KASPERSKY lab THE POWER OF PROTECTION

The true value of digital privacy: are consumers selling themselves short?

Kaspersky Lab Global Privacy Report 2019

March 2019

Introduction

Sharing personal and valuable information online has become essential in modern life. A decade ago, the majority of organizations were still prepared to interact with their customers through physical means. But now the tide has turned, and businesses rely on consumers using digital platforms to complete transactions – and vice versa.

In the banking arena for example, figures suggest that the use of mobile banking will reach 2 billion by 2020, representing more than one in three of the global adult population. That is a lot of consumers trusting their devices and the internet with sensitive personal and financial information. But whether it's online or mobile banking, shopping or renewing a passport online, there are a wealth of reasons why sensitive data is shared via the internet for business and service transactions.

Even when it comes to the way we communicate with friends and make our opinions known, a lot has changed in 10 years. For instance, when social media platforms first launched in the mid-2000s, many users didn't worry about posting their personal information for all to see – such as addresses, date of birth and photographs – so anyone could find it. But now, people are being urged to protect their data from falling into the wrong hands and potentially used against them – be it by cybercriminals looking for financial gain or another third party looking to take advantage such as a disgruntled friend or potential employer.

While transacting and communicating via the internet makes things easier and more immediate, there is also the terrifying possibility of losing control over our personal data, or what we openly share online leading to serious consequences in our everyday lives. The Facebook data breach in 2018 is a prime example of when people's sensitive details were put at risk. In the same year, Quora accounts were also breached, with names, addresses, personal data and account passwords accessed by cybercriminals. While these two examples centre around cybercriminal activity for monetary gains, the threats to our data could be much closer to home and have far reaching effects.

But, despite outrage and worry around high-profile scandals, is this concern translating into good personal 'data hygiene'? The information we commit to and share online – at any time in our lives – can have a huge impact in the real world. It has become popular for the entertainment industry to demonstrate how potentially insecure the internet is and that users must remain cautious. A great example is an episode of Black Mirror called 'Shut Up and Dance', in which a young man believes he has downloaded a safe anti-malware tool, only to discover his entire life has been ruined by a mysterious hacker.

Despite governments and the mainstream media encouraging users to keep their personal information private, many of us still find it a challenge. Even when we take steps to keep information safe or to stop cybercriminals accessing personal and confidential data, many of us simply do not believe that keeping this secure online is achievable in today's modern digital world. We must also consider that consumers are not necessarily as worried about cybercrime as the media would like us all to believe.

To understand consumer attitudes and expectations around data privacy, Kaspersky Lab surveyed over 11,000 consumers across the globe, the findings of which form the basis of this report.

Methodology

The Kaspersky Lab Global Privacy Report 2018 is a study into the state of consumer attitudes towards online privacy.

A total of **11,887** consumers were surveyed in **21** countries.

Key findings

- Only two-fifths (41%) of consumers are more worried about their digital and online privacy than their offline privacy, despite media hype and high profile data breaches
- Cybercriminals top the list of the people consumers are most afraid of accessing their data online. But the internet in general and the government closely follow as the most feared of prying eyes
- A quarter (25%) of consumers cover their webcams to keep data private
- Over a third (39%) of people would accept money in exchange for giving a stranger complete access to their private data online
- More than half of consumers (56%) believe keeping information completely private on the internet is impossible
- Almost half of respondents (46%) had their private data accessed via online accounts without their permission

What is fuelling data privacy fears?

With nine in ten (89%) consumers going online several times a day, the internet has become inextricably linked to everything we do – from shopping and watching movies, to making our next career move and socializing.

