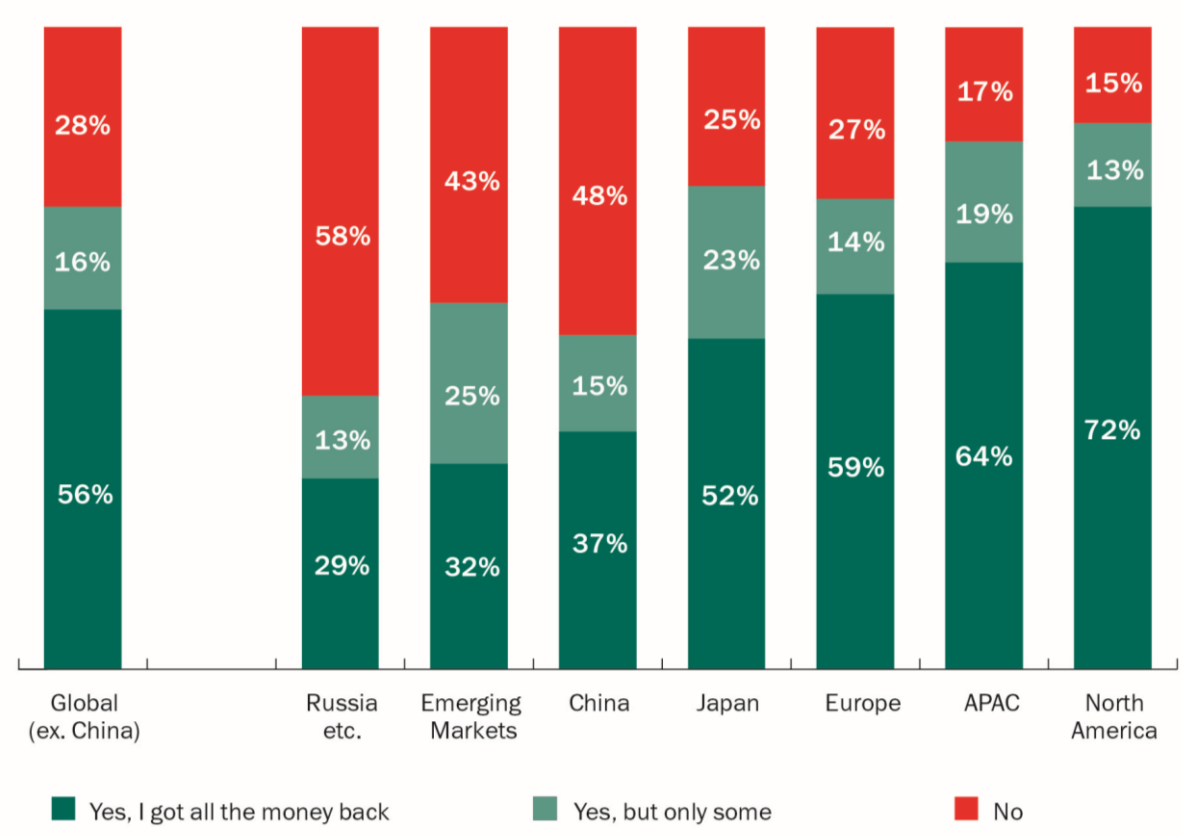
For respondents who had money stolen from them directly via a fraudulent scheme, **the average cost per user per incident was $218, with 18% of users having lost an amount exceeding $1000:**



In terms of the biggest losses reported by users from Europe and North America, the average amount of money stolen was $314 and $263 respectively. Most money was lost by people aged between 25 and 34:



We should note that **44% of victims said that they were unable to fully recover their stolen money.** The most unlucky users in this respect were from Russia – 71% of Russian users did not get their money back in full; the lowest figure was from North America (28%). Such a large gap can be explained by the policies of financial and e-commerce companies for recovering funds for users and victims of financial fraud, which vary from country to country.

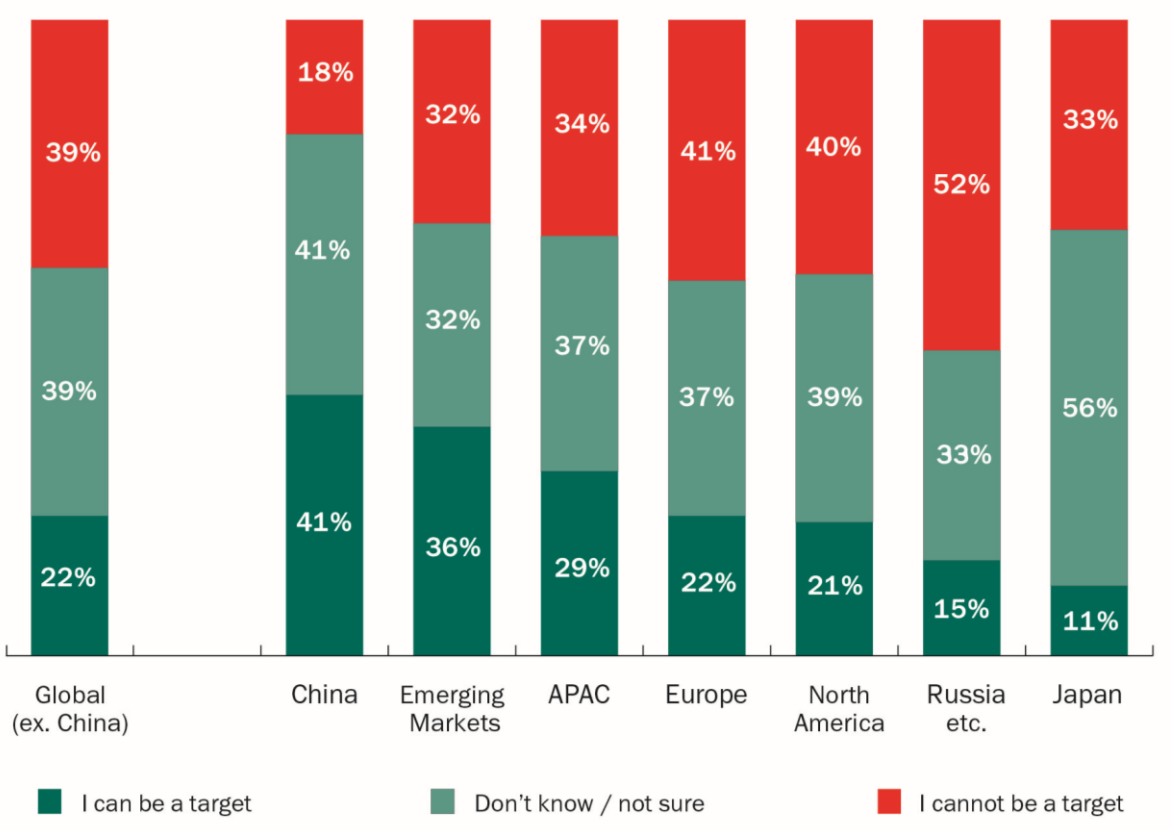


Having established the threats faced by the respondents during the period in question and the costs incurred, we can compare this information with what they think about the threats they face, what they know about the current cyber threat landscape and who they think is responsible for their protection. The next section will discuss these points.

