Consumer appetite versus action: the state of data privacy amid growing digital dependency

Kaspersky Consumer IT Security Risks Report 2021

kaspersky BRING ON THE FUTURE

Learn more at kaspersky.com

Contents

Introduction

The world became a very different place in 2020. Cut off from face-to-face interaction, social media, collaboration apps and emails became indispensable communication lifelines for millions of people around the world.

The necessity of technology has tied our society to digital devices even more than before. According to a DoubleVerify study, daily time spent on consuming content online has doubled globally since the start of the COVID-19 pandemic, from an average of 3 hours 17 minutes to 6 hours 59 minutes.

By March 2020, Gartner reported 88% of organizations worldwide made it mandatory for employees to work from home after COVID-19 was declared a pandemic. Our work and personal lives began to blur online as people had many opportunities to practice their digital skills when working from home, video chat with friends, 'go' online shopping and consume social media.

Video conferencing grew from being a collaborative business tool, to the way we did just about anything; birthdays, baby showers, online quizzes, personal appointments, work meetings and everything in between. As of June 2020, use of Microsoft Teams grew by 894% compared with its base usage on 17 February 2020, and Zoom increased by 677%.

This increase in reliance on the internet to carry out daily activities means the spotlight is starting to turn towards IT security awareness at all levels. To find out the extent and attitudes towards online privacy, we commissioned research to explore consumers' main privacy concerns and measure their knowledge of digital security. The resulting findings outlined in this report aim to raise awareness and to enhance users' actions when it comes to online safety.

Methodology

The Kaspersky Consumer IT Security Risks Survey (Consumer ITSR) interviewed a total of 15,070 adult consumers globally (including those in China, India, Japan, United States, Colombia, Mexico, Brazil, United Kingdom, Germany, France, Netherlands, Sweden, Italy, Spain, Czech Republic, Poland, Russia, Turkey, United Arab Emirates, South Africa, Vietnam, Indonesia and Australia) between September and October 2020, about their attitudes towards online privacy.

Respondents were asked about their household devices, how they use them, the personal and work apps and services they use, their security attitudes and, finally, about any security incidents they had experienced in the past 12 months.

Not all survey results are included in this report.

Key findings

80%
consumers who work from home use personal computers for work-related purposes

Eight-in-ten consumers

53%
of respondents that were a target of ransomware (56%) paid the ransom to restore access to data stolen from them. Yet despite paying, 17% who paid the ransom didn't get their data back

Over half of respondents

50%
users whose devices were lost, stolen or damaged, had secret information revealed

Half of users

60%
of online users are concerned that someone could watch them via a device's camera which has been attacked by malicious software

Six-in-ten users

23%
always give apps and services permission to access their microphone or webcam

Almost a quarter of users

50%
consumers would no longer use an online service provider following a data breach

Half of consumers

The impact of shared devices in households

To understand consumer awareness of online privacy and security, it is important to first look at the device environment in each household and the habits and behaviors associated with them.

When it comes to home computers, user behavior is commonly based around convenience and ease of use. **For a third** of personal computer users (**35%**), the **main computer in their home is shared with older members of their household or with children** (**13%**), **3%** even share access with colleagues and friends. This is where users can benefit from security awareness to help them optimize shared devices for safety and privacy.

The issue is exacerbated further when you look at what the devices are used for. **As many as eight-in-10 consumers who have computers at home regularly use their personal computers for work-related purposes.** This is despite **over half** (**51%**) claiming that they are also provided with a device by their employer for use at home. This tells us as much about the behaviors that are blurring between personal computer usage as it does about the frequency. Crucially, it suggests that many home workers are relying on devices that are not primarily intended for work.

With many workers facing a future where flexible and hybrid methods of remote working are the norm, it is important that they are supported to protect their multi-use devices. For example, **14% of all surveyed respondents had their devices lost, stolen or damaged over the past 12 months.**