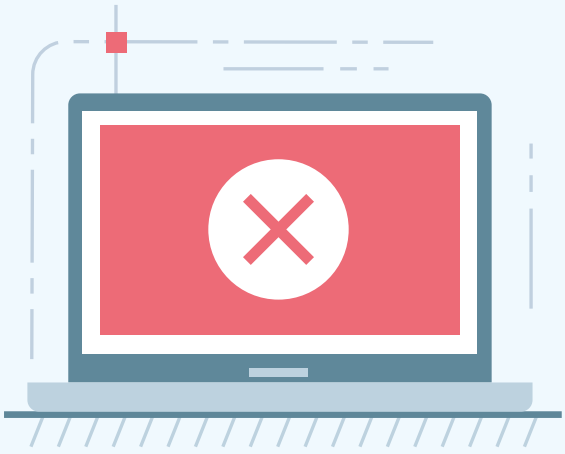
But while more and more transactions are carried out online, and consumers constantly told by media pundits and regimes to safeguard personal and confidential data, people are still more worried about what happens in the physical world than in the digital space. Less than half (41%) of consumers are more apprehensive about what happens to their information online than offline. Yet those who are concerned about cybercrime are made to feel even worse by the seemingly daily occurrence of data breaches or cyberthreats hitting the headlines – striking doubt into the mind of even the most tech savvy user.

As a result, cybercriminals lead the way as the people we are most afraid of seeing or having access to our private data. This is closely followed by the internet in general and the government. The apps we use and rely on daily are also cause for concern among internet users, with two thirds (68%) of people worried about their data being collected by these apps on their mobile devices.

And according to our data, it is not just financial fears or identity theft that is worrying consumers about people having access to their private data. Despite a more tolerant global society, the online world is marred by cyberbullying, stalking and trolling, with many people hiding behind an online persona to inflict pain on others. As a result, for almost three-quarters (72%) of consumers we spoke to, other people knowing their sexual orientation is a concern and something they would rather keep secret when online. This concern by consumers is starting to translate into action by some social media apps, with the likes of TikTok making it easier for users to protect themselves from online bullying by setting filters to block potential hurtful and harmful comments.

So, it seems that despite our reliance on the internet, many consumers are still worried about just who could have access to their personal data and the potential repercussions.

TOP-5 – Who are we most afraid of seeing/having access to our private data?



- Cybercriminals
- The internet
- The government
- Social networks
- Big IT companies

Top five entities we are most worried about seeing our personal data

Keeping personal data from prying eyes

What are worried consumers doing to help keep these fears at bay? Our study found that around two-thirds (62%) password protect their devices to keep information private and when it comes to securing online accounts, over two-thirds (68%) try to use only strong passwords. A third (35%) regularly check and change privacy settings on the devices, services and apps they use (rising to 42% of 16-24 year olds and dipping to just over a quarter (28%) of the over 55s).

We've all heard the story of Mark Zuckerberg covering up his webcam with tape to stop prying eyes, but despite this sounding like paranoia, webcams and microphones on devices are another potential entry point for cybercriminals to gain access to your personal details – even if you are not a celebrity or in the public eye. One family in Texas had their Nest camera hacked and received threats of kidnapping and assault aimed at their baby son. A woman in the Netherlands also got a shock when her webcam started moving and following her across the room, as well as speaking to her, after being hacked by a sexual predator.

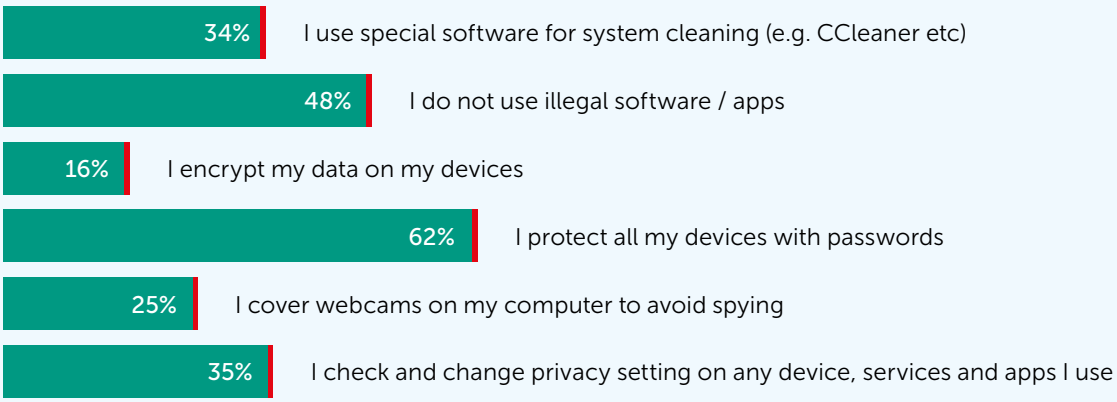
The recent admission by Google that its Nest Guard home alarm products contain a microphone which was not disclosed to users, also serves as yet another example of the vulnerabilities associated with our reliance on digital devices. Indeed, our research found that as a result, a quarter (25%) of internet users do cover their webcams to keep data private, and when it comes to encrypting data, one in five (21%) men do this compared to just 11% of women.

