kaspersky

Defending digital privacy: taking personal protection to the next level

Contents

Methodology

The Kaspersky Global Privacy Report 2020 is a study into the state of consumer attitudes towards online privacy. The survey was conducted by independent research agency Toluna between January and February 2020.

A total of 15,002 consumers were surveyed across 23 countries.

Key findings

- A third (34%) of consumers have faced incidents where their private information was accessed by someone who did not have their consent. This rises to 39% among those aged between 25 and 34

- Four-in-five people (82%) have tried to remove their private information which is publicly available, from websites or social media channels, but a third (37%) of those we spoke to have no idea how to go about it

- A significant proportion of people apply additional measures when browsing the internet, to hide their information from cybercriminals (43%), the websites they visit (41%), and other individuals accessing the same device (37%)

- A fifth (22%) allow the browsers on their computers, smartphones or tablets to save and store passwords, which could easily be accessed for cybercriminal gain

- 28% claim that it is important for them to keep web searches about porn private

- More than half (54%) of people don't know how to check if their passwords have been leaked

- One-in-five (21%) are very concerned about the user data collected by apps on their mobile devices

Introduction

The rise in app usage on our devices is growing at a phenomenal rate, with predictions suggesting that by 2022 annual app downloads are projected to reach 258 billion - a 45% increase since 2017. Our increased reliance on apps to do everything from shopping to socializing can be convenient, but sharing our data through these apps can also open more windows into our personal world. It is therefore important to remain vigilant and secure in order to safely benefit from online services.

For instance, Cameo, a popular app that lets you pay celebrities to record short shout-out videos, compromised user information including customer emails and in-app messages. Even phone numbers and it falling into the wrong hands or being viewed by someone we'd rather not have the chance to see it. passwords were potentially at risk after an apparent misconfiguration of its app exposed user data.

And, with more of us now working from home, the rise in usage of video call apps – including Zoom and Houseparty – to stay in touch with colleagues and friends, has heightened the need for users to keep conversations in these apps private.

Our reliance on different forms of technology just keeps growing, as innovation and choice continues to increase. It's therefore no surprise that protecting the privacy of our personal data and interactions online is fundamental to ensuring technology continues to play a positive and essential role in all our lives. Indeed, four-in-five (82%) of us have tried to remove private information which is publicly available, from websites or social media channels, to stop

While there are many forms of regulation designed to keep our data safe and give consumers some comfort that firms will be held responsible for any mishandled personal data, there is still much more that individuals themselves can and want to do, while they continue to conduct their lives online. Personal privacy online today goes far beyond just safeguarding our names and email addresses. It's about protecting the conversations, photos and digital information that is for our eyes only.

This report looks at current consumer attitudes towards online privacy and what steps people are taking to keep private information from falling into the wrong hands. In this age of cyber-awareness, are we all doing enough to keep ourselves safe and how can we continue to safeguard the future of our online and offline lives?

The true extent of personal privacy

With figures suggesting that by the end of 2020 there will be 20.4 billion connected devices in use across the globe, that's a lot of people, sending and storing a lot of data over the internet. But just how secure is the information that we entrust to everyone from retailers and banks, through to social media sites and dating apps?

The pace of privacy

In 2019, a third (34%) of people we surveyed claimed that they had faced incidents where their private information was accessed by someone who shouldn't have been able to. While this might not seem a very high number, 29% of the cases where information fell into the wrong hands was used or shared in some way – resulting in financial losses and emotional distress, among other consequences. For more than a third (35%) of those affected by an incident, it meant that someone was able to gain access to their devices without permission.

Notable recent examples include the 2019 WhatsApp attack, and a mistake in iOS 12.4 which let hackers install spyware on iPhones, putting the security of people's personal data at risk. A data breach by Virgin Media left more than 900,000 customer details exposed and freely available online for 10 months, again showing why effectively protecting personal privacy is so important.

These are just a few examples of potential data and app breaches, which have resulted in a quarter (24%) of those we spoke to finding that their personal data or information about their family has become publicly available without their consent.

Understandably, these incidents have led 82% of people to try and remove private information which has become publicly available, from websites or social media platforms. However, how to go about this isn't always clear, as over a third (37%) of those wanting to take this course of action admit to not knowing where to start.

Have we got something to hide?

Although many of us are happy to conduct everything from shopping to sexual encounters online, our research shows we would rather keep these habits and preferences to ourselves. Despite being a global and essential entity, many see the internet as a place to hide.