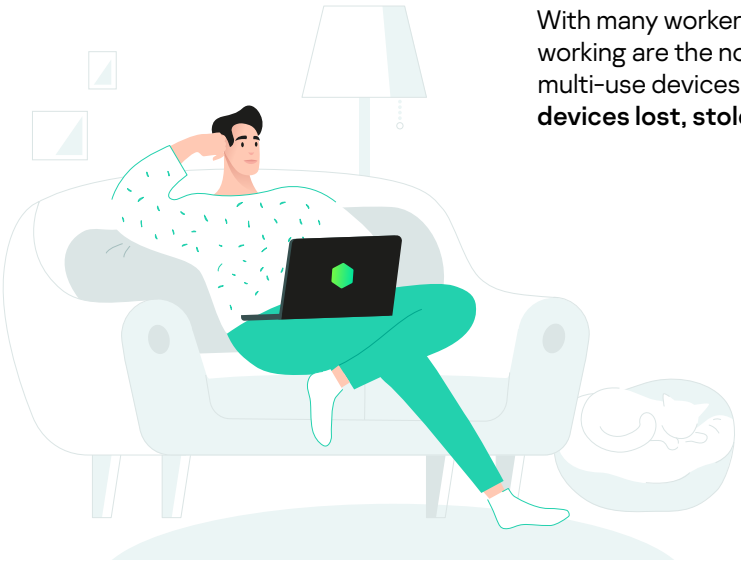
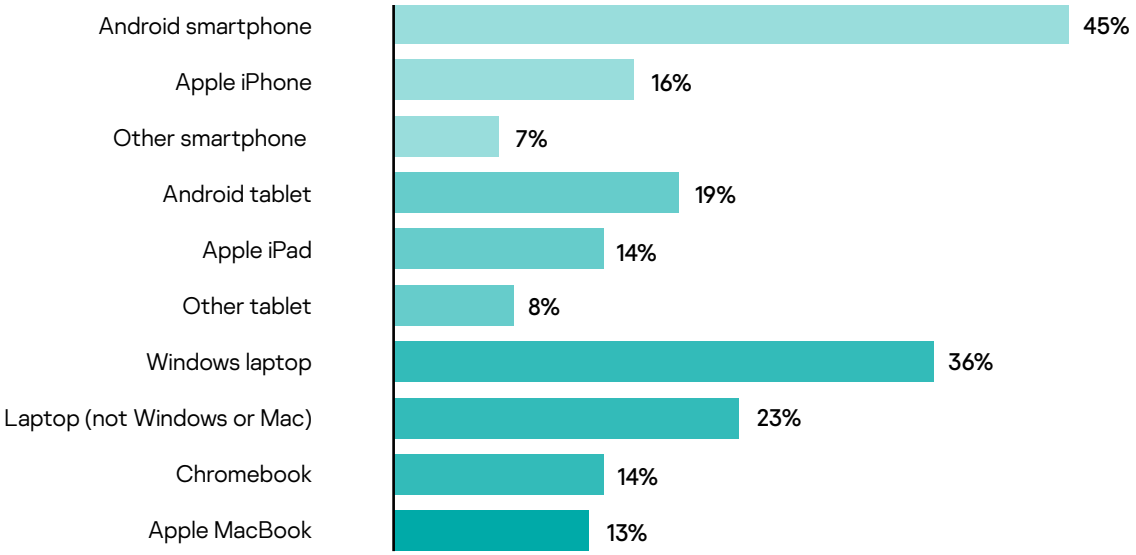


Figure 1: Breakdown of users who had their devices lost, stolen or damaged



The consequence of losing a device is, at best, a nuisance, and at worst it can be extremely unpleasant. Of the devices that were lost, stolen or damaged, the personal data of 54% was used for criminal activity, 50% had either personal or secret information revealed and 47% lost personal files.

This means that for every instance of a lost, stolen, or damaged device, half, on average, end up with data getting into the wrong hands. When it comes to damaged devices; within Windows laptops, only less than a half (**46%**) of owners managed to recover data, while **51%** of Android device users lost all the data permanently.

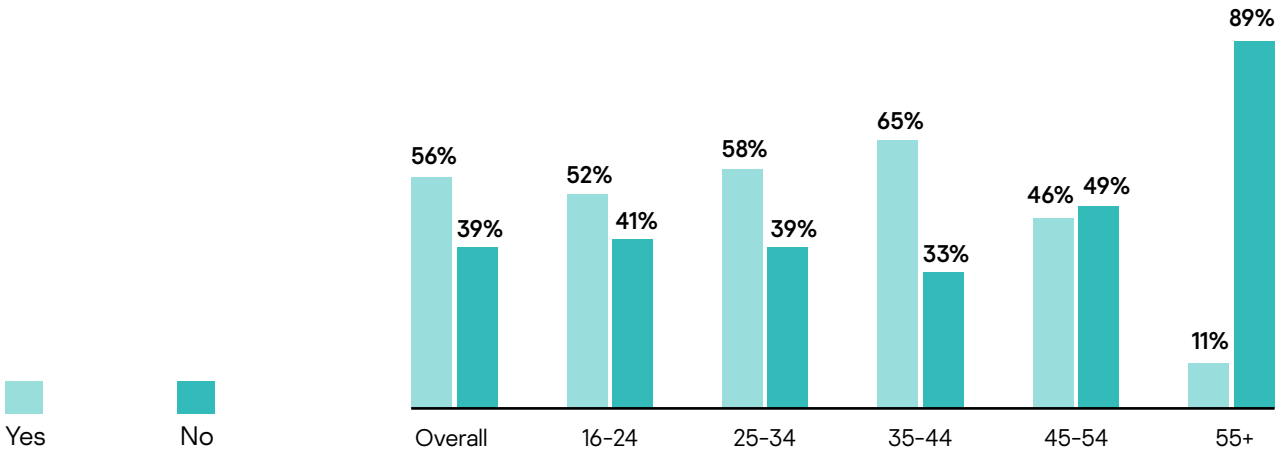
Devices don't only need protecting when they are out of our hands. Over the past 12 months, cybercriminals have taken advantage of the confusion presented by the pandemic to increase activity. This is reflected in **as many as 31% of all respondents having experienced some kind of infection or intrusion on their devices and more than half (53%) of them having found that it incurred financial costs to them as a result of infection or intrusion. The costs incurred varied between users, but for 40% it amounted to $101 or more and the average totaling $209.**

