Security in a multi-device world: the customer's point of view

August, 2013

Introduction

The world of digital devices is constantly changing. New gadgets, online services and applications are appearing all the time. More and more people rely on their computers, smartphones and tablets to store valuable information and carry out important tasks. These devices have changed people's lives, but at the same time users must be aware of the dangers posed by many existing cyberthreats.

Kaspersky Lab never stops striving to improve the protection quality of its solutions. To ensure its products meet the needs of users, the company conducts an annual customer survey in conjunction with international analytic agencies. These worldwide studies help us to understand how people perceive information security, what threats they have encountered, and what measures they are taking to protect themselves.

In summer 2013 Kaspersky Lab joined forces with international research agency B2B International to conduct a new survey. There were 8,605 respondents, men and women from 19 countries in Europe, the Americas, the Middle East and the Asia-Pacific region. All participants were over 16, more than one-third of them have at least one child and the overwhelming majority use the Internet and various mobile devices.

Main Findings

According to the results of the survey, the main trend in consumer electronics over the past 12 months was the transition to an increasingly multi-device, 'always-on' world.

Multi-device is the conventional name for today's model of using always-on devices like smartphones and tablets alongside computers and laptops. Light, powerful smartphones and tablets enable users to interact and share information, download media content and use online services in much the same way they would on conventional desktop computers. According to the survey, the average household owns approximately 4.5 devices that might be used for very different tasks. Most often they are used for financial transactions:

- 98% of respondents use a device to conduct financial operations;
- 74% of respondents regularly use e-wallets and payment systems;
- Online shops, banking services and social media are the most popular resources among owners of always-on devices.

Use of online financial services inevitably leads to the risk of criminal attack. On the whole users are aware of the danger that cyberthreats represent, as the survey shows. For instance:

- 73% of respondents stated they regularly update software on their devices;
- About half of the respondents think any device (regardless of the operating system – Windows, Mac OS X or Android) can only be considered safe if security software is installed;
- 69% of respondents feel that personal data on their devices requires additional security.

At the same time, there is still a substantial group of users who do not pay enough attention to security or place too much trust in third parties:

- 34% of respondents take no security measures when using public Wi-Fi networks;
- 40% are certain that the websites they use provide adequate protection for their passwords;
- 45% are confident that their bank will return any money that is stolen from them online.

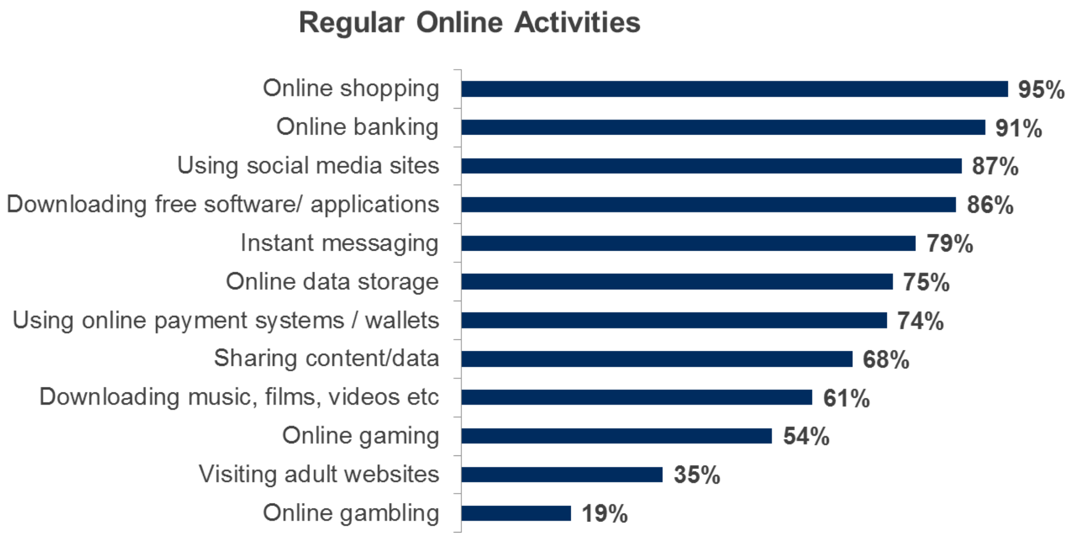
Even with a fairly responsible approach to information security, a significant number of people suffer malware attacks – and real financial losses as a result:

- 27% faced malware attacks;
- One in five of those attacks led to personal data leakage;
- 62% of respondents have experienced at least one incident where there was an attempt to steal financial information;
- The average cost of an attack was $74 per person;
- 41% of financial attack victims were unable to get all their money back.

The survey included further questions about the Internet, mobile threats and computers. In particular, it sought opinions on cyberthreats, on how users protect passwords and personal data, and issues related to children's use of the Internet. The results of these questions and more can be found in the analysis of the B2B International and Kaspersky Lab study below.

Online activities: everything from shopping to sharing data

Banking and shopping the most popular activities

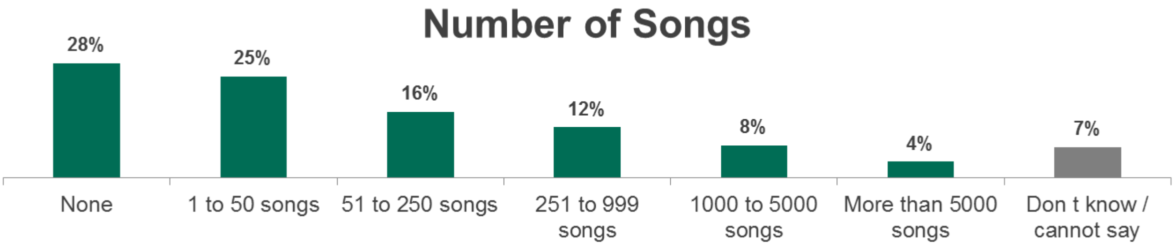


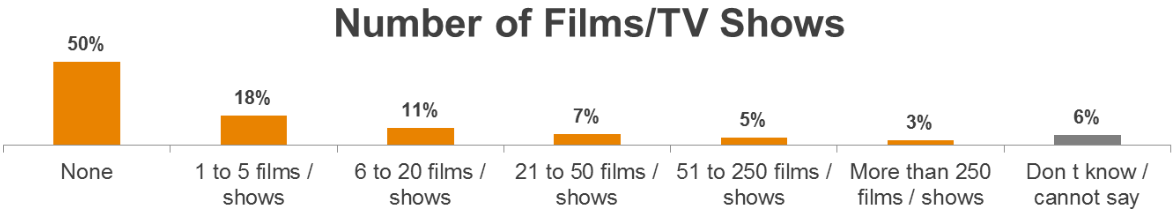
Online shopping, banking and social media are the most popular online services for computer, smartphone and tablet users. Our survey found that 98% of respondents regularly use various online financial services, be it banking, shopping or e-payment. A computer or laptop is still the major tool for accessing such services – 77% stated they buy goods in e-stores with their PC, while 71% use it for online banking. However, a significant number are using mobiles for these services. As they become more convenient, financial services are spreading beyond traditional desktop computers and arriving on mobile platforms.