In his book, '*Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are',* Seth Stephens-Davidowitz argues that people are more honest with sites like Google than they are in 'real life' when speaking with others. For example, he says that fewer than 20% of people admit they watch pornography, but there are more Google searches for 'porn' than 'weather'. Indeed, over a quarter (28%) of respondents to our survey said it was extremely important to keep their web searches for pornographic material private.

For the people we spoke to, the thought of others having access to their private data online is a real concern. Family members, colleagues and the government make up the top three groups of people we do not want to know certain things about us.

Colleagues finding out our personal information was highlighted more often by the majority of respondents, compared to other groups who could gain access – such as cybercriminals or their employer. Almost nine-in-10 (89%) do not want their colleagues to know their sexual orientation, the groups or organizations they are a member of (87%) or the people they interact with (86%).

To ensure this information is kept private, some respondents admit to putting special techniques in place to protect their browsing habits from potential sources that could cause leaks or unauthorized account access. These include cybercriminals, websites they have visited, other people using the same device, network managers and their ISP.

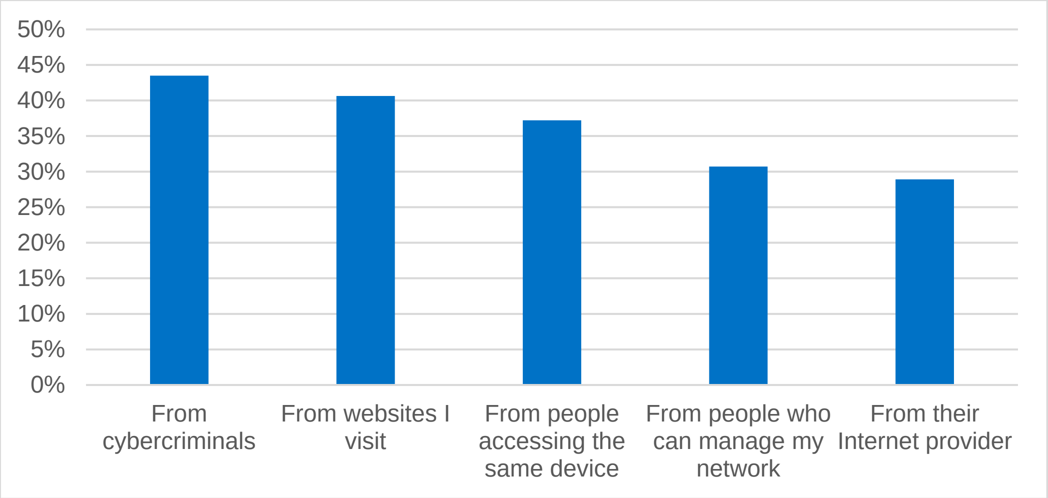

Chart 1: Who are you keeping your browsing secrets safe from?

Staying on top of all our passwords

Remembering passwords for our devices, apps and accounts is not a new challenge, but we could argue that it is getting harder. With estimates suggesting that people have 27 online accounts on average - there can be a tendency to re-use the same password to make them more memorable. The problem with this is that it also makes it easy for someone to potentially reveal our details – and this could lead to account information being discovered and put into the public domain. And with 83% of respondents making up their own passwords, without using password generation tools to create them a more robust and secure one, we could be more exposed than we think.

Some respondents (22%) allow browsers on their computers, smartphones or tablets to save and store passwords so they do not have to remember them. 15% of people still rely on writing down their passwords on a piece of paper or sticker near to their device. Surprisingly, those aged between 25 and 34 years old are more likely to take this approach.