Section 5. Respondents' attitudes towards cyber security

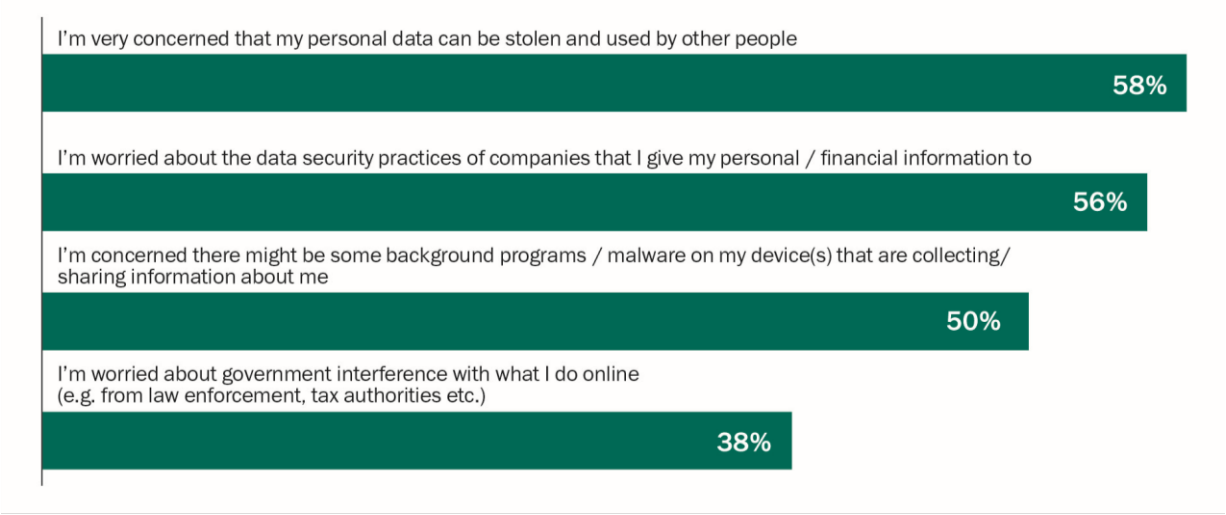
Perceptions of online threats

Despite the fact that the number of online threats is growing every year, not only quantitatively but also qualitatively, **only 22% of users today believe that they could be the target of cyber attacks.** Users in China and the emerging markets believe themselves to be the least vulnerable:

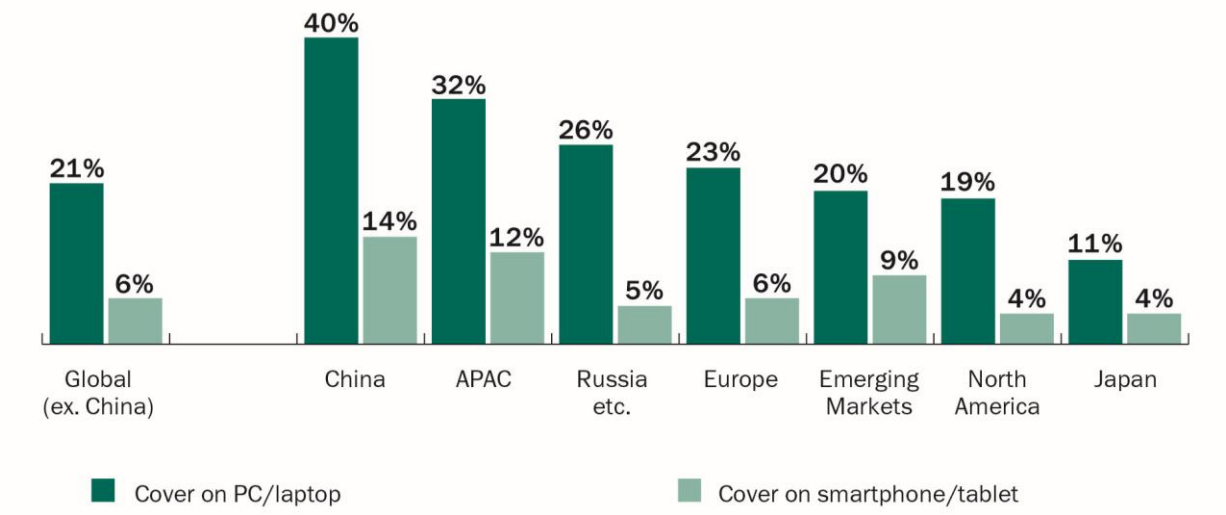


Moreover, **13% of respondents believe that security solutions are a gimmick and do not believe that they are necessary.** The highest numbers of people who think like this live in the Asia-Pacific region (24%), the emerging markets (20%) and China (23%).

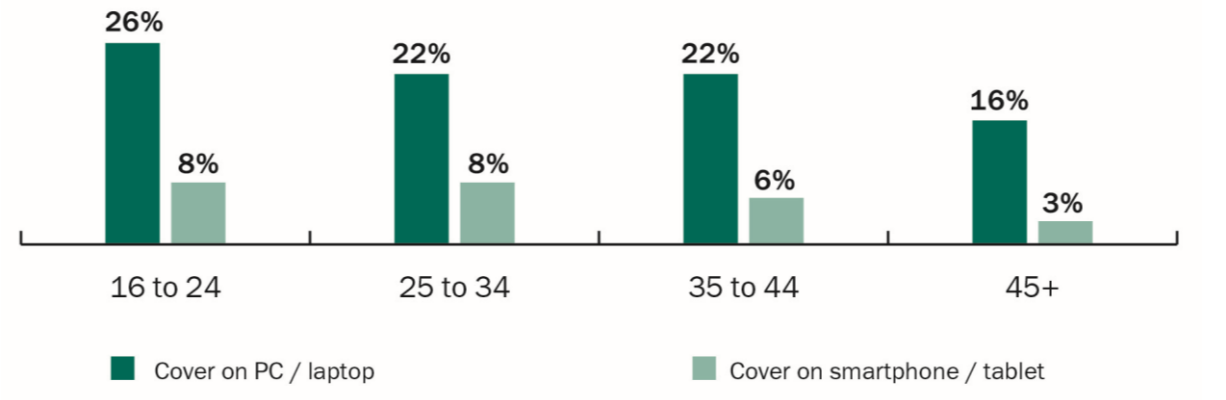
In contrast, at least half of the respondents feel that they face a direct threat: **58% worry that their personal information may be stolen and used by other people, and 50% worry that they may be spied on through their device without them noticing.** Many users are also wary of surveillance by government institutions and do not trust the companies that they send their data to:



Furthermore, **38% of users worry that someone may get access to their webcam, and 21% of respondents admitted that they covered it up because of this** (interestingly, 23% of men do this). Moreover, 6% of respondents even cover the camera on their smartphone. Respondents from China and the Asia-Pacific region do this most frequently:



Younger respondents were more suspicious than the older generation:



If you add together all of the users who are worried about possible surveillance from malware and webcams, it would appear that 60% of respondents have such fears. However, despite the fact that users are worried about their personal online space and about the safety of confidential data, a third (33%) of respondents admitted to giving their personal information to a third party at some point in order to receive discounts or prizes, and 18% admit that they reveal more personal information than they should on social networks.

Furthermore, one in five users (20%) believe that you can become careless on the Internet if the device has a security solution. At the same time, security solutions cannot protect against all threats. For example, 31% of users still enter their personal data on sites, even if they are unsure of their legitimacy.

Understanding the cyber threat landscape

In order to find out how aware users are in general of current cyber threats, they were given a list of threats with a brief description of each one and were asked to state whether they knew about them or not and how much they worried about them. The results were as follows:

Cyber threat	Concerned and very concerned	Aware but not concerned	Not aware or partly aware
Adware	**50%**	**32%**	**18%**
Data interception when using Wi-Fi	**53%**	**27%**	**20%**
Denial-of-service (DDoS) attacks	**38%**	**33%**	**28%**
Global online espionage campaigns	**41%**	**29%**	**30%**
Malware targeted at mobile devices	**46%**	**26%**	**28%**
Malware that accesses webcam	**44%**	**32%**	**24%**
Malware that gathers data/intercepts passwords	**67%**	**19%**	**14%**
Online account hacking	**68%**	**20%**	**12%**
Phishing emails/websites	**57%**	**31%**	**12%**
Pornware	**42%**	**29%**	**29%**
Ransomware	**45%**	**22%**	**33%**
Software exploits	**50%**	**23%**	**28%**
Spam	**45%**	**46%**	**9%**
Threats targeted at bank accounts	**58%**	**24%**	**18%**

The survey showed that most users are worried about possible account hacking (68%) and malware that can collect data and passwords (67%). Users were least aware of ransomware, which encrypts user data or blocks access to a computer until the user pays a ransom (33%). At the same time, according to the Kaspersky Security Network, the number of attacks by this type of malware is growing rapidly: in 2013 alone, there were more than 2.7 million registered attacks, which is 9 times higher than in 2012.