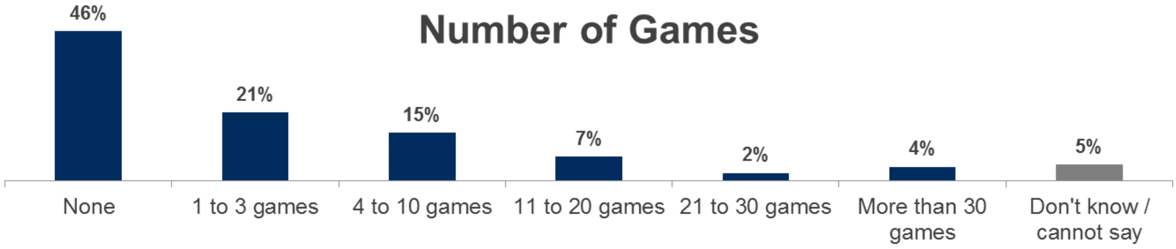
For instance, 19% of respondents use their smartphones for bank operations and 18% use their tablets to access e-stores. The importance of using security products on these devices cannot be overestimated.

However, financial activity involves more than shops, banks and payment systems. Content – music, videos, games, etc. – is a popular commodity for users to spend money on.

Content among the most popular purchases





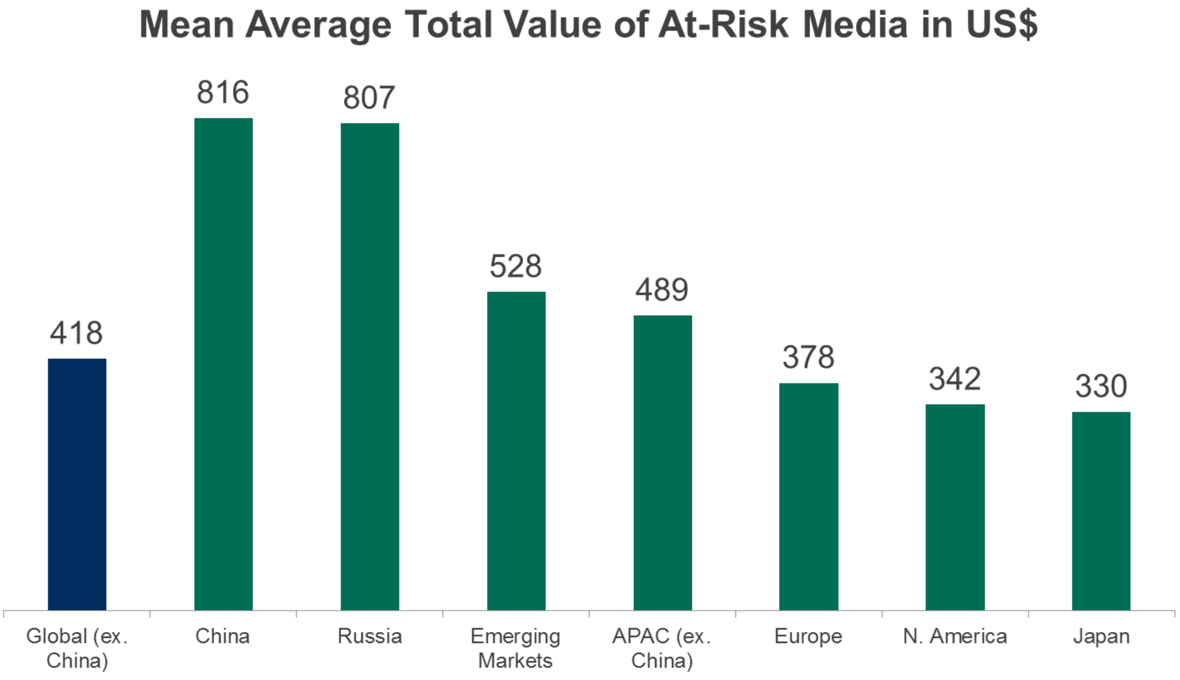


About a quarter (24%) of respondents stated they have bought or downloaded more than 250 music tracks over the last 12 months. Approximately every tenth user downloads six to 20 movies or TV series in a year, another 15% of respondents download from four to 10 games.

At the same time users don’t worry much about keeping their content safe – more than a third (35%) said they make no backup copy of their media content, and another 18% have backed up less than 20% of their media library. Only 23% of respondents make backups of 90% of their music, movies, games and other multimedia content. This careless approach to saving data can result in serious consequences.

If a device breaks down or suffers a malware attack, users could lose their entire media library of music, movies, photos and documents. Moreover incidents like this may result in direct financial losses.

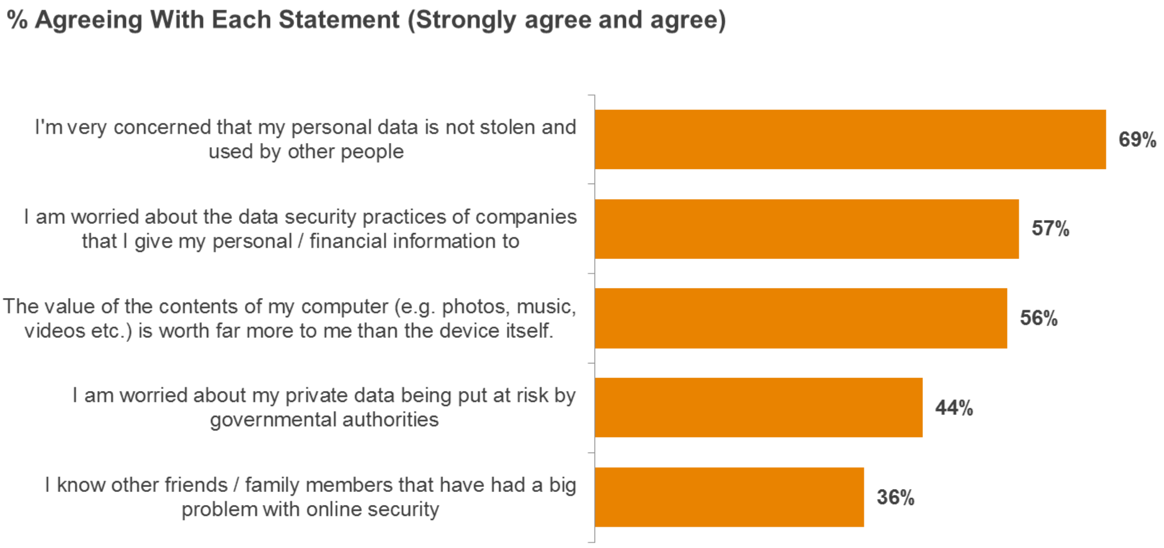
Lost content inevitably costs money



Failing to back up content properly can lead to real financial costs. On average, the loss of media collection following a malicious attack or device failure will cost the user **$418**. This figure represents the approximate price of the content that users own, factoring in those files with no backup copies. These costs are especially high in China ($816) and Russia (**$807**), since in these countries many users fail to back up much of their media. 26% of Chinese users and 55% of Russians make no backups at all.