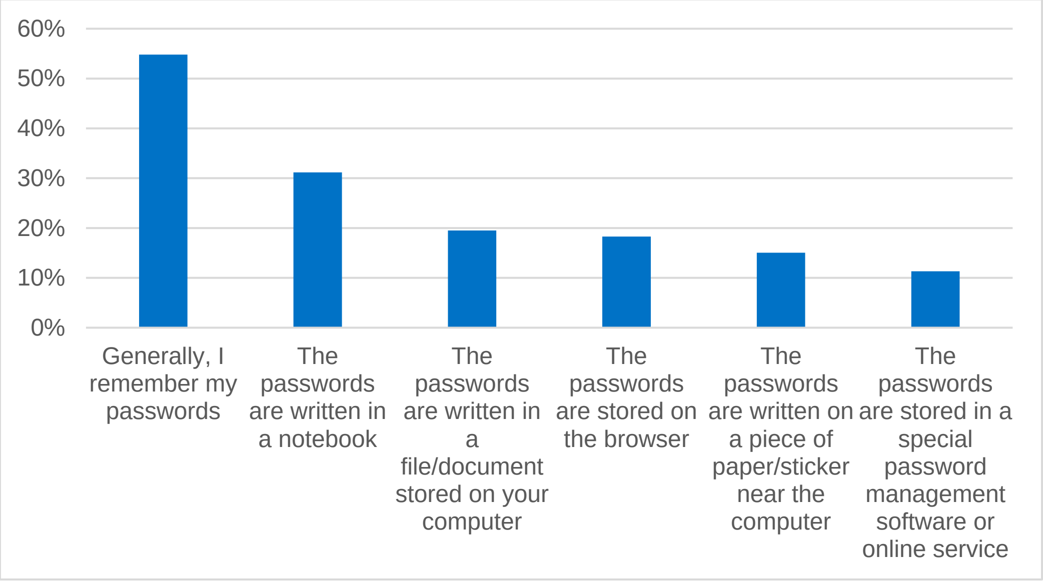

Chart 2: Which of the following methods do you use to store or remember your passwords?

With passwords so valuable to securing our devices, apps and accounts, keeping them secure is very important. This is why we need to put extra controls in place to make sure credentials remain safeguarded. It's not just financial records or personal details that could be compromised, but the information we share with family and friends, as Facebook users found out in 2019, when 540 million personal records were exposed – including IDs and passwords – after being left on unprotected servers.

But for many users, despite these high-profile cases, they remain unaware if they are affected by password breaches. Almost half (46%) have never checked if their passwords have been stolen or leaked, with 54% unsure how to go about it. With 80% of respondents admitting to regularly using their home computers for work-related purposes, this could have even more far-reaching consequences than just exposing personal information. For instance, concerns have already been raised about the rise of remote working and video conferencing in 2020 during the coronavirus pandemic.

The convenience of using your own device for work related purposes could see two worlds collide unless strict controls are in place. If there is a password breach, it won't just be your personal privacy that could be compromised but confidential work files or emails. To overcome this, IT security teams need to offer learnings about why staff should only use business devices to do work-related tasks, while businesses are urged to communicate with their employees about how best to keep corporate data safe while working from home.

Protecting permissions

Some of our survey respondents remain cautious when it comes to app permissions, with a fifth (21%) concerned about the personal data collected by the apps they use on their mobile devices. However, over half (58%) of respondents admit that they are fine with the permissions set on their applications by default.

This concern is very well warranted, as there could be a silent and unwelcome guest in many of our social networking apps unless permission settings are locked down. The use of stalkerware - commercial software used to secretly monitor online interactions of users, partners or colleagues – is on the rise, with new types emerging every day.

Kaspersky researchers recently uncovered a new sample whose functionality surpasses all previously discovered stalkerware. MonitorMinor enables stalkers to covertly access any data and track all activity on the devices on which its installed, including data from popular messaging services and social networks including Google Hangouts, Instagram, Skype and Snapchat.

But, with many of us trusting 'factory settings' and that our applications will keep things private by default, this is not always the case. Research by the International Computer Science Institute (ICSI) in 2019 found that over 1,300 Android apps can scrape certain personal data - even if a user has explicitly denied access to it.

This makes it even more important to be aware if passwords or apps have been infiltrated to keep your personal data and movements private as you browse and interact online.

Putting a lid on privacy

Putting passwords and permissions aside, users are trying to take privacy matters into their own hands by silencing their virtual assistants and covering webcams from being a potential source of privacy breach.

With more than half (54%) of the US population having used voice-command technology - including virtual assistants on smartphones, smart speakers and other devices - there is a trade-off between a convenient service and protecting our personal information. The last few years have seen many instances of private conversations being recorded and shared by Amazon's Alexa, but despite enhanced security measures by manufacturers, flaws still exist today.

With these types of devices also needing to listen for their 'wake word', a very small percentage of our conversations (less than 1% according to Google and Apple) are recorded for device improvement purposes. None the less, this is still an area of concern for users. Indeed 53% of respondents put measures in place to protect their voice assistant speakers from hearing things that they don't want them to.

When it comes to stopping prying eyes online, the most popular methods to protect webcams from being hacked include, putting a piece of tape or a sticker over the lens (47%), covering it with a special sticker (35%) or disabling the webcam in the device management settings (35%).