Ransomware attacks were also on the rise over the past year, most likely due to their efficacy as a lucrative means to extort money from internet users. A staggering **56%** of respondents that were affected by this form of attack paid the ransom demanded to restore access to their data. This is highest among those aged **35-44, of whom 65% paid to restore their data, compared to just over half (52%) of those aged 16-24 and a far smaller 11% of those over the age of 55.**

Not only does paying the ransom make the attack vector more appealing to the criminal underworld, but it also does not necessarily guarantee the return of stolen data, as evidenced by 17% of respondents who have paid the ransom and faced this reality. In addition, respondents lost substantial amounts of data. **Only 29% of users who experienced such incidents were able to restore all their encrypted or blocked files after an attack. Half lost at least some files (32% lost a significant amount, and 18% lost a small number of files). Meanwhile, more than one in ten who did experience such an incident (13%) lost almost all their data.**

Notably, although ransomware is on the rise, awareness of the tactic is still not very widespread. Just four-in-10 (**40%**) of all surveyed respondents had seen or heard of ransomware in the last 12 months. Of those, 29% had seen it in the media, while 11% knew someone affected by the issue. To better help consumers protect themselves against this growing form of cyberattack, they need to understand what to look out for. Therefore, it is important that users are provided with more education to protect themselves and know what to do if they are attacked by ransomware.

Figure 2: Cases of paying ransomware among users who experienced ransomware infection, by age breakdown



Consumer attitudes to online risks vs rewards

The popularity of connected devices is plain to see by their prominence in our everyday activities. And they aren't confined to our houses or in our pockets anymore – take our cars as an example.

Traditionally, a vehicle was designed to get you from A to B, but now, of the **86%** of respondents that have a car for personal use, over a third (**36%**) said that it was connected to the internet and another third (**33%**) had a multimedia center or car-PC connected to the internet. Yet, it's clear that many consumers have worries when it comes to giving the internet more access to their lives. **57% of respondents said that they are worried about their security and privacy being affected by 'smart' and internet connected devices.**

Unsurprisingly, the same can be said for our growing use of the mic and camera functions on our devices. Last year saw a near worldwide shortage on webcams with many of the leading suppliers seeing vastly increased demand for their products to help people work from home. With it harder to find devices, many consumers were less able to select the most secure webcams, and in one case, a particular webcam app left thousands of user accounts exposed online.

As a result of our increased use of webcams, our concern about them has also risen. Over half (**59%**) of people are worried that someone could watch them through their webcam without them knowing, and **60%** are concerned that this could be done via malicious software. Conversely, **only 13% never give apps and services permission to access their microphone or webcam, while 23%** always do. **With cameras and collaboration apps more important for us to connect with the world, it can be easy for users to approve video and microphone access without thinking. However, these figures show how important it is for users to reflect and make informed decisions when installing apps or services.**

This trend is seemingly less apparent among people who are 55 years and older where caution levels rise, **with 38% never giving access to their mic and camera, compared with 27%** of people aged 25-34 who always do.