As expected, spam appeared as a threat that most people know about, but this threat worries users least. Second place in this category was taken by DDoS attacks, which also makes sense when you consider that this type of attack is often written about in the media and at the same time is not directed against users, but against corporate online resources.

The fact that almost a **third of respondents did not pay enough attention to such well-known threats as phishing and the interception of data via Wi-Fi is alarming**, even though these methods are often used by cyber criminals to steal user data and money, as they require a minimum investment from the criminals.

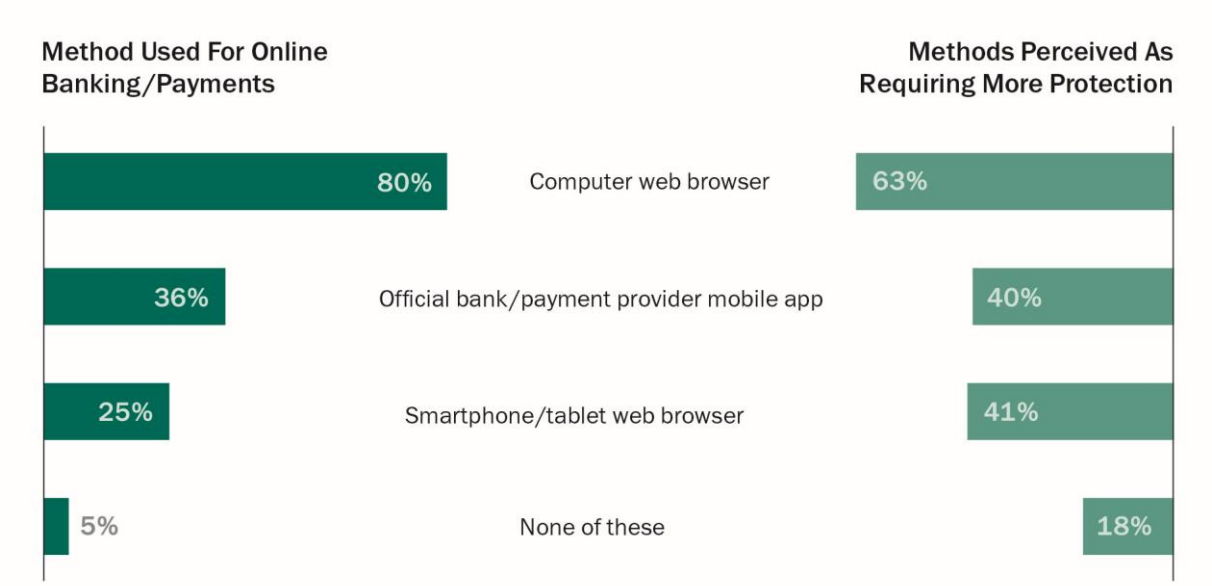
The survey also showed that 26% of users are aware of mobile malware but do not consider how dangerous it can be, while 28% did not even know about it. In this respect, the respondents were asked a few more questions about mobile threats. A good indicator was that **67% of users agree that mobile devices are currently as vulnerable to cyber threats as computers.** However, at the same time, one in five (19%) still feel completely safe when using the Internet on their tablet or smartphone – a reckless behaviour considering mobile devices are more prone to many types of threats, as already mentioned in previous sections. These include financial threats, for example.

Understanding financial threats

In circumstances when cyber criminals increasingly focus on users' financial data, it has never been more important for users to know about the risks they face and to understand how to protect themselves against them. The respondents were therefore asked to agree or disagree with one of a list of statements about the cyber threats targeting their money.

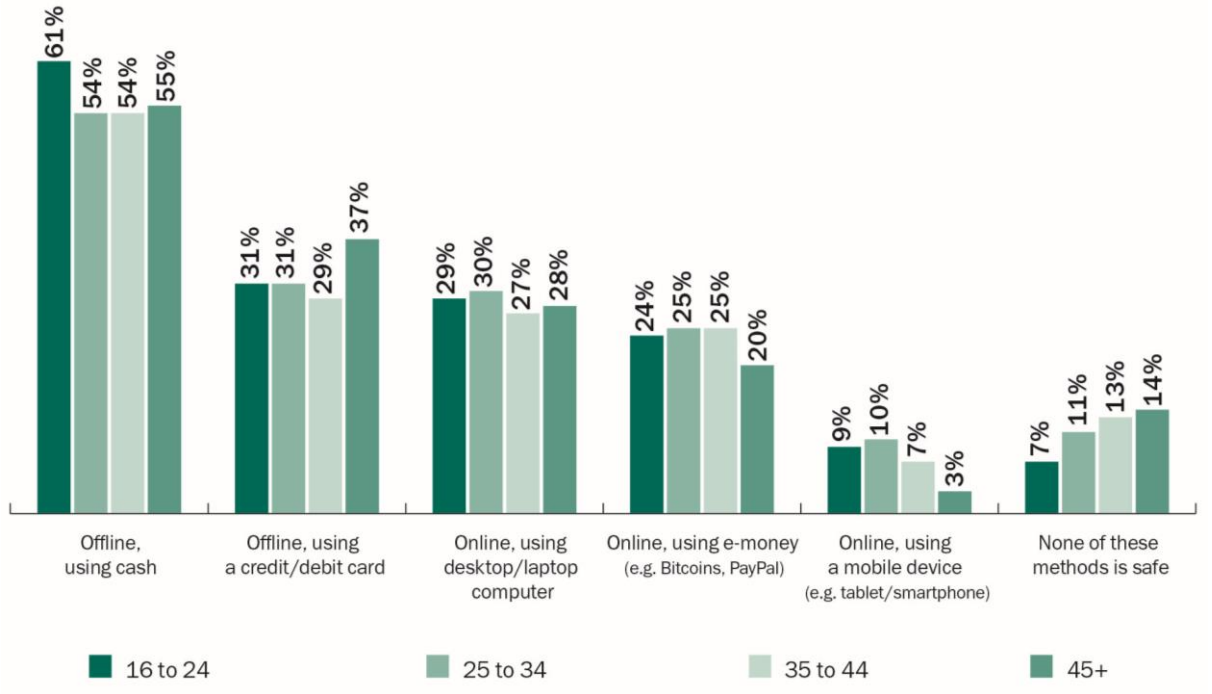
The survey showed that **62% of users were worried about the possibility of online financial fraud.** Another 49% of people reported that they feel vulnerable when buying anything online or completing a financial transaction. Unexpectedly, 16% of users said that cyber crime aimed at stealing money via the Internet was something of a rarity, and that it was unlikely to happen to them. The highest number of respondents who were sure about this point live in the Asia-Pacific region (31%) and China (24%).

80% of respondents making online payments use a web browser and 25% use a mobile browser. Another 36% of users choose an official mobile application provided by a financial provider (a bank or payment system). At the same time, only 18% of respondents believe that these methods are safe enough:



People who live in China and the emerging markets trust online payments the least: only 4% and 6% of respondents from these regions reported that none of these methods require additional protection.