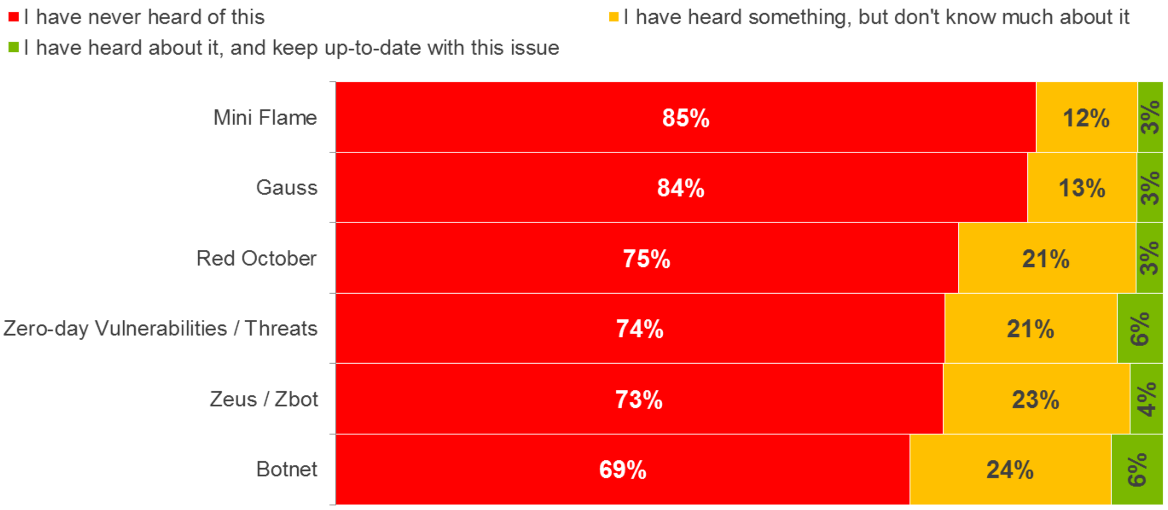
Attitudes to cybersecurity – privacy more important than the risks of cyberwarfare

Protecting private data is the biggest concern



About 56% of users stated they value important data stored in a computer's memory more than the computer itself. Because personal data has such value, people are worried about its safety. In particular, users fear their personal data might be stolen by third parties – a problem picked out by 69% of respondents. In 57% of cases people are not sure whether the protection technologies of companies to which they entrust their personal data, including financial information, are safe. 44% of users have the same fears about government agencies – these people are uncertain that government information services can safely store personal data. As more services become available, so these worries increase.

Cyberwarfare and state-sponsored attacks? Most people have never heard of them

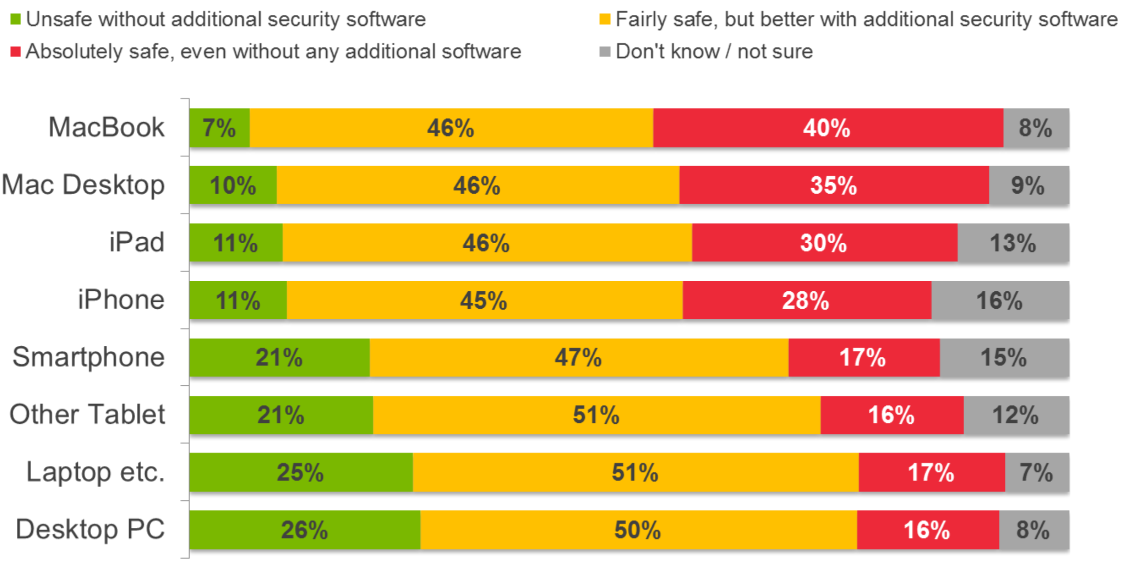


Although 31% of respondents said they were worried about cyberwarfare and the damage it could cause, relatively little is known about the kinds of weaponry used. The vast majority of people know nothing about malware such as Mini Flame, Gauss, and the Red October cyber espionage campaign, despite information on these malicious programs being widely available.

There also seems to be little concern over trends like ‘hacktivism’, the fact that some cyberattacks have the indirect backing of governments, or attacks on software, video game and media companies such as Adobe, Microsoft, Oracle, Sony, and The New York Times. On average, only a third of those surveyed said they thought this was cause for concern.

At the same time, better understanding of different types of cyberattack, their structure and potential consequences can go some way to safeguarding our digital lives. The more users know about threats, the harder it is for cybercriminals to involve them in fraudulent schemes.

Device type & security – Windows demands additional security, but don’t forget about your Mac



Desktop PCs running Windows are still seen as the most vulnerable to attack, with 76% of those surveyed stating they should not be used without additional security software. As usual, a high proportion of users remain confident that Macs (35%) and MacBooks (40%) are impervious to cyberthreats. However, there are more users who think OS X is not sufficiently secure, with over 53% agreeing that additional security software needs to be used with Apple computers.

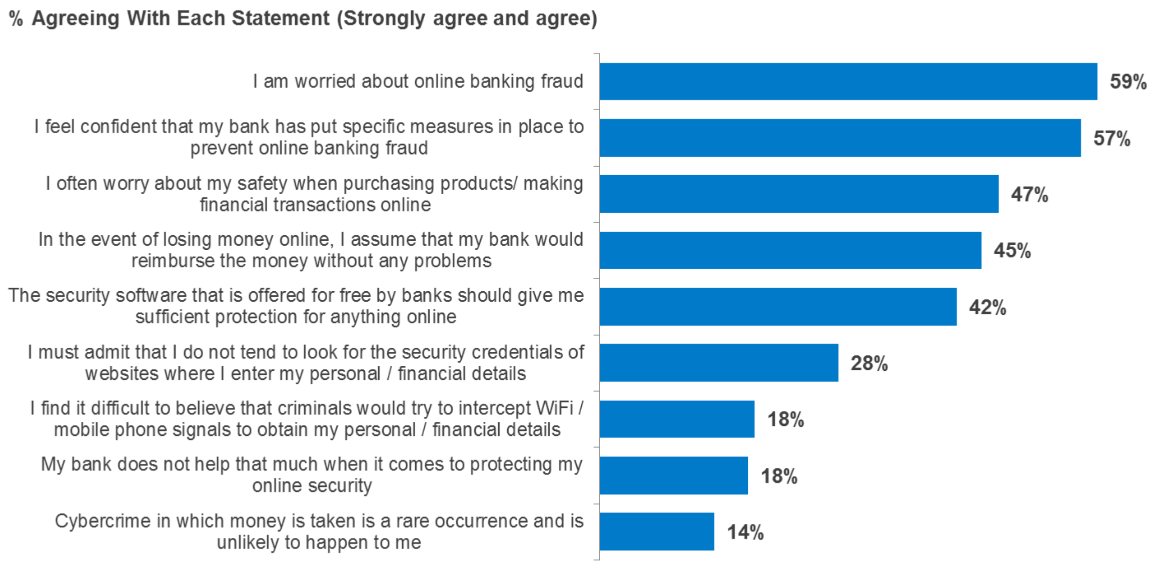
The majority of users feel that mobile devices need specialized protection: 72% of tablet users and 68% of smartphone owners agreed with this.

The most vulnerable to cyberattack is the Windows operating system (plus Internet Explorer) (68%). 34% view the Oracle Java platform as unsafe, while 21% feel Android’s level of security poses a threat.

The respondents had a remarkably accurate view of the most vulnerable platforms – Windows, Java and Android are indeed attacked most frequently by cybercriminals.