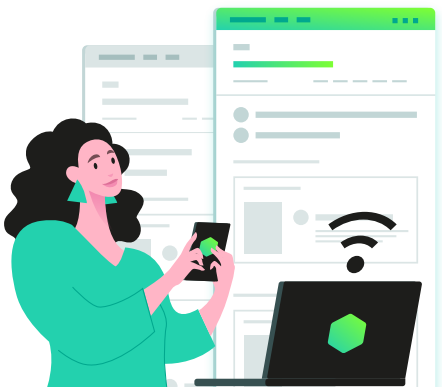
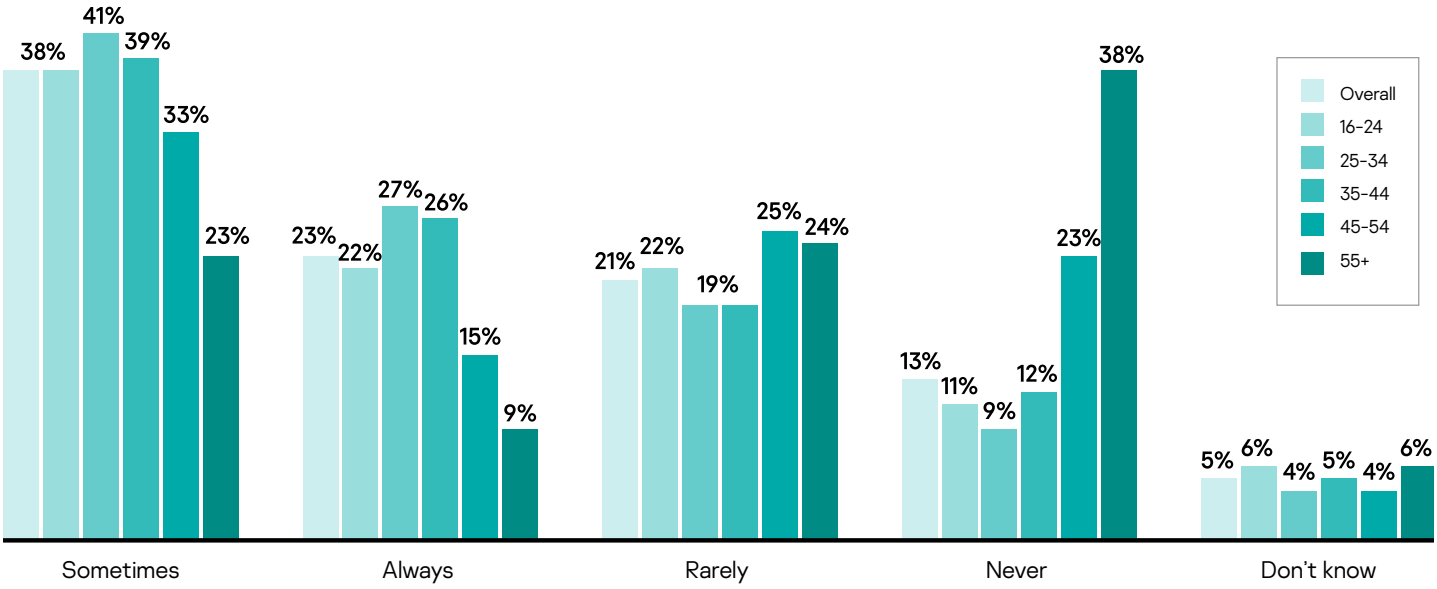
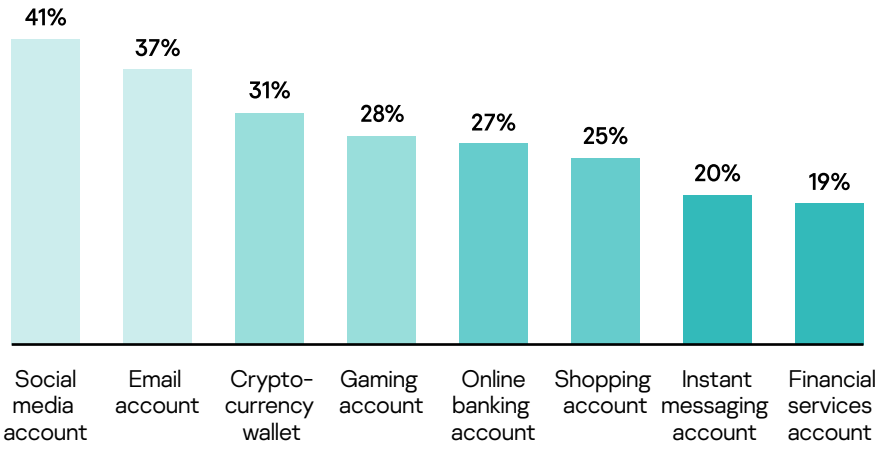


Figure 3: **Those allowing microphone or webcam access in apps and services, by age breakdown**



But there is more to the high degree of concern about our online worlds. As evidenced further back in this report, rates of account hacking attempts registered by users over the past year are rising. **28% of online users experienced attempts to hack their online accounts**, with a large number (**41%**) of these people reporting that they had their social media accounts targeted. A similar number (**37%**) **had an email account that had been targeted and 31% had a cryptocurrency wallet targeted**.

Figure 4: **Online accounts targeted in a hacking attempt in the last 12 months (multiple answers allowed)**

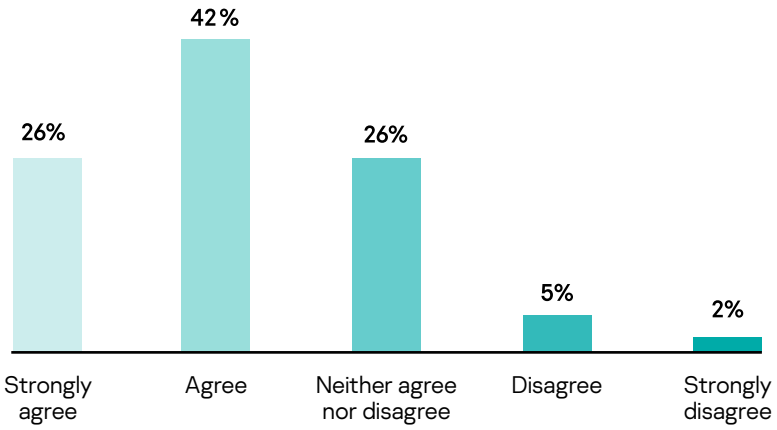


The impact of account hacking can be significant. **One third of those (30%) who lost money as a result of a scam or hack reported that they did not manage to get it back.** This increases to 55% among people who are 55 years and older, demonstrating that vulnerability can rise with age. **26% estimated that the amount of money they lost as a result of the scam or fraud was under $100, while almost one-in-10 (9%) lost a staggering sum, between $2,000 and $4,999.**