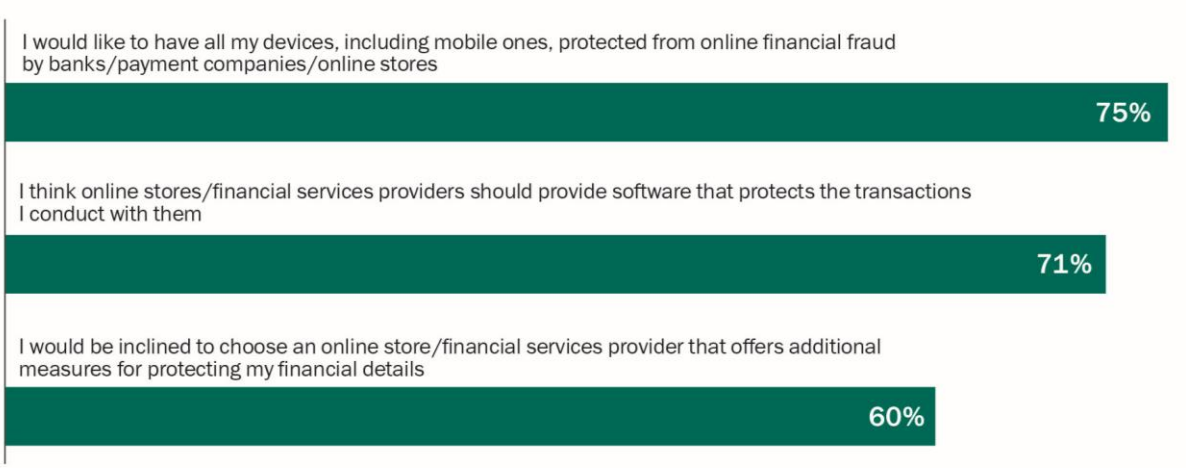
When users were asked to choose two of the most secure payment methods, including offline payments, web browsers running on a computer was third in popularity – 28% of respondents selected this as the safest method. Offline payments came in first and second place: 56% chose cash and 33% a bank card. Interestingly, 23% of users said that the most secure way to pay was using electronic money (bitcoins, PayPal, etc.), while the figure was lower (20%) in the group of respondents aged 45 and over, as expected:



If we exclude e-money from the list of the safest ways to pay, the figures are as follows: 54% respondents say only offline methods are safe (cash and bank cards); 17% chose only online

methods (computer and mobile devices), 17% said both, and 12% answered that none of these methods is safe.

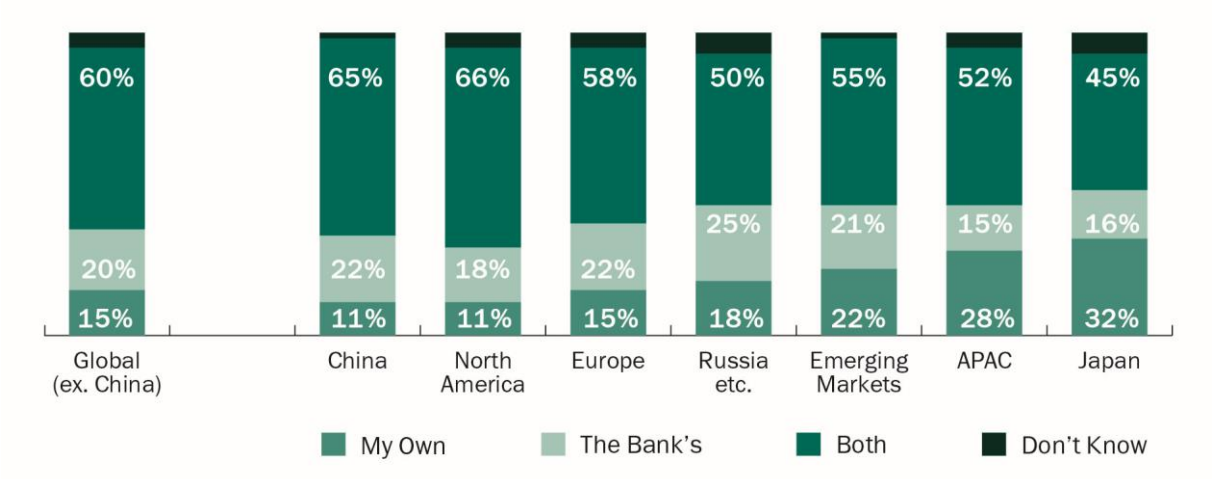
At the same time, the vast majority of users agree that the security of financial transactions must be ensured by the companies conducting these transactions. **Three quarters of respondents prefer banks, payment systems and online stores to provide them with special security solutions, including applications for mobile devices**:



Moreover, the level of protection for online transactions directly affects the financial activity of online users: **42% of respondents said that they would use such a payment method more often if it had a reliable security solution for their device**. 37% of users had refused to continue with online payments halfway through because they were not sure how safe they were.

Furthermore, users acknowledged that if a fraudulent scheme was successful for criminals, they expected financial companies to reimburse the stolen funds without question – 40% of respondents were of this opinion.

In terms of who should be responsible for the protection of online financial transactions, only 15% of users said that they themselves should be, while 20% placed full responsibility on their bank. Most (60%) believed that both sides should ensure the protection of electronic transfers and payments equally:



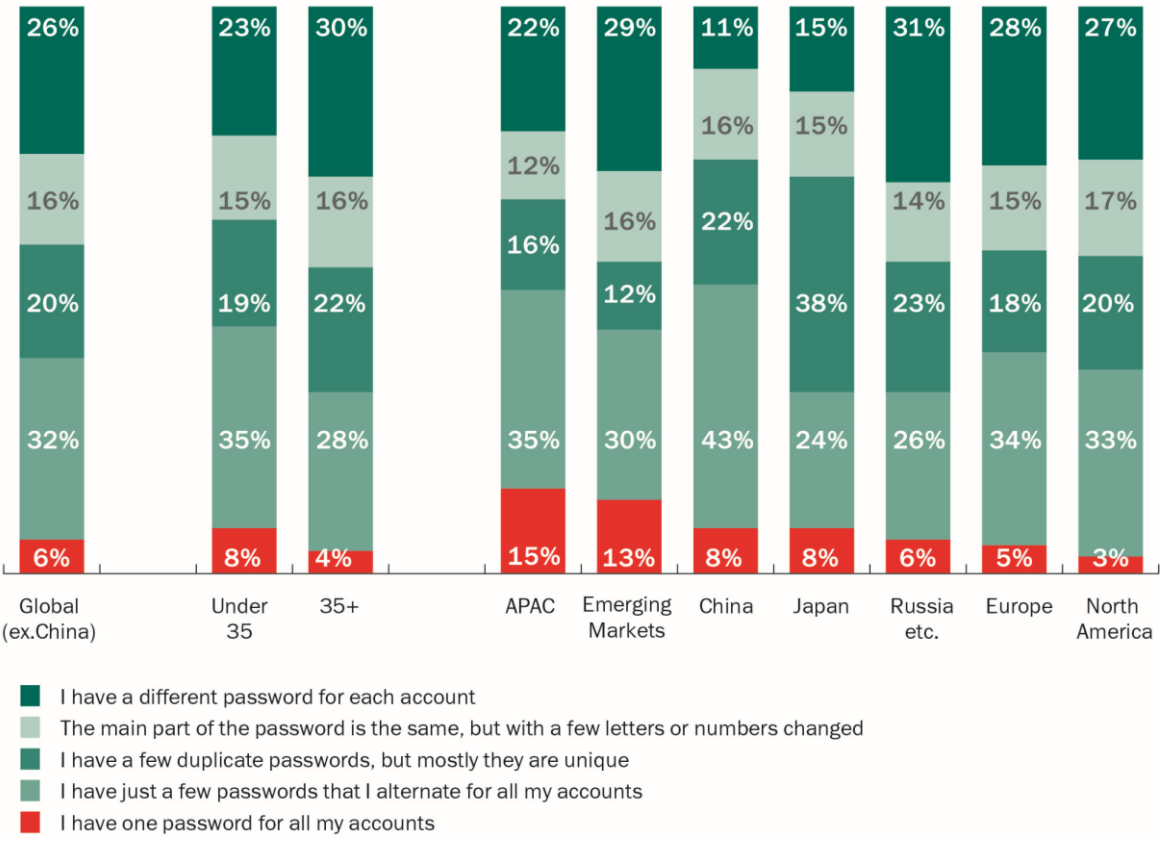
It is interesting to note that Russians are the most likely to rely on protection from their bank (25%), while the victims of online fraud from this country were least successful at returning stolen money.