Yet another important area for users is the security of online financial services.

Online finances – some are too trusting

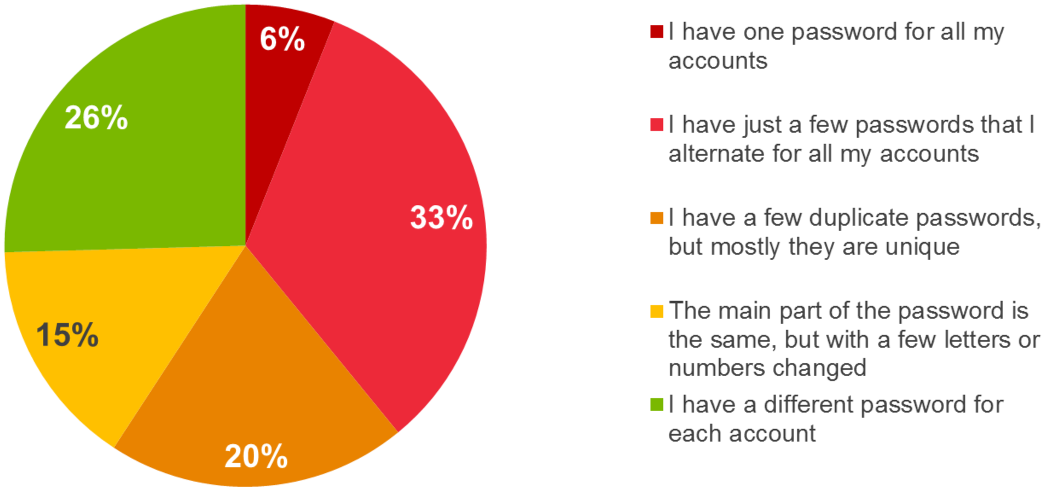


The survey results show that users are reasonably well informed about just how widespread financial fraud is online and the consequences of such crimes. 59% of respondents said they were worried about this, while 47% admitted they felt vulnerable when conducting financial transactions online.

Many of those surveyed believe that banks should be responsible for the security of any transaction. For example, 45% state that a bank should reimburse any money that is lost during online operations and 42% believe a bank should provide software to safeguard payments online. However, the reality is rather different. Banks do not always reimburse stolen money, and are even less likely to offer additional security software to customers.

Any data linked to online finances obviously needs to be protected. At the very least, a password is required, but even this simple measure isn't always applied by some.

Data protection – few use special software to securely store and generate passwords



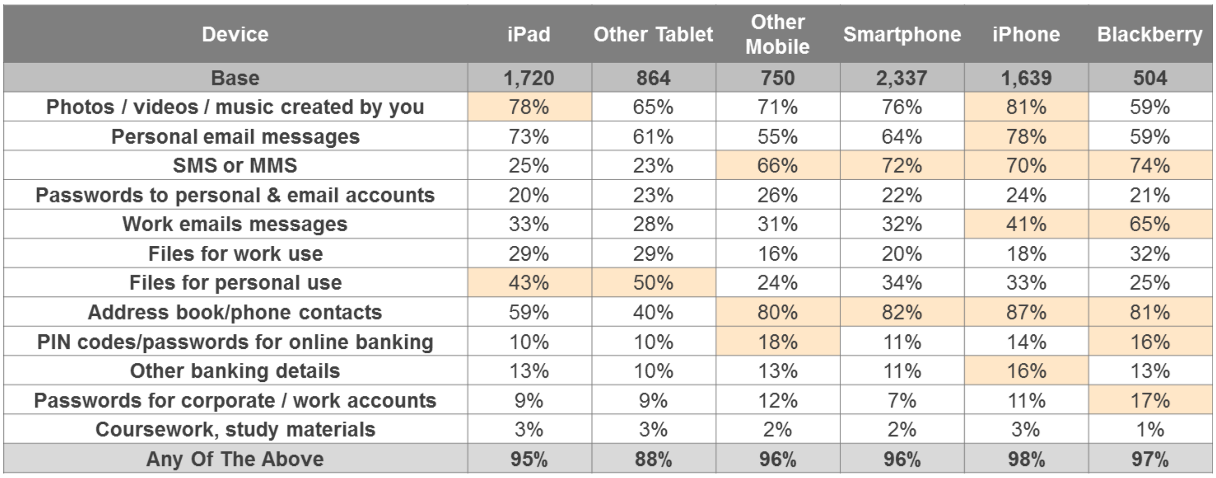
About 40% of those polled said they had just one password, or at best a small collection, for all of their accounts. 15% said they use passwords that differ only slightly from account to account, while slightly more than a quarter said they use a unique password for each account. The practice of using just a few passwords for numerous accounts is not surprising because the majority (65%) like to keep no written record of them – not everyone is capable of remembering lots of different passwords.

Only 6% use dedicated programs for creating and securely storing passwords. Those other respondents who didn't rely on their memories to keep track of their passwords tended to resort to inherently risky storage methods. They used a notebook (16%), a document stored on the computer itself (11%) or a piece of paper that can usually be found near the computer (10%).

However, users are not completely apathetic to the risks posed by insecure passwords. The survey shows that 72% use distinct passwords for financial services and social networking sites. But many still place too much trust in third parties. In particular, 40% assume that the sites they visit have reliable protection for password databases and keep them safe from cybercriminals. In reality, many sites store passwords under encoding that is publicly known and therefore easy to decode.

Mobile devices – widely used, poorly protected

People actively use their devices to work with sensitive data



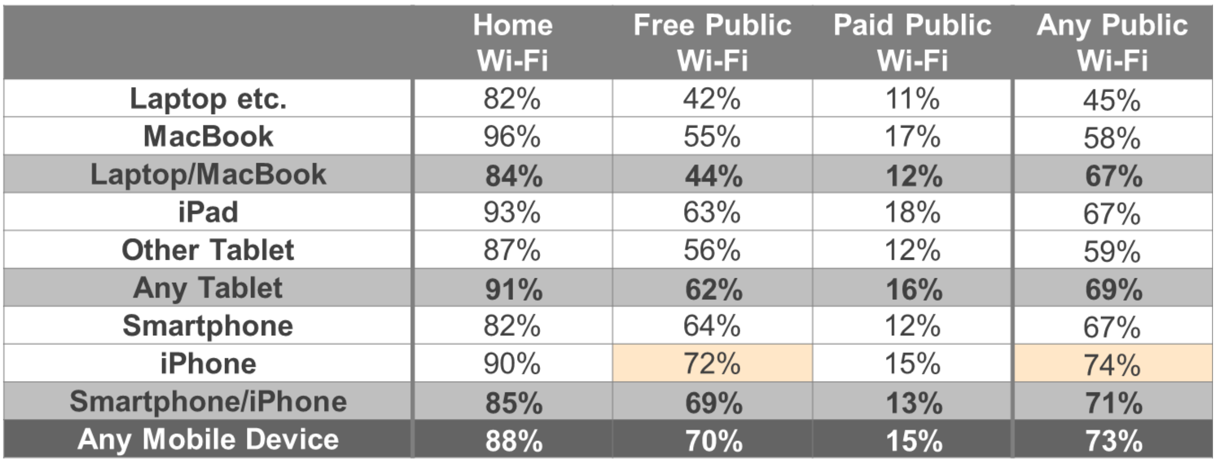
Device	iPad	Other Tablet	Other Mobile	Smartphone	iPhone	Blackberry
Base	**1,720**	**864**	**750**	**2,337**	**1,639**	**504**
Photos / videos / music created by you	78%	65%	71%	76%	81%	59%
Personal email messages	73%	61%	55%	64%	78%	59%
SMS or MMS	25%	23%	66%	72%	70%	74%
Passwords to personal & email accounts	20%	23%	26%	22%	24%	21%
Work emails messages	33%	28%	31%	32%	41%	65%
Files for work use	29%	29%	16%	20%	18%	32%
Files for personal use	43%	50%	24%	34%	33%	25%
Address book/phone contacts	59%	40%	80%	82%	87%	81%
PIN codes/passwords for online banking	10%	10%	18%	11%	14%	16%
Other banking details	13%	10%	13%	11%	16%	13%
Passwords for corporate / work accounts	9%	9%	12%	7%	11%	17%
Coursework, study materials	3%	3%	2%	2%	3%	1%
Any Of The Above	**95%**	**88%**	**96%**	**96%**	**98%**	**97%**