Consumers are also wising up to the dangers and vulnerabilities of using illegal apps, with 48% of people steering clear, in a bid to protect their data (rising to 58% of the over 55s we spoke to).

For those consumers with children, keeping their online activities safe from prying eyes also includes their children. For those with kids under 18, it seems they take extra measures to stop their children stumbling across information they shouldn't – with 53% regularly reviewing and clearing their web browser history to cover their tracks.

Taking these steps to keep data safe is certainly a great place to start, but solely relying on technology to keep information private online is only part of the solution. Delving a little deeper into how much we really value and protect our information, many consumers are – perhaps unwittingly – putting themselves at increased risk by not playing safe with their personal data. This could undermine all of the measures put in place to keep it secure.

Do you regularly do any of the following to keep your data private on your devices?



How people keep their data private on their devices

One step forward, two steps back

For all the good measures that consumers take to try and limit their data being misused or falling into the wrong hands, over half of internet users (56%) feel that complete privacy in the modern digital world is impossible. The number of people who feel this way is higher amongst those aged over 55 (63%), compared to those who have grown up with technology and a life online.

So, as we have made peace with the fact that we can never guarantee our digital security, many of us are choosing to sell-out when it comes to securing the integrity of our data and persona online – but with big potential costs. In fact, many people are unwittingly making themselves an open target.

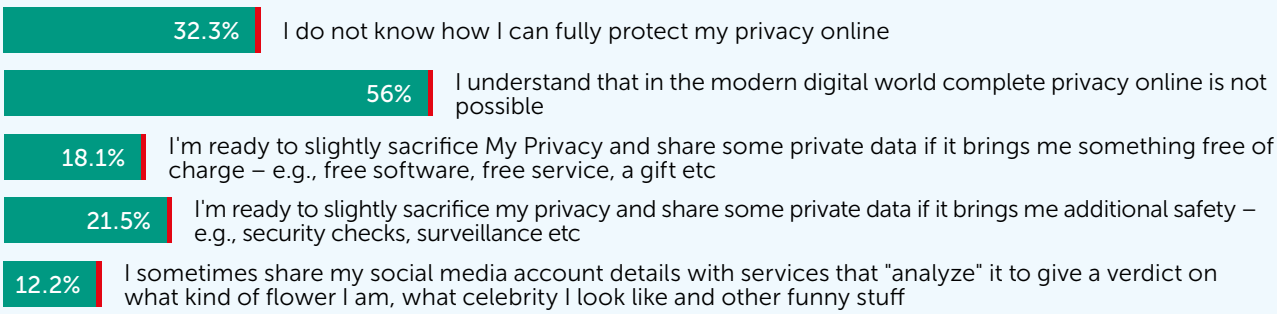
Despite the very real consequences associated with personal data being misused or falling into the wrong hands, one in five (18%) people would happily sacrifice their privacy and share data if they got something for free. 39% would even accept money in exchange for giving a complete stranger full access to their private data, with 37% saying they would sell it for $1 million. It is a sum of money that would let you hire a butler, a valet, a private chef, a personal secretary and a housekeeper for two years. Alternatively, you could use the money to buy a supercar, such as the McLaren Senna, complete with transparent doors, 789 horsepower, and 590 torque; or invest in a one-bedroom Manhattan apartment. However, with internet users more likely to share their private data if there is something in it for them, taking this short-term approach can lead to long-term damage.