One of the simplest and most effective options for cyber criminals to access user data, including bank accounts or a personal page on an online store, is to use the users' own login details and password.

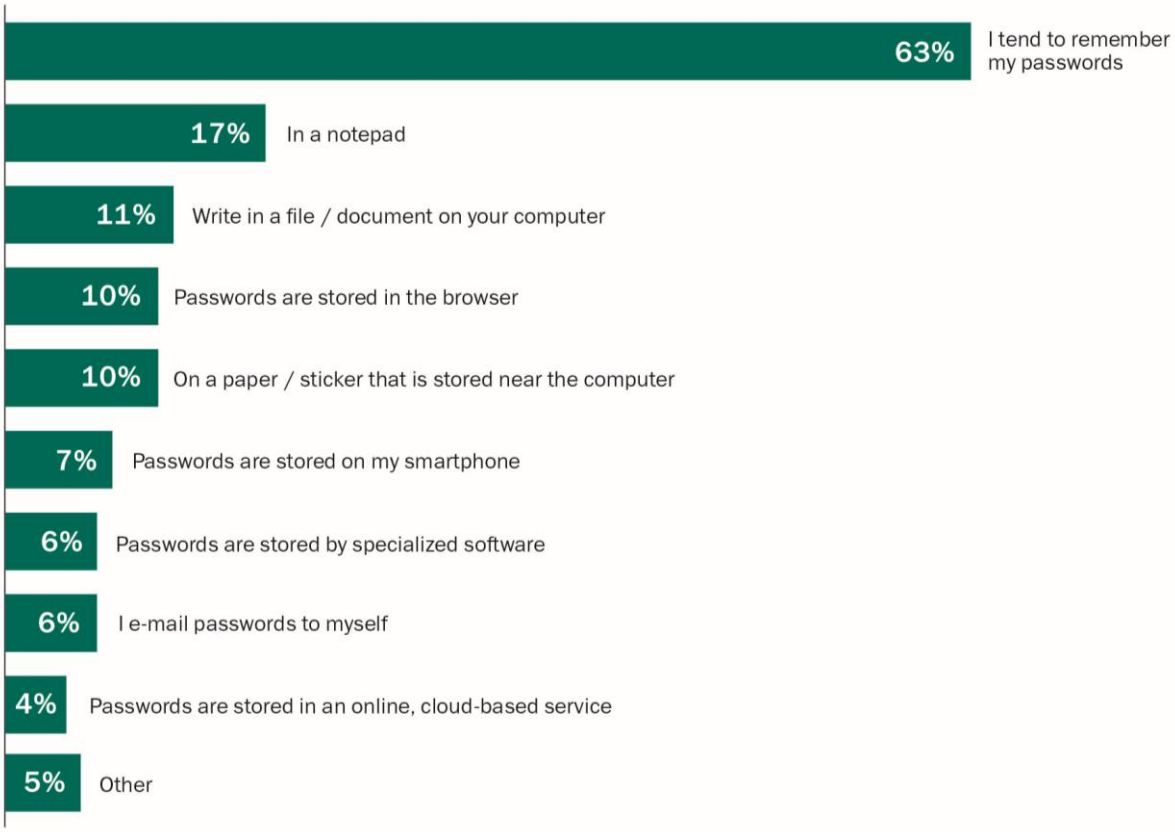
Attitude towards passwords

Scammers can obtain users' passwords through different means: by using special malware, so-called phishing web pages and emails, by hacking into Wi-Fi connections, etc. At the same time, threats to users are even more serious if they use the same password for different accounts. This would mean that criminals could use a single password to gain access to multiple resources and it would therefore be of great use to them.

The respondents were therefore asked how many passwords they use on the web. The survey found that only 26% of respondents have different passwords for different accounts, and the majority (32%) only have a limited number of passwords. People aged over 35 are least careful in this respect – 29% of respondents from this group use the same password for all online resources. Furthermore, the least concerned in this respect were residents from the Asia-Pacific region and the emerging markets: 15% and 13% of them stated that they use only one password for all of their pages. In North America, this figure was only 3%:



This approach to passwords could be due to the fact that the vast majority of users prefer to remember passwords, rather than using special solutions to generate robust passwords and storing them in a secure manner. Worst of all**, 45% use potentially unsafe methods for storing passwords such as a notepad, a sticker next to their computer, their mobile phone, etc.:**



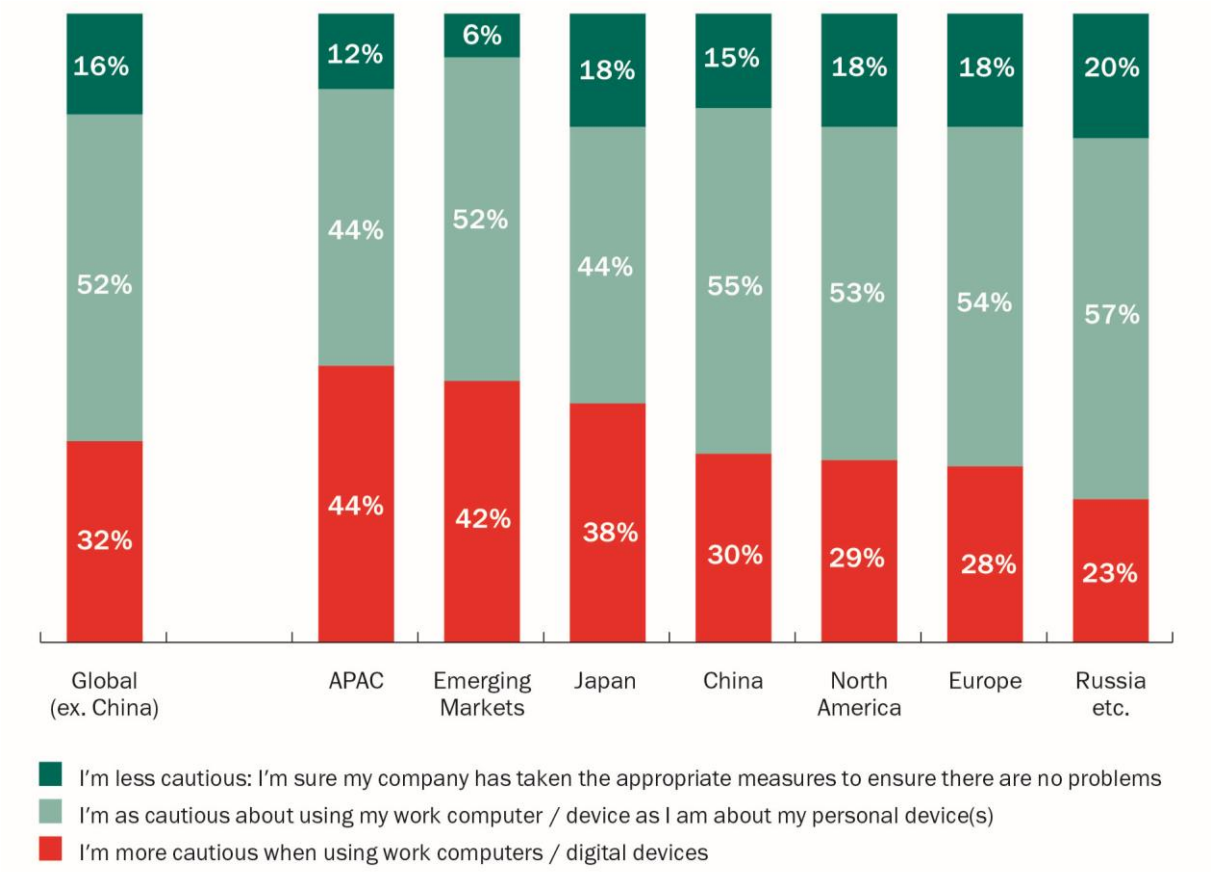
Despite the fact that 63% of users rely on their memory when it comes to passwords, only 15% have never forgotten them, and 6% said that they had lost access to their account because of this.