Personal mobile devices are often used to store what is, in fact, very important personal data. For example, 22% of smartphone owners (not including iPhone owners) store information needed to access their personal email accounts, and another 32% store their work email account information on their phones as well. Tablet owners (not including iPads) do the same: 29% store their work documents on these devices, while 28% store work email information, and another 23% store the information needed to access their personal email accounts.

Meanwhile, smartphones and tablets are also used to store personal photographs, videos, and audio files. An average of 65% of those surveyed stated that they use their always-on devices for these purposes.

Mobile devices are now frequently used to store critical data. In addition, people often use smartphones and tablets to access all types of online services, which can pose a major security threat. This is particularly true when an Internet connection is established via Wi-Fi.

Few people think about online security for mobile devices on Wi-Fi



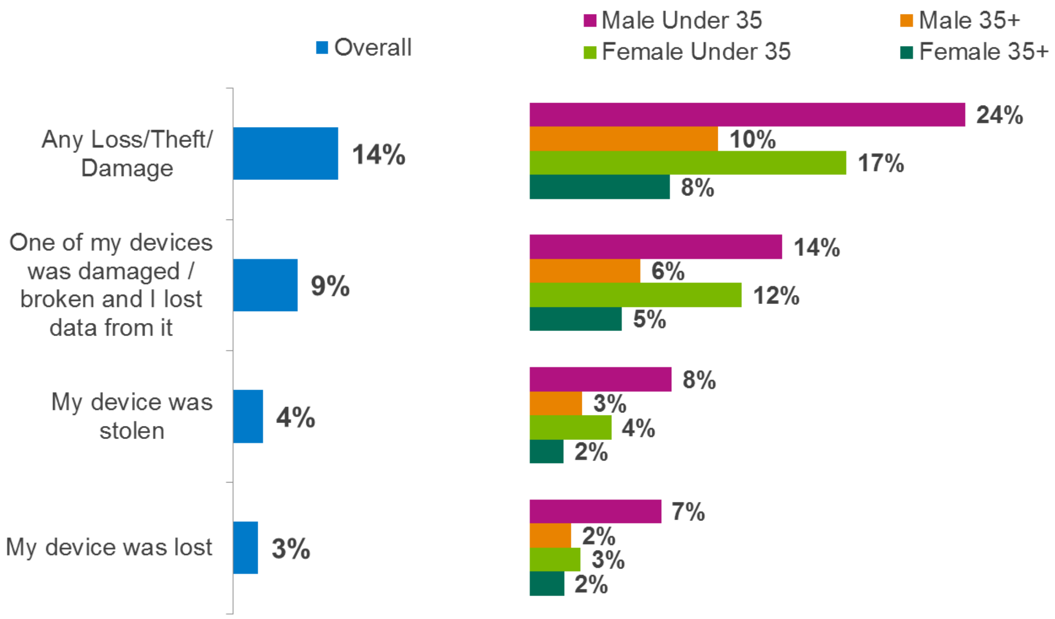
	Home Wi-Fi	Free Public Wi-Fi	Paid Public Wi-Fi	Any Public Wi-Fi
Laptop etc.	82%	42%	11%	45%
MacBook	96%	55%	17%	58%
Laptop/MacBook	**84%**	**44%**	**12%**	**67%**
iPad	93%	63%	18%	67%
Other Tablet	87%	56%	12%	59%
Any Tablet	**91%**	**62%**	**16%**	**69%**
Smartphone	82%	64%	12%	67%
iPhone	90%	72%	15%	74%
Smartphone/iPhone	**85%**	**69%**	**13%**	**71%**
Any Mobile Device	**88%**	**70%**	**15%**	**73%**

Table shows the % of respondents owning each device who use Wi-Fi

An average of 69% of respondents with a mobile device that can connect to the Internet say they use Wi-Fi connections, while 70% use free public access points.

When working with these types of hot spots, it’s important to take additional security measures, since Internet traffic could be intercepted by malicious users. However, few users recognize this. As many as 34% of those surveyed stated they do not take any additional security measures when they connect to public hot spots. Another 14% reported that they are not concerned about using open access points when using services that process personal financial data, such as online stores, online banking services, and e-payment systems. Just 13% of surveyed mobile device users said that they ask about the encryption standards used before connecting to hot spots with their personal devices.

Loss or theft: fewer than 25% of respondents use anti-theft software for mobile devices

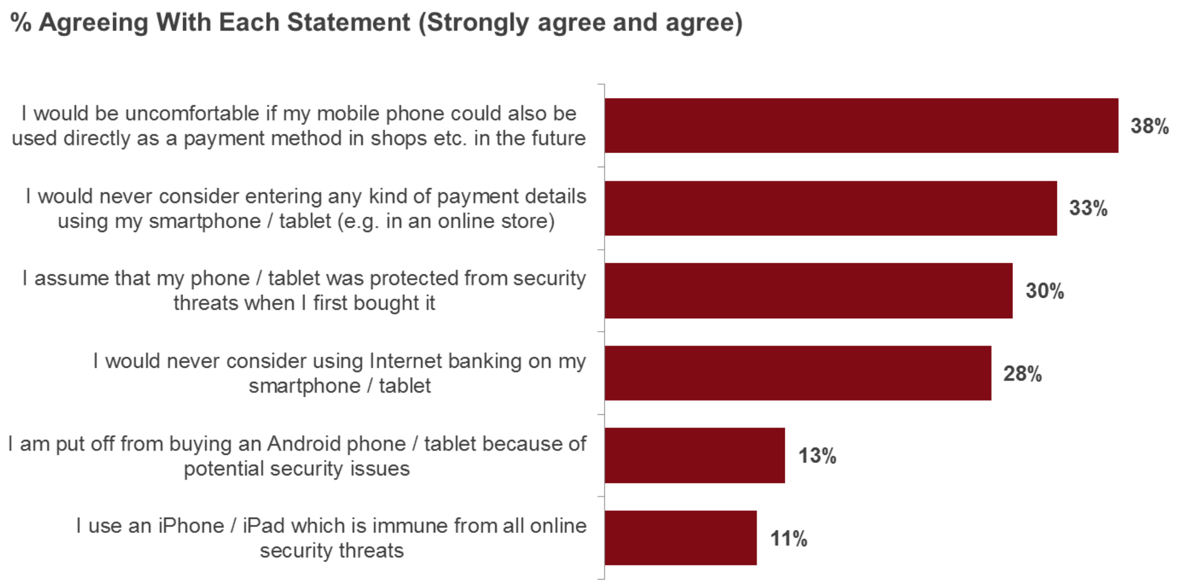


About 14% of respondents reported that over the past 12 months, one of their online devices was lost, stolen, or broken. The most common occurrence noted is a damaged device (9%). The theft or loss of a mobile device was noted less frequently (4% and 3%, respectively). At the same time, the loss or theft of mobile devices (7% of respondents combined) takes place more often than incidents related to the loss or theft of payment cards (6%), wallets (5%), wristwatches, house keys, or passports (3% each).