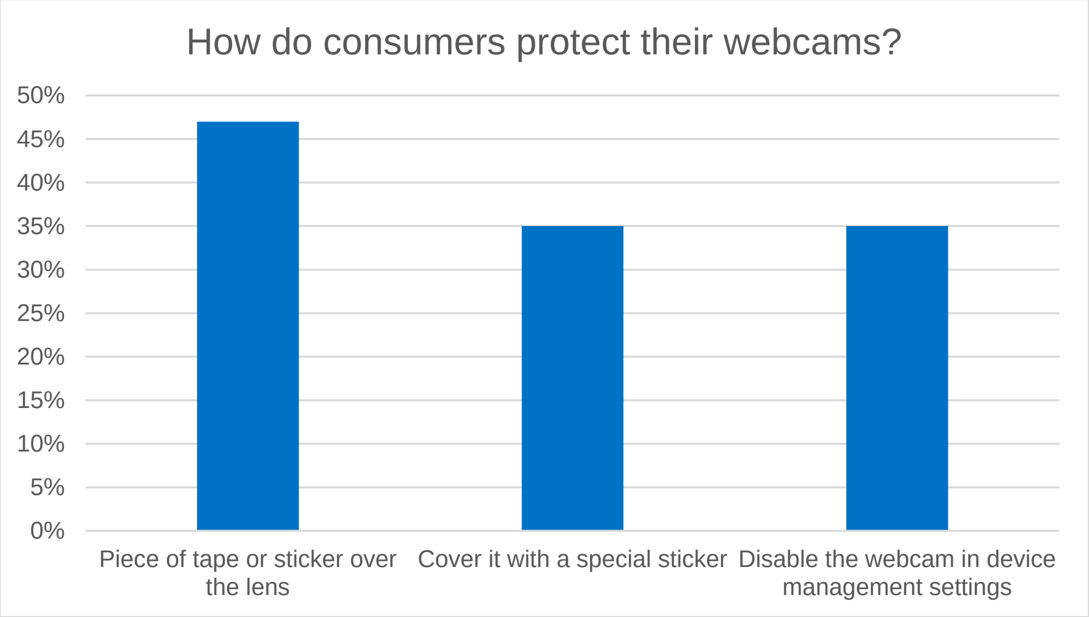

Chart 3: Which of the following methods do you use to store or remember your passwords?

The next step for privacy provision

As we commit more of our lives to online based applications and accounts, the measures we take to protect our privacy online need to evolve at the same pace, to ensure that the internet continues to be a valuable and safe resource for all.

Despite measures put in place by regulators and companies alike, it is still important that we do all we can to protect the privacy of our own online conversations and interactions. Although many individuals are taking steps to protect themselves online, it is clear that there are still gaps in public knowledge, which is understandable given the pace of change in technology innovation and cybercriminal tactics. It's not just about protecting our financial and personally identifiable information on banking and shopping apps. Data and insights gleaned from our browsing history and all the apps we use on a daily basis are just as important to keep secure.

Dating apps

For example, popular dating apps such as Tinder and Badoo, can be used to spread mobile malware or retrieve personal data that can later be used to bombard users with unwanted ads or even encourage them to spend their money on expensive paid subscriptions. In fact, analysis of malware using the names of over 20 popular dating applications and the keyword 'dating' revealed 1,963 unique files were spread in 2019 under the guise of legitimate applications. These range from Trojans that download other malware to ones that send expensive SMS communications. Cybercriminals also attempt to acquire personal data by launching phishing attacks by creating fake copies of popular dating applications and websites.

Safeguarding

However, despite a constantly changing cyberthreat landscape, the same principles still apply when it comes to safeguarding your personal privacy and information online. Here are some additional ways to protect your private information or check if your passwords or data have become compromised without your knowledge:

- To make sure people close to home, including family, friends or colleagues, can't access your devices or accounts without your consent, never share passwords even if it seems like a good idea or convenient to do so. Writing them on a sticky note next to your screen might be helpful to you but it might also be helpful for others to access things you don't want them to.

- Ensure you always check permission settings on the apps you use, to minimize the likelihood of your data being shared or stored by third parties – and beyond – without your knowledge. You might end up giving consent by default, so it is always worth double checking before you start using an app or service.

- There is no substitute for strong and robust passwords. Use a reliable security solution like Kaspersky Password Manager to generate and secure unique passwords for every account, and resist the temptation to re-use the same one over and over again.

- To find out if any of the passwords you use to access your online accounts have been compromised, use a tool such as Kaspersky Security Cloud. Its account Check feature allows users to check their accounts for potential data leaks. If a leak is detected, Kaspersky Security Cloud provides information about the categories of data that may be publicly accessible so that the individual affected can take appropriate action.

- European users can regain control over their personal information, which has become publicly available on the Internet, using a new Kaspersky-backed service called Undatify. The solution simplifies the complex process of communicating with organizations that store user data and requesting a copy of your information, or completely deleting those records in line with policies set out by GDPR. More territories and international regulations are set to follow.

For more information and advice on how to look after your digital privacy, visit our website.