However, users are rather optimistic when it comes to passwords: **one in five (20%) are confident that their passwords could not be useful for cyber criminals**, and 17% do not keep their passwords a secret from family and friends. Furthermore, every fifth user takes no additional action to protect their password, and a further 36% believe that all websites securely store their passwords. At the same time, on the other hand, user passwords are periodically made available as a result of major leaks at companies.

The survey showed that, despite all their fears, most users are still unconcerned when it came to protecting their digital identity and their personal data online. It was therefore interesting to clarify whether they were just as unconcerned at work.

Attitudes to threats at work

According to the survey, **85% of respondents use their device for work as well.** 16% admitted that they are less careful in this respect as they believe that their company has taken all of the required security measures:



It is interesting to note that 39% of respondents who use their device for work believe that cyber threats for home users and companies do not differ much. At the same time, only 60% were sure that they could distinguish between a real e-mail and spam, and 29% do not check links and attachments received through their corporate e-mail account:

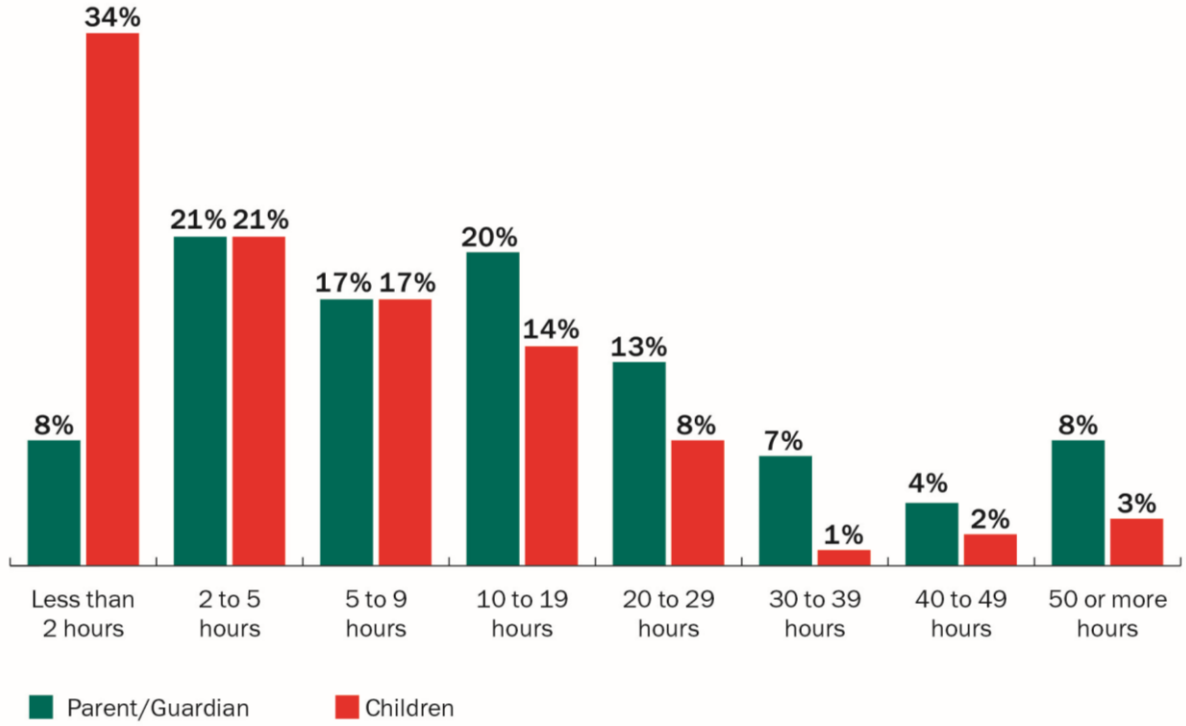
Users are therefore jeopardising not only personal, but also business information. Moreover, **nearly a third of respondents (28%) admitted that they had opened a potentially dangerous link or attachment** at least once. Participants from China and the Asia-Pacific region (58% and 42%) were most likely to do so.

The next section shows the results of research into how users relate to what is happening on the web in terms of their children, and whether or not they are able to protect them against cyber threats.

Section 6. Children online: parental attitudes, incidents and solutions

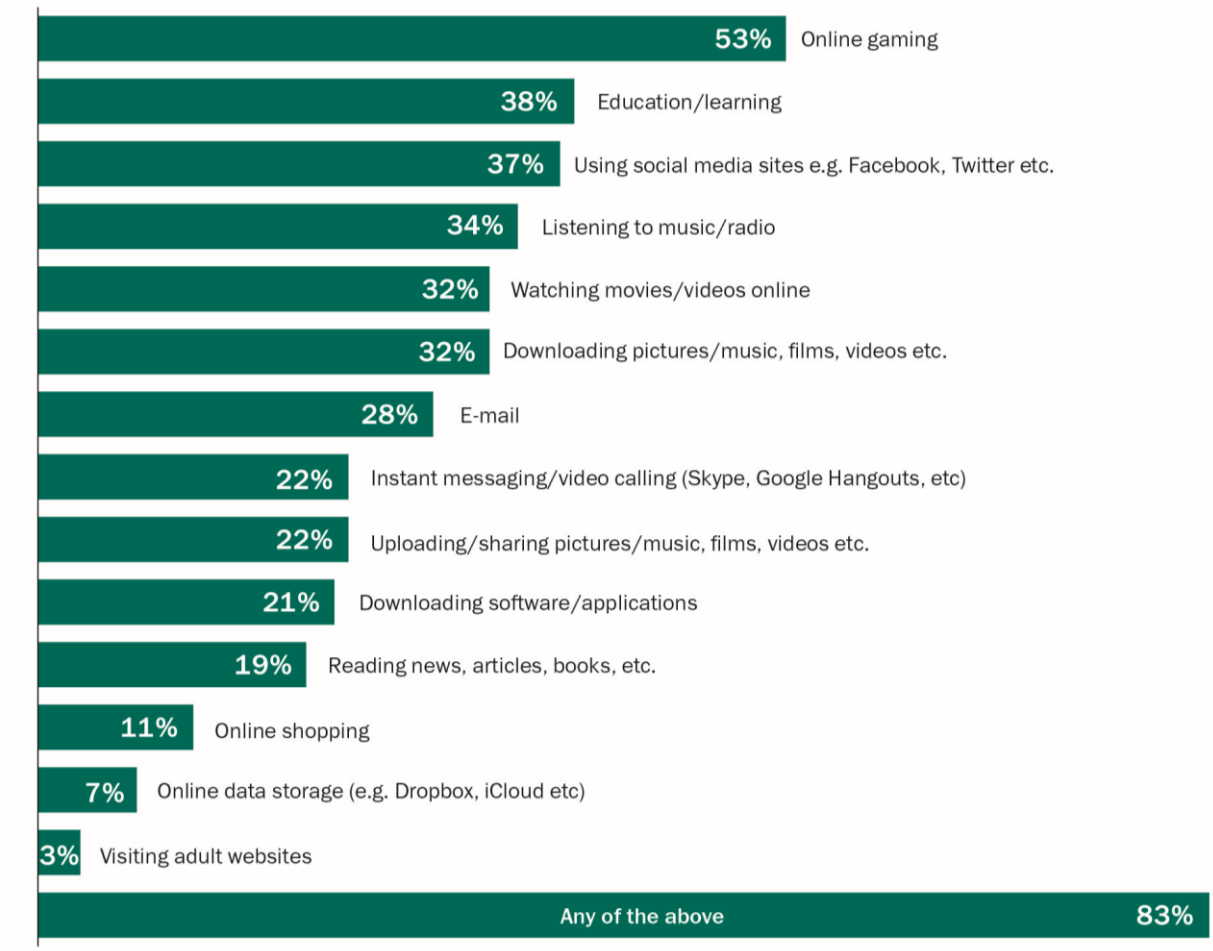
More than a third (37%) of respondents reported that their families have children under the age of 16. This group of users were asked about the threats faced by children online and the security measures they took. In particular, most adults are seriously concerned about security issues in relation to their children being on the Internet, with **40% of adults agreeing with the statement that the number of online threats to their children is growing**.