According to the study's data, mobile devices are stolen relatively rarely. However, when reviewing these numbers, it's important to keep in mind that even though over 8,500 people took part in this survey, the experts at B2B International made an effort to ask the group of people who best represent a typical mobile device user. In light of this fact, it would be possible to extrapolate the survey results to a global user base of mobile device users in order to get an idea of the actual scale of the problem of mobile device loss and theft. If we look at just the smartphones (whose numbers are in the billions according to various research firms), then it stands to reason that each year roughly **40 million** smartphone users become victims of theft, while approximately **30 million** lose their personal devices.

Some 50% of respondents said they block their SIM card immediately after discovering the loss or theft of their mobile device. Slightly less (43%) stated that they change their online account passwords. Nearly 41% of those surveyed use an app that allows them to remotely block access to a lost or stolen device. Considerably fewer users (24%) resort to a specialized mechanism that can remotely delete all sensitive data from a device, or photograph the face of the person that took the phone (12%) in order to subsequently submit that photo to the police.

Almost one-third of people mistakenly think their devices include protection out-of-the-box



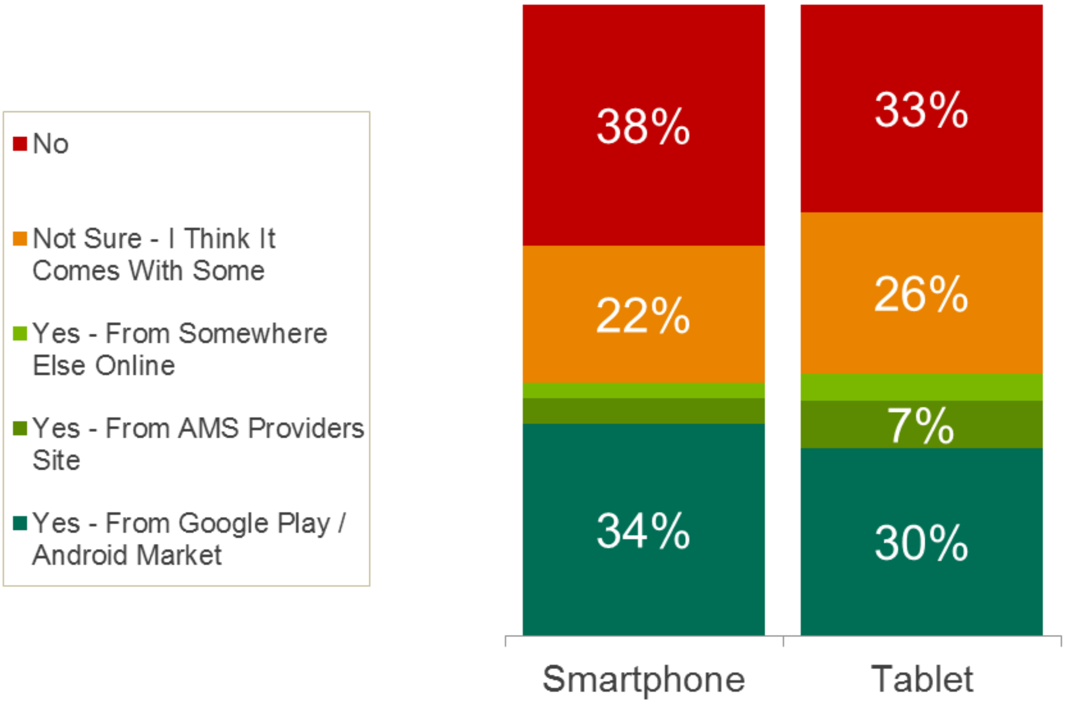
In general, a large number of users do not completely trust the level of protection against cyberthreats on mobile devices. For example, 38% noted that they would not feel secure if they needed to access online financial services with their smartphone or tablet, and 33% said they would never do so. Another 13% of those surveyed reported that they decided against purchasing a mobile device running Android — currently the most popular mobile operating system — based on what they hear about security. There are constantly new malicious programs being reported on Android, and the OS's vulnerabilities have damaged consumer trust in the Android system.

When asked about the security of their mobile devices, a substantial number of users expressed opinions that actually contradict fact. For example, 30% of respondents presume that the smartphone or tablet they purchased already feature protection against cyberattacks right out of the box, and this is not always the case. Only a handful of smartphone manufacturers build security solutions into their devices, and when they do, the software is typically the simplest available, with very limited functions.

Furthermore, almost every tenth user of a mobile device made by Apple — an iPhone or an iPad — state that one of the reasons they chose their device was precisely because of its invulnerability to hacker attacks. In fact, these devices are much less frequently the target of malicious attacks than Android devices. However, there are still holes in their security systems, just like any other mobile device, and information about these holes is made public on a regular basis.

All the same, Android remains the primary subject of discussion when it comes to security on mobile devices.

Security solutions for Android still not widely used

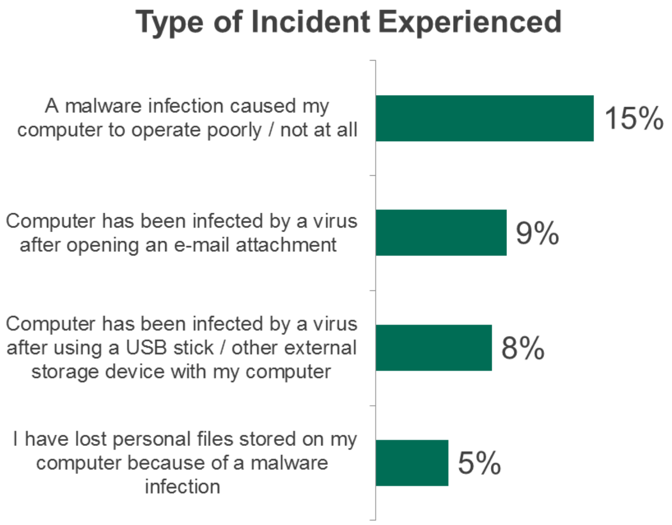


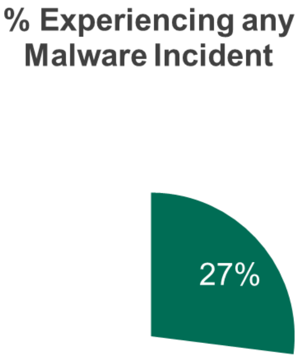
Remarkably, even though the level of concern about mobile device security against cyberthreats is high — including those running on Android — the security solutions available to protect these devices are not used by many. Just 40% of smartphone owners and 42% of Android tablet owners reported using these types of products. And the situation involving the use of encryption is potentially even more of a threat: 81% of tablet users and 84% of smartphone owners said that they don't use any kind of encryption technology to secure their personal data.

This situation is particularly worrying when one takes into consideration the variety of cyberthreats that the owners of mobile devices have encountered.