Only a quarter (26%) of all the respondents strongly agree with the statement: 'If I had a choice between privacy safeguards and convenience of online services, I'll always choose safety'.

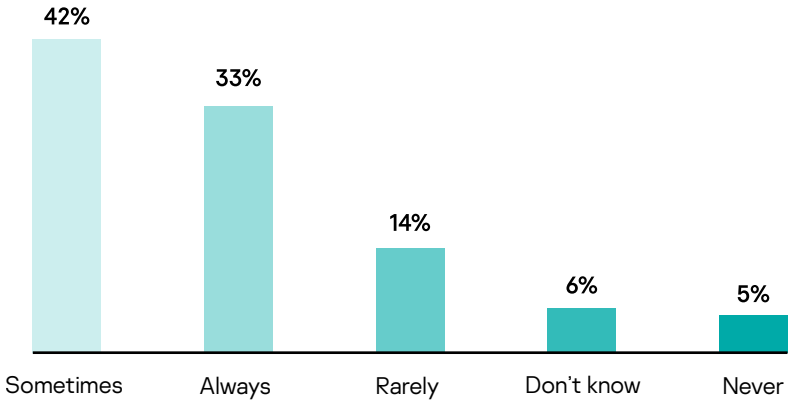
Although security incidents are on the rise, users are still developing cyber-awareness and are looking for support to help them expand their security education. Perhaps our attitude between reward and risk are weighted unfavorably due to the high degree of reward on offer with the internet. **When speed, convenience and a gratifying user experience is available to us at the touch of a button, many don't have the time or inclination to stop and assess the potential risk.**

Figure 5: **If I had a choice between privacy safeguards and convenience of online services, I'll always choose safety**



Meanwhile, concerningly, three quarters (**75%**) of people agree with default settings in apps or online services, either 'sometimes' (42%) or 'always' (33%). Default settings are often set up with usability rather than security in mind. Such a high number may either reflect a disproportionate level of trust in the apps they are using or perhaps a lack of security awareness. With internet users having an average of 8.6 social media accounts each, this is important to take into account. Whether it's the pace of our lives or our reliance on the businesses that provide the apps and services in the first place, it's clear that consumers would benefit from more education in this area.

Figure 6: **Do you choose the default settings in apps or online services?**



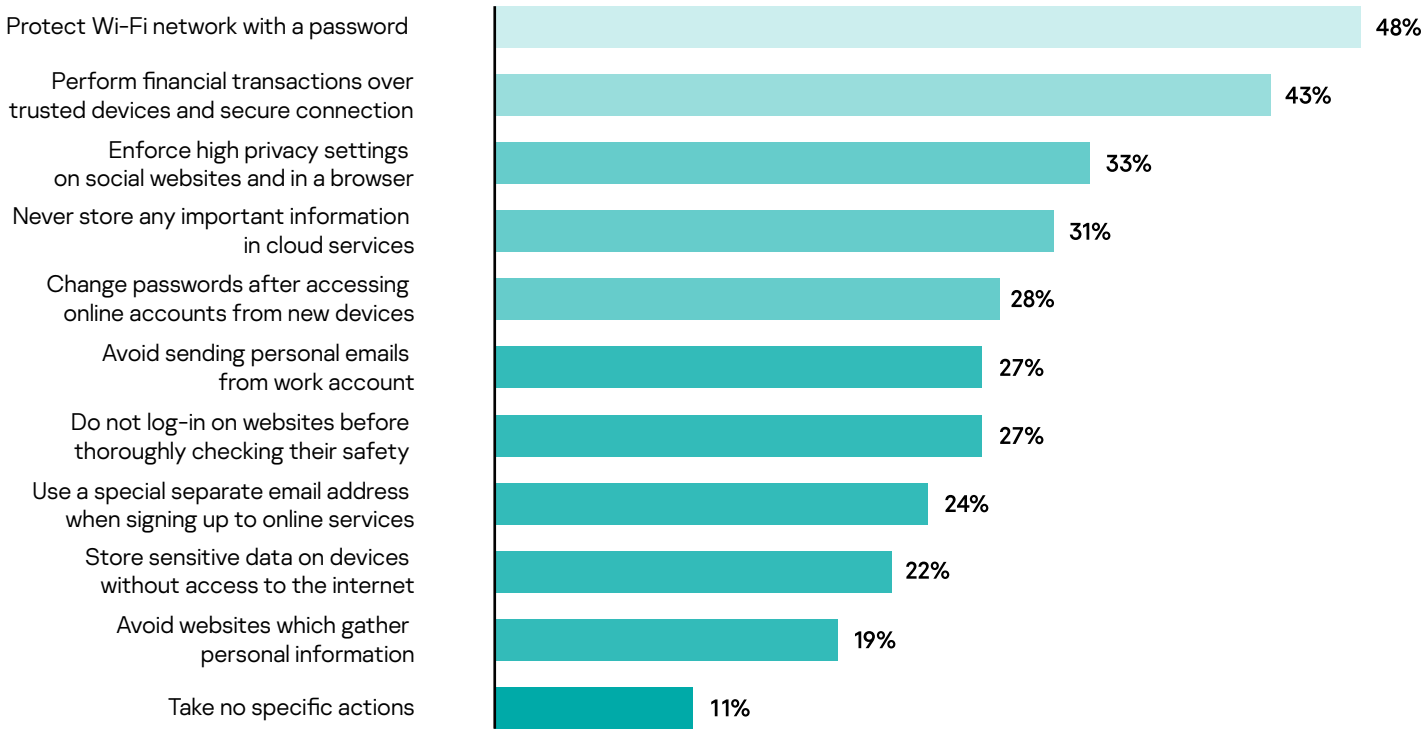
Taking action to build a strong first line of defense