According to the survey, children often use the Internet as much as their parents – 22% of children and adults use the Internet for about the same amount of time, and 15% of children are online for longer than the adults. Children of the respondents were most likely to use the Internet for at least two hours per week:



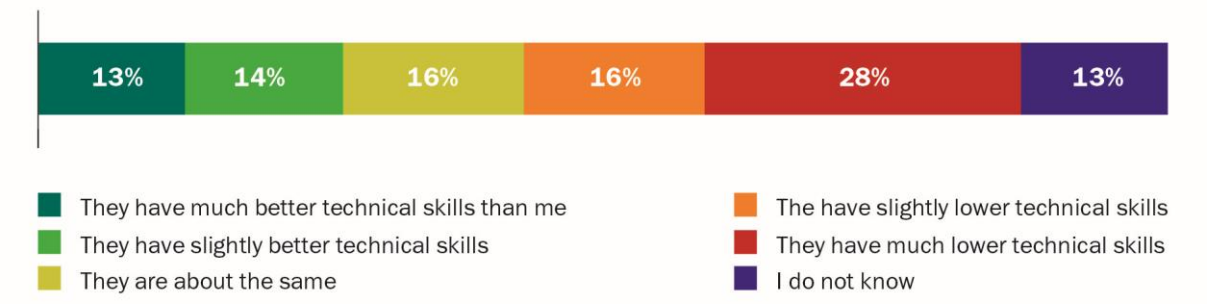
Residents of Japan are the strictest with their children and the "less than two hours" option was chosen by 52% of respondents in this country. Furthermore, this option was selected by 45% of respondents aged between 25 and 34. Adults aged older than 45, on the other hand, were more likely to report that their children spend more time online than they do themselves. This can be explained by the fact that young parents have children who are too small to use a computer, while children of those aged 45 and over, on the other hand, are old enough to spend a few hours online.

Most adults (53%) said that their children play online games when asked about what their children do on the Internet. Interestingly, just as in the case of adults, social networks came in third, but education came in second place instead of reading:

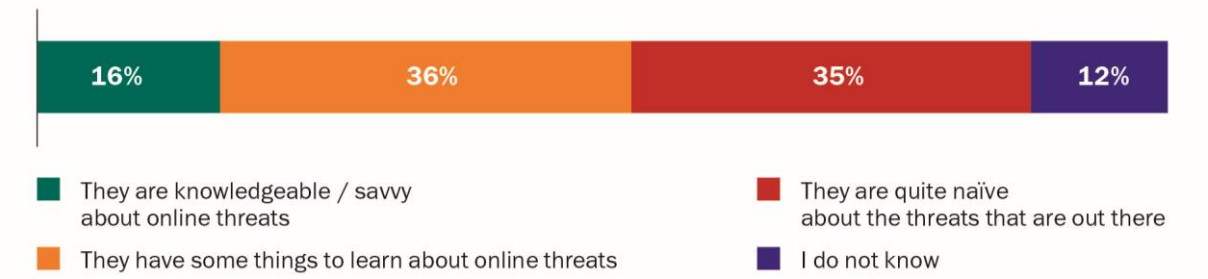


Unfortunately, we do not know how these questions would be answered by the children themselves, because not all adults know exactly what their children do online. Half of the respondents (50%) worried that their child may see unwanted web content, almost as many (48%) worried that their child may become a victim of online harassment, 40% worried that their children could chat online with suspicious strangers, and 27% of respondents believed that they share too much personal information on the web.

Moreover, **27% of respondents believed that their children know more or even much more about information technology than themselves**:

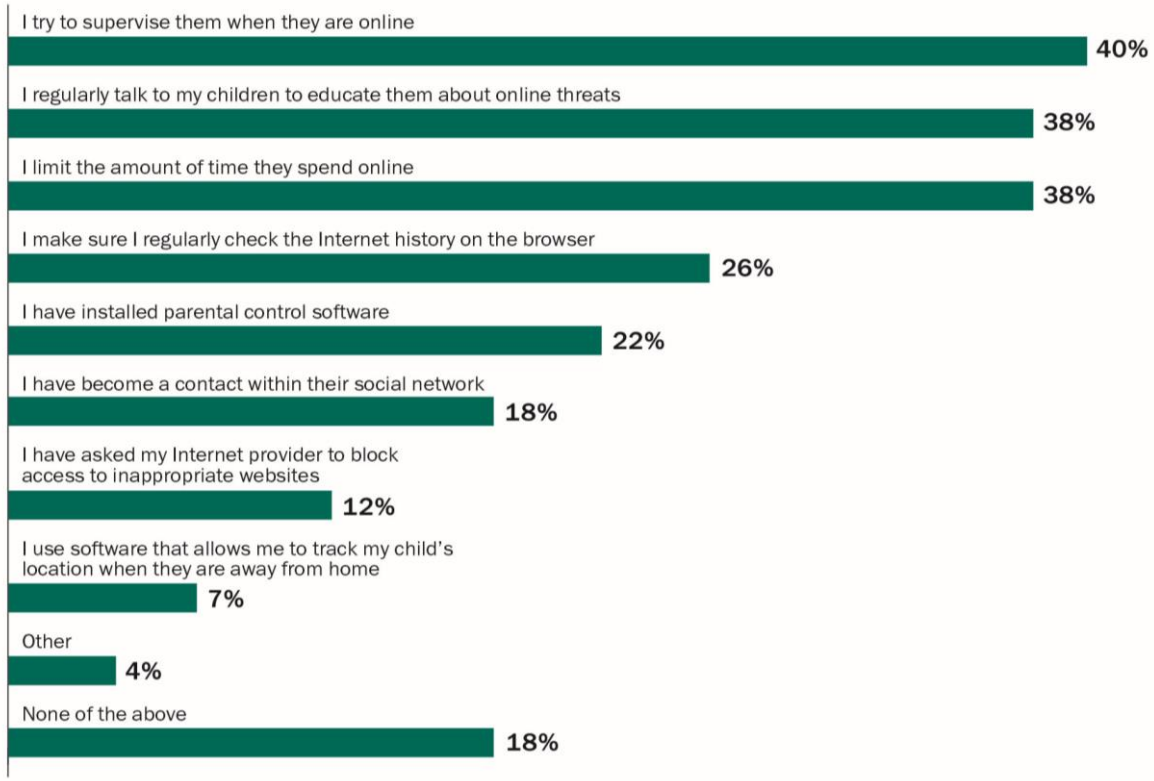


In the Asia-Pacific region and the emerging markets the percentage of adults who gave this response was much higher than in the rest of the world – 42% and 38%, respectively. Similarly, only 35% of adults believed that their children know nothing about cyber threats (51% in China, 44% in Russia):