Cyberthreats: 1 in 4 users fall victim

Nearly 20% of all malware attacks resulted in the loss of sensitive data

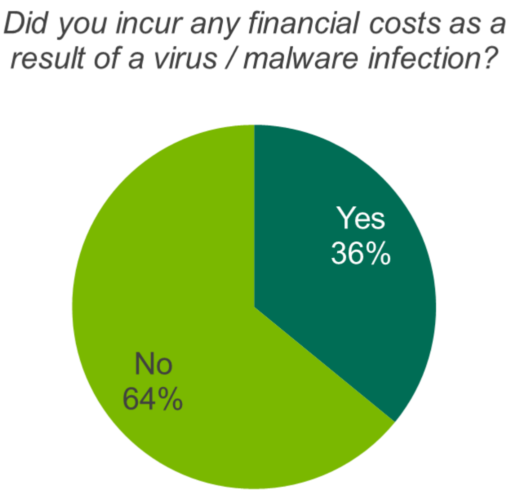


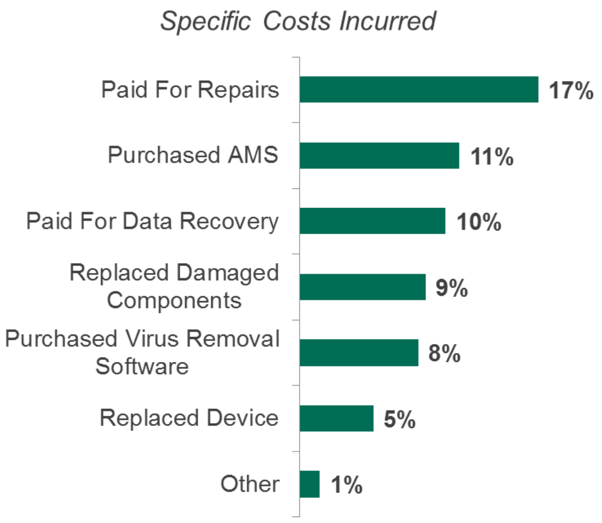


Altogether, nearly 27% of those surveyed said their device had been infected at least once over the past 12 months. Most often (15%), an infection results in unstable performance, or the device malfunctions completely. In 5% of cases, infection has resulted in the loss of data stored on the device.

Nearly 20% of all malicious attacks led to a leakage of sensitive user data. In 61% of all cases, data restoration was not an option. Malicious attacks also led to financial losses.

Just 1 attack could cost a user up to $600

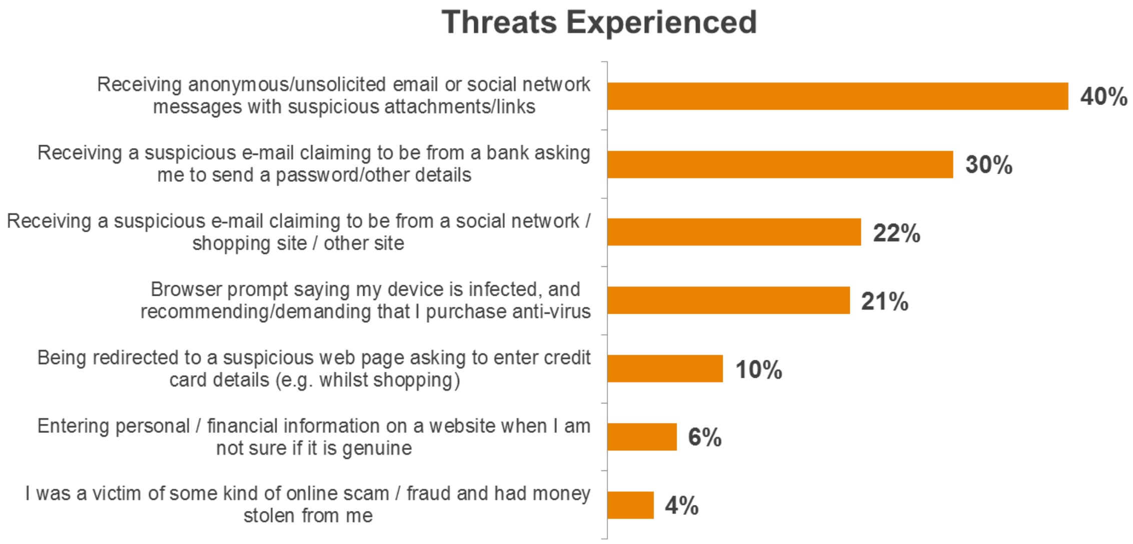




In 36% of cases, users lost money after falling victim to a malicious attack. Most often (17% of respondents) had to spend money for services to fix their device and remove the infection. Another 10% of users paid for data restoration services.

On average, one successful malicious attack against a mobile device will cost its owner **$74**. However, in some cases, the stakes are higher. For examples, repair and data restoration services can cost up to **$120**, and if the attack causes a device to completely malfunction, the cost might even reach the full price of a completely new unit — an average of up to **$600** for a new tablet or laptop.

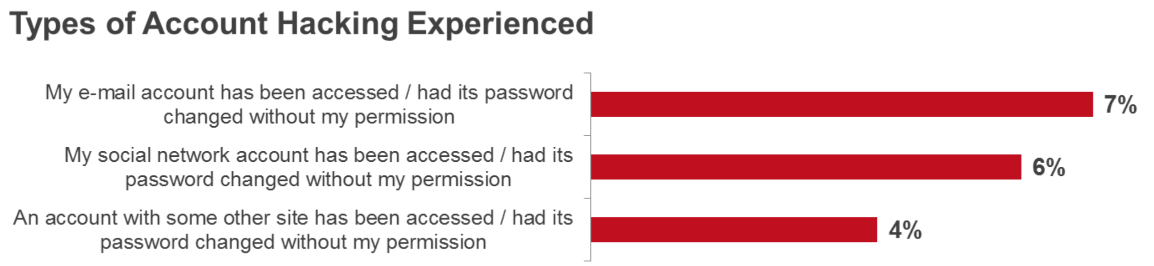
62% of mobile device owners have encountered at least one financial threat

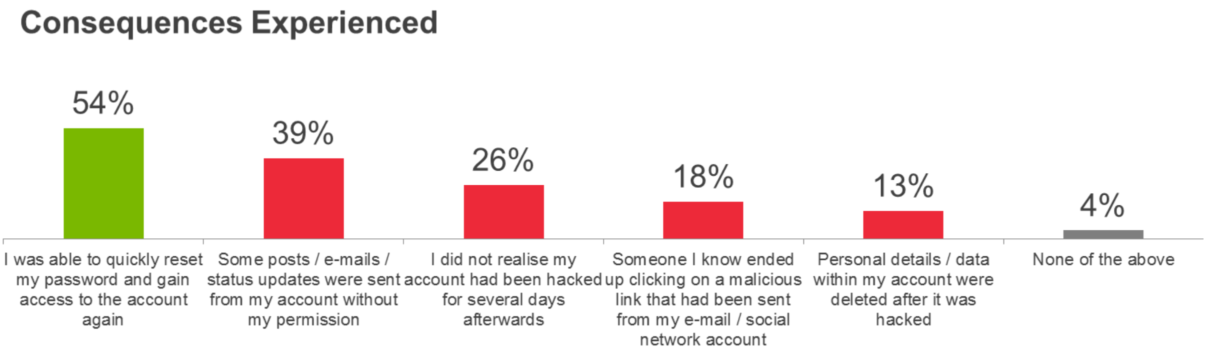


Roughly 62% of Internet users who took part in the study reported that they were targeted attacks aimed at stealing personal financial data at least once. For example, 30% of respondents stated they had been the recipients of a suspicious email claiming to be from a bank, when that was in fact not the case. Nearly 21% of all mobile device owners were subjected to attacks by malicious users distributing fake antivirus solutions, and every tenth mobile device user was redirected to a suspicious webpage and asked to enter credit card information at least once. Nearly 4% of those surveyed stated that they had fallen victim to financial scammers — and of those, 41% were unable to fully recover their losses.