But it's not all bad news; consumers have made great strides in protecting their online lives, perhaps driven in part by more safeguarding efforts by businesses offering online services, but also by greater awareness.

This is apparent by such a high number (89%) of all respondents taking some of the more common, but effective, personal IT security actions and putting them into practice to protect their privacy and keep their personal information safe.

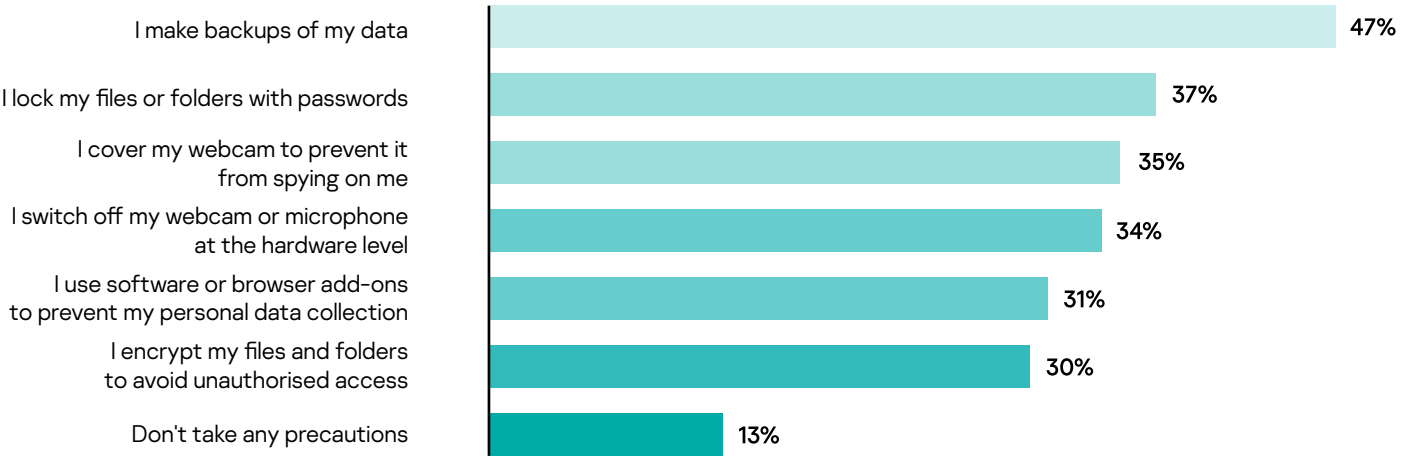
Taking time to protect a Wi-Fi network with a password is perhaps a good example of this. 48% of people are taking this necessary step to prevent outside intruders accessing their network, stealing files, and spreading viruses. As mentioned before, this may be down to greater safeguarding by ISPs and network hardware suppliers, but also with a better understanding of the simple steps they can take to protect themselves. Other actions that scored highly among respondents were performing financial transactions only over trusted devices and secure connections (43%), and enforcing high privacy settings on social websites (33%). The chart below shows the other popular security actions that people are now taking. Interestingly, only 11% of people take no specific actions at all.

Figure 7: **Actions people take to protect their privacy and keep personal information safe**



When asked specifically about computer usage, an encouraging 87% of users of this kind of device also took precautions here. Almost half (47%) take the important step of backing up their data. Perhaps this demonstrates that as much as our personal and work lives have successfully been taken online, the fragility of our data has become more apparent. Likewise, 37% of people use passwords to lock their files, ensuring that their data remains in their hands. Over a third (35%) cover their webcam to prevent people from hijacking it to spy on them.