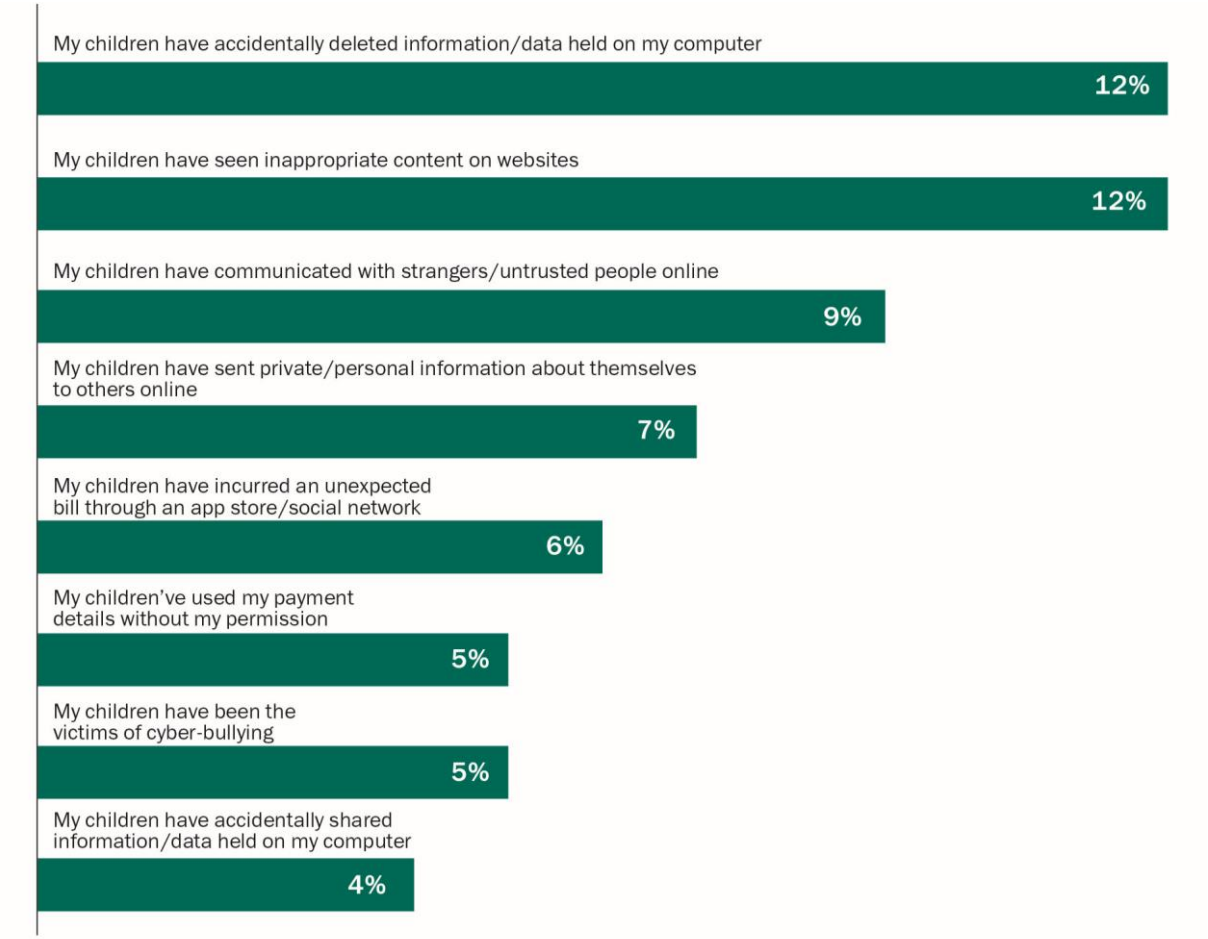
Furthermore, **one in five adults (22%) feel that they cannot control what their child sees or does online.** In terms of the steps they take to protect their children against threats on the Internet, 39% of users said that they monitored what the child did online, 38% had conversations to educate them or limited connection time, and 19% added them as a friend on social networks for this purpose. Only 23% of respondents used special software enabling them to filter out unwanted content for a child or to limit the amount of time spent on the web.

It is interesting to note that 18% (nearly one in five parents or guardians) do not use any of these measures. The highest number of users who do not pay attention to protecting their children against cyber threats live in Japan (35%), and the lowest figure came from the Asia-Pacific region, the emerging markets and China (9%).



At the same time, a significant number of respondents stated that their children face online threats or that the web is a source of threats: **22% of respondents said that their children**

had encountered an incident directly threatening them over the past 12 months and **21% said that their children did something that led to the loss of an adult's money or data**:



Both types of incidents occurred most often with children from the Asia-Pacific region and the emerging markets, where parents seek to protect their children online more than anywhere else. Likewise, these incidents happened least often in Japan, where the highest numbers of adults take no action to monitor their children online. This may be due to the fact that, according to the survey, residents of Japan are less aware than other respondents of the existing cyber threats (see the previous section).

One of the most unpleasant occurrences on the Internet is the cyber bullying of children, on social networks for example. 5% of parents mentioned cyber bullying in the past 12 months, but in some areas, for instance in the Asia-Pacific region, the percentage of victims was much higher (11%).

According to the study, in most cases cyber bullying had negative consequences: 44% of parents were forced to intervene to resolve the issue, in 26% of cases of online harassment the children had to go offline, and **in 25% of cases the child was so psychologically traumatised that it took a long time for him/her to recover**.

In other words, the Internet is all encompassing and poses threats to everyone: children and adults, customers of online stores and fans of social networks, Windows users and Apple OS X users. Users must therefore be cautious and know the threats posed by different activities on the web. Forewarned is forearmed.

Conclusion

Users now go online from several devices and trust them with their most valuable data: their secrets, private information, their 'digital self'. Not surprisingly, most of them are aware of the importance of the digital part of their life and fear losing this data or are worried about being spied on online by third parties. However, despite their fears, people still tend to be unsafe in their behaviour; many not only do not install security solutions on their devices, but they do not even protect them with a password, and only a small number of users are aware of the threats they or their relatives may face on the net.

At the same time, statistics show that more and more owners of devices lose their files, money or their digital identity online, which are sometimes impossible to get back. Kaspersky Lab therefore not only recommends using protective solutions for your safety and security, but also advises users to exercise caution on the Internet, especially when transferring confidential information and completing financial transactions: use robust passwords, do not enter data on untrusted sites or via an unsecured Wi-Fi network, do not open unknown files and do not forget about protection for children.

Interesting links:

Infographic: Multi-device threats in a multi-device world: http://media.kaspersky.com/Images/Infographics/MD-usage.png

Report: Financial threats in 2013: http://media.kaspersky.com/en/Kaspersky-Lab-KSN-report-Financial-cyber-threats-in-2013-eng-final.pdf

Report: IT threat evolution Q2 2014: http://securelist.com/analysis/quarterly-malware-reports/65340/it-threat-evolution-q2-2014/

Blog post: Social network frauds: http://securelist.com/analysis/publications/63855/social-network-frauds/

Blog post: Children online – the security formula: http://securelist.com/analysis/publications/63866/children-online-the-security-formula