Incidentally, malicious attacks do not always lead to financial losses. Victims have suffered other unpleasant consequences, as well — such as having their accounts hacked.

Unauthorized posts and deletion of personal data are typical consequences of online account hacking incidents



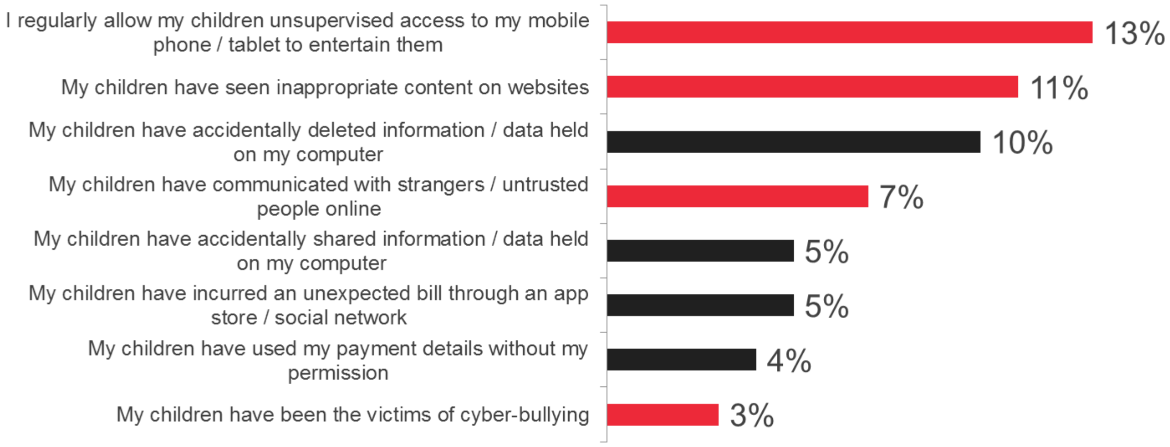


In total, nearly 14% of those surveyed had dealt with at least one incident where one of their accounts had been hacked. More than half (54%) of respondents said they were able to change their password in time and regain access to their account, but other hacking victims were left to deal with a mess. Specifically, 39% of those surveyed said that things had been published in their name, and 18% said that some of their online friends had clicked on malicious links sent from their hacked account. Another 13% said that the hackers had stolen their personal data.

For many users, any cyberattack is an attack on their virtual space which can be blocked when proper, responsible steps are taken to protect their data. However, things can get complicated when the subject turns to users with underage children.

1 in 4 kids are exposed to online risks

Typical incidents involve inappropriate content and dangerous conversations with strangers

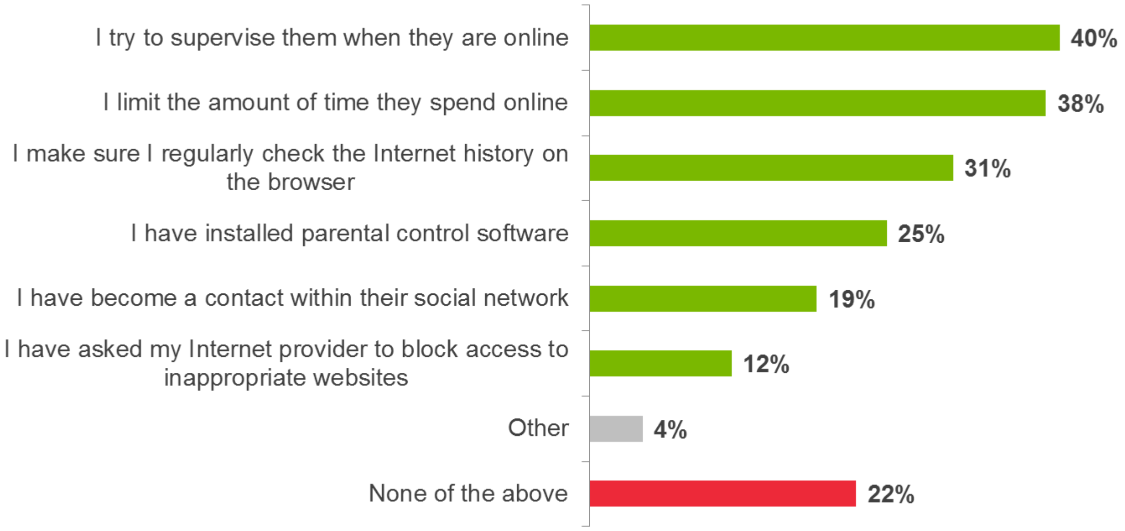


Nearly 27% of parents admitted that their children face risks when they use the Internet. In particular, 11% of children came into contact with inappropriate content, and 7% began chatting with strangers. Furthermore, 18% of parents incurred financial losses or lost sensitive personal data due to their children's actions. Often, kids accidentally deleted important information and used fee-based resources without asking permission.

Overall, 64% of parents agreed that children should not be able to use the Internet if the device they are using does not have a specialized security solution installed.

So what have parents done to protect their kids?

Many parents do nothing to protect their children online



Although most respondents believe that children require online protection, there were extreme variations in the methods they chose to achieve that goal. For example, 40% of respondents stated that they try to control what their children do online. Another 38% limit the amount of time their children are allowed to use the Internet, while 31% regularly check their children's browser history.

Some 22% of parents do not limit their children's online activities — ultimately allowing them to be subjected to the risk of encountering inappropriate content or strangers.

Meanwhile, just 25% of parents use a security solution with Parental Control features, which typically allow parents a lot of flexibility in how often and for how long a child may access the Internet, and which websites a child may visit.

Conclusion: multiple mobile devices means special security needs

Based on the survey results, we can see that it has become commonplace for one person to use multiple mobile devices, making online life interesting and convenient. However, this recent trend has also added to the list of cyberthreats to which people are vulnerable.

The functions offered by today's mobile devices let people use smartphones and tablets to record video and take photographs. Moreover, these devices have so many features, that people can use them for both personal and work-related needs. However, these practices only increase the risk of a malicious attack, or the loss or theft of a device, as well as the loss of critically important personal data, such as personal photographs, videos, audio, sensitive work documents, and in the end, this could all lead to major financial and moral damages. It is also worth noting that many users do in fact approach digital security responsibly; yet at the same time, there are also a large number of people who are perhaps too trusting — perhaps even careless — when it comes to the security of their mobile devices.

In order to minimize the chances of an incident related to the security of digital valuables, owners of mobile devices should follow several simple IT security rules:

- Use reliable security solutions on all of the mobile devices used by your family.
- Act responsibly when it comes to creating new passwords for online services, particularly those associated with financial transactions.
- When using financial services, make sure that there is additional protection in place for transactions from a specialized security product, such as Safe Money, a component included in Kaspersky Internet Security.
- Back up your valuable data regularly, not just the data on your PC, but the data on your mobile devices as well.
- Don't forget that the Internet cannot distinguish the ages of different users, and children will automatically have free access to all of the content available on the Internet. In order to ensure their security, parents should use a security solution with Parental Control features.
- Only use secure connections with Wi-Fi hot spots.

For those who own several Internet-ready devices, Kaspersky Lab offers Kaspersky Internet Security – Multi-Device*, a powerful security solution that bundles together a number of different products to ensure that the personal data of those using devices running on various operating systems (Windows, OS X, and Android) can keep their data secure. Each product in this solution is designed with advanced technology capable of countering all types of cyberattacks. These technologies are optimized for each specific platform so as to minimize any interference with the performance of a smartphone or tablet, making protection as convenient as possible.

**Set for release in September 2013*