Figure 8: Precautions taken while using computers



Many people now recognize that whilst their first line of defense includes good backup procedures and password management, they also need protection from some of the more widespread or sophisticated attack vectors online. Fittingly, the majority (**65%**) agree with a statement that antivirus software is required for good 'digital hygiene' – just like washing hands before eating. **58%** of the respondents are currently using an internet security software (excluding built-in software) on the devices (computer or mobile) they use personally.

There is also another side to this story, however. A significant **45%** of respondents do not believe that they are a target for cyberattacks and cybercriminals, with a further 30% stating they are not sure. This may be somewhat naïve given the fact that only **13%** can definitely say that they know enough about the methods of scammers and criminals to avoid any problems.

Another surprising finding is that torrenting is still a trend. A large number (**65%**) **of the respondents admitted to downloading a music torrent, 66% were downloading films and 61%** were downloading software from a torrent. This is despite our security awareness seemingly improving in other areas and the fact that torrenting sites are commonly known to be littered with malware.

Users expect greater transparency on how their personal data is used

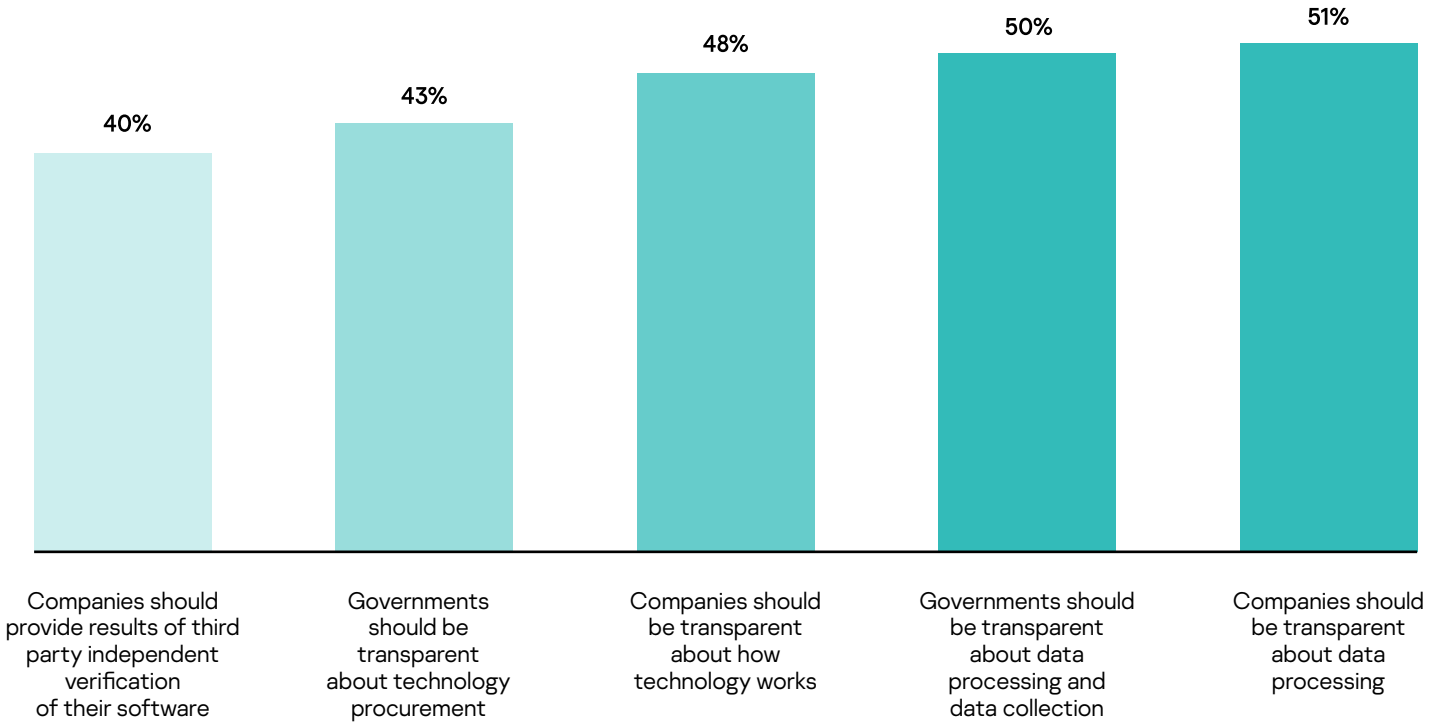
There is a growing worry about the companies that we entrust to handle our data online when using various apps and services, and a distaste about the 'big brother' effect on their ability to track our movements online. This is demonstrated by **62% stating that they worry their online activities are being constantly tracked by the websites or services they visit**.