Social media sharing, for example, can also be a downward spiral, with many of us reckless with data and personal information online in a bid to achieve short-term gains and social 'likes' – with often disastrous long-term consequences. You only need to look at recent cases such as the James Gunn or Kevin Hart Tweets to see how the data you publicly post online could come back to bite you in ways you could never imagine – damaging reputations and careers.

Whilst this might sound an extreme scenario, for the 'man on the street', it is also becoming more common for employers and potential employers to scour LinkedIn, Instagram, Facebook and Twitter to check that staff and candidates are reputable and workers not bringing the company into disrepute.

Employees themselves also need to be wary of revealing too much about themselves and their jobs on social media. Indeed, figures from Career Builder[1] suggest that 57% of employers have found content on social media that caused them not to hire a candidate, and a third (34%) have reprimanded or fired an existing employee due to content they have found online.

Which of the following statements do you agree with?



The extent of privacy sacrifice and confidence in the ability to protect personal data online

1 http://press.careerbuilder.com/2018-08-09-More-Than-Half-of-Employers-Have-Found-Content-on-Social-Media-That-Caused-Them-NOT-to-Hire-a-Candidate-According-to-Recent-CareerBuilder-Survey

The reality of data misuse

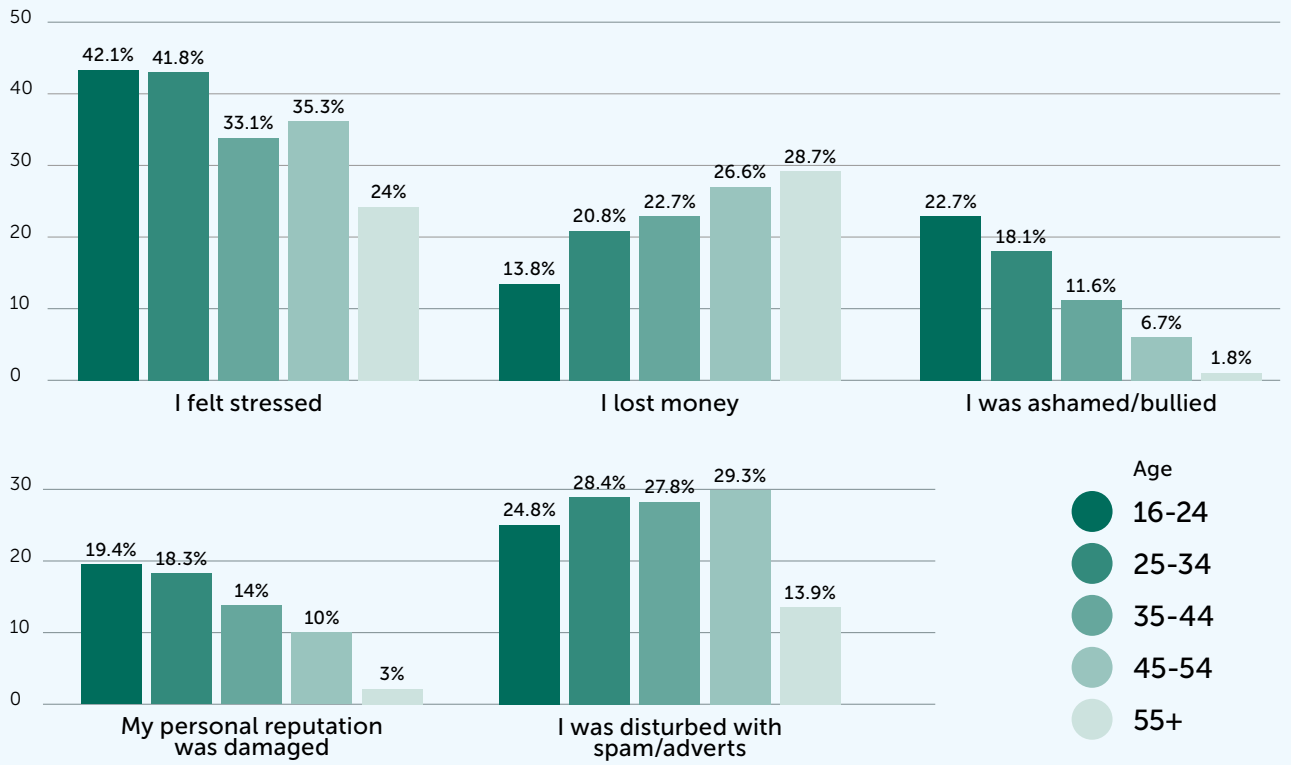
Whether we openly share it or not, if our information falls into the wrong hands online, it can have a huge impact in the real world.