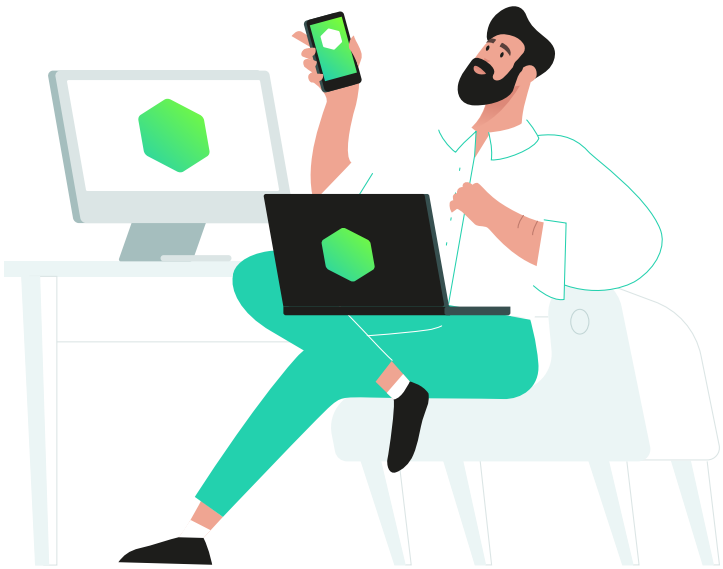
In the past 12 months, more than one-in-10 (**12%**) had their data shared or leaked inappropriately by a third party. For some this may rightfully feel like an invasion of privacy, but for others it also led to some additional negative consequences. A large majority (82%) experienced **problems** such as suspicious activity on a social media account, money loss (62%), personal or secret information being revealed (64%) and receiving suspicious emails (76%).

Many consumers take a zero-tolerance approach to this form of breach of their data and believe the buck stops with the online service provider that sold their data to a third party. This leads to shunning; with **63%** saying that they would no longer use the service provider. Another cautious number (**50%**) of people would no longer use an online service provider that collects their personal information in the event of it suffering a data breach.

Whilst consumers do not seem to disregard the need for companies to use their data to improve their products and services, they instead take a cautious approach and wish to be armed with the knowledge about how that data is used. The majority (**63%**) of people believe that transparency of technologies and companies is necessary for digital transformation. **Users rely on businesses and government to provide that transparency.**

Figure 9: How should transparency be implemented by companies or organizations?





The need for a security-first future

We're living in a world ignited by growth in consumer technology innovation and by the digital transformation of businesses. Whilst on the one hand, consumers want to wholeheartedly embrace all that the internet has to offer – we can see this with the uptake of internet-enabled devices and the apps and services that they consume – they are rightly concerned about their safety while being connected to digital devices. Their concerns are justified by the frequency of the IT security incidents they face.

There was already a trend forming towards more flexible, remote working, but in 2020, a new work-from-home mode was triggered on a monumental scale. Employers and workers do not want to lose the benefits of this change, but with it comes the need to raise common IT security awareness.

There is a movement against businesses that do not value consumer privacy. This is evidenced by **63%** saying that they would no longer use a service provider if it sold their data to a third party which was then breached. Therefore, **businesses must prioritize the transparency of how data is collected and the care that is taken when it is in their hands. This was a view shared by 51% of consumers wanting companies to be transparent about data processing.** The same must be said for businesses and the way that they take care of their workers, not only extending their protection of networks and devices when working from home but also creating a more security-aware workforce.

It's important for individuals to keep in mind the following steps to maintain a good level of online privacy:

- **Enjoy a safe and private internet experience by equipping all your devices with a reliable security solution.** If budget is an issue, even a free service is better than no protection at all and will significantly reduce the risk of getting infected
- **Update programs and operating systems often.** Within these updates, vulnerabilities are patched which means that cybercriminals can no longer exploit them
- **Choose an encrypted Wi-Fi connection to keep your computers and information safe from prying eyes.** When working from home you can set up home network monitoring with a solution like Kaspersky Security Cloud, which also offers a wide range of tools like anti-ransomware, mobile security, password management and more
- **When you have to connect to public Wi-Fi, consider using a virtual private network (VPN).** It protects your data and doesn't keep your history of visited sites, search queries, or other actions, so you can be reassured about your privacy
- **Change account passwords regularly, as well as default passwords for your devices and router.** Default passwords are too weak and already known across the internet
- **Finally, remain vigilant to malicious, yet convincing emails and always be aware of privacy safeguards within all apps and services.**

Digital environments will continue to revolutionize the way we live, but with these advances comes an increased need for security awareness and support. With increased education about cyber-activity, consumers can improve their cyber-identity. Above all, we should be aiming for a security-first approach to help us get the most out of technology.

Cyberthreat news: securelist.com
IT security news: business.kaspersky.com

kaspersky.com

kaspersky

GBD-7688 Q1/21 V1