From financial through to emotional consequences, the misuse of our data can be far reaching, and the effects felt for years to come. Despite media hype, online privacy breaches are very real. Our research found that over a quarter (26%) of people have had their private data accessed by someone without their consent – rising to almost a third (31%) of 16-24 year olds. For 24% of these people, their private or secret data was stolen and used. Almost half (46%) had their private data accessed via online accounts without their permission. And you don't have to look far to find examples of accounts being infiltrated and the effects of such an incident, including the Marriott data breach[2] in 2018 which affected 500 million customers and saw many become a victim of identity fraud as a result.

With cybercriminals being a main source of concern for consumers, there is often complacency that exploitation of our personal information can be much closer to home. Take the recent story of when a musician's[3] former girlfriend used his email account to turn down a music scholarship in a bid to prevent him from moving away from Montreal. The people we love can also become the people who deceive and threaten us, so trusting even them with our personal information has the potential to lead to dire consequences.

It is evident that the consequences of personal data misuse are wide and varied but more than a third (36%) of those affected felt stressed when it happened – rising to 42% of 16-24 year old respondents. One in five (21%) of the consumers we spoke to have experienced monetary loss and a quarter (25%) were disturbed by spam and adverts.

What were the consequences of data leakage?



Differences between age groups in data breach experience/consequences

2 https://www.travelandleisure.com/travel-news/marriott-paying-new-passports-after-data-breach

3 https://www.telegraph.co.uk/news/2018/06/15/clarinetist-awarded-214000-damages-girlfriend-faked-rejection/

Striking the right balance

Despite our fears and the realities associated with online data use, data privacy is and should be achievable by everyone. Secrets can stay safe and data loss should not be an expectation but an exception when transacting online. Good digital hygiene and an awareness about the importance of online privacy and how to safeguard yourself could stop you and your data from becoming compromised.

To help keep your online world private and stop you from falling victim to data misuse, there are some simple steps to follow:

- Think twice before you post on social media channels. Could there be wider consequences of making your views or information public? Could content be used against you or to your detriment now or in the future?
- Don't share passwords to your online accounts with family or friends. It might seem like a good idea or a convenient way of sharing accounts with loved ones, but it also adds to the likelihood of passwords being uncovered by fraudsters. Keep them to yourself and safeguard your private information to protect you, should relationships turn sour.
- Take your online privacy seriously and don't share or permit access to your information with third parties unless absolutely necessary, to minimize exposure of it falling into the wrong hands.
- A combined solution of security products and practical steps can minimise the threats and keep your data safe online. Reliable security solutions for comprehensive protection from a wide range of threats – such as Kaspersky Security Cloud and Kaspersky Internet Security, coupled with the use of Kaspersky Password Manager to safely store your valuable digital data – can help solve the problem of keeping your personal information under control.

For more information and advice on how Kaspersky Lab products can help keep your data secure, please visit our website.

www.kaspersky.com