To protect the data we store on our devices and upload online, we first need to understand where the key risks may lie.

Protecting your personal data online at every point

kaspersky BRING ON THE FUTURE

Contents

Methodology

All statistics used in this report were obtained using the Kaspersky Security Network

All statistics used in this report were obtained using the Kaspersky Security Network (KSN), a complex distributed infrastructure developed by Kaspersky and dedicated to intelligently processing cybersecurity-related data streams from millions of voluntary participants around the world.

Key findings

- In 2019, 85% of Kaspersky Security Cloud users took advantage of its “Account Check” function on mobile devices and found out that their email addresses were in the public domain. This was probably due to data leaks and breaches from web services that occurred over the last few years.
- Kaspersky products detected 222,434 installations of stalkerware (a legal type of spyware used to spy on children, colleagues or relatives) on users of Windows devices, with the top three most affected countries being Russia, India and Germany.
- Anonymized insight from the Do Not Track feature found that popular data trackers DoubleClick, Google and Facebook were detected on 13%, 10% and 4% of pages visited by Kaspersky users throughout the year, respectively. To put this into context, the 100% reference value was for all Do Not Track triggers across all trackers in each country or region analyzed.
- Anti-phishing technologies prevented at least one phishing attack on the computers of 15% of Kaspersky users.
- 2019 saw a 72% rise in the number of users hit by malware designed to harvest consumers’ digital data, reaching almost 2,000,000 users.

Introduction

The amount of digital data we provide has become subject to many potential risks.

Growing technology innovation has helped to solve many daily challenges and problems for consumers. For example, 10 years ago, we did not have the level of mobility in cities that is now available — thanks to Uber, Lyft and other companies. We also couldn't find love in just five minutes, through the likes of Tinder and other dating apps and platforms. In return for this convenience, these services require a certain amount of personal information in order to continue to be of value in the future. As a result, we find ourselves providing more and more personal information to different services and applications, to satisfy our needs.

However, at the same time, the amount of digital data we provide has become subject to many potential risks. From the moment we wake up in the morning and update our social media status and check emails, through to late night shopping and paying bills just before bed - the personal data we share openly and confidentially online can be easily accessed by malicious means for criminal gain.

Data-stealing malware can access our personal information through a simple click on a malicious link in an email or by abusing our permission settings on an unprotected app. A scorned lover could upload spyware on a device to record keystrokes and use information against us. And a data breach by a service provider, including banks, airlines or retailers, could see our confidential account and financial details made available on the black market for a certain cost, but with big implications.

However, the measures to safeguard data are becoming more effective and complex, despite the nature and number of threats rising every day. The ability to safeguard every piece of personal data residing on our devices and the internet might sound impossible, but it is something that every individual can take control of.

Everything we upload or reveal about us can be potentially of value to a whole host of interested parties - from marketers and corporations wanting to personalize their promotions and offers, through to cybercriminals wanting to profit from making money out of our personal data. We usually don't mind that the locations we check-in to provide a picture of where we go and what we do; and our online search history reveals our interests and what engages us; at the same time the confidential data and credit card details we enter on apps and websites could be highly lucrative if they fall into the wrong hands.

To protect the data we store on our devices and upload online, we first need to understand where the key risks may lie. This report reviews some of the main stories and tactics we have seen affecting data privacy over the past 12 months and provides advice on how individuals can keep control over their personal data at every turn.

Your data journey: out of sight, but not out of mind

85% of user emails on mobile devices were compromised due to data breaches occurring in recent years.

As well as the apps on our devices proving a vulnerable point for data privacy breaches, there are understandable concerns around what happens to our personal data when it is given to an organization and out of our hands. It seems that barely a day goes by without a corporation being hit by a data breach and personal information put at risk.

The recent ransomware attack on global currency giant Travelex shows that not all corporations respond appropriately to protect users' data. It is also a good example of where individuals can feel a loss of control without permission over data and that companies are not always doing right by it. Indeed, data from Kaspersky Security Cloud 'Account Check' function (which checks your accounts for potential data leaks) showed that 85% of user emails on mobile devices were compromised due to data breaches occurring in recent years. And it's not just our own insight that is fueling concern around data compromise.

Data breaches might be the more high-profile story affecting the security of our information, but the uncertainty of the journey taken by our data online once we entrust it to third parties is also a point of concern for consumers. Despite tighter controls regarding data protection - with the introduction of GDPR for example - and increased transparency regarding data sharing and the ability to opt out of details being shared more widely beyond its intended use, consumers across the globe feel this has not gone far enough. They are calling for tighter controls around the security and sharing of their data – with 75% of respondents to an Internet Society survey expressing concern that their personal data is being shared without their permission.

In the midst of a lack of decisive action by corporations and legislations to guarantee watertight security and that our data is not at risk, individuals themselves can keep a track of what is happening to their data stored on the websites they visit. For example, it is possible to check your user data for potential leaks, giving you peace of mind that it is secure or arming you with informed insight from which to take remedial action if a leak has occurred and before information falls into the wrong hands.

Mind the app: the perils of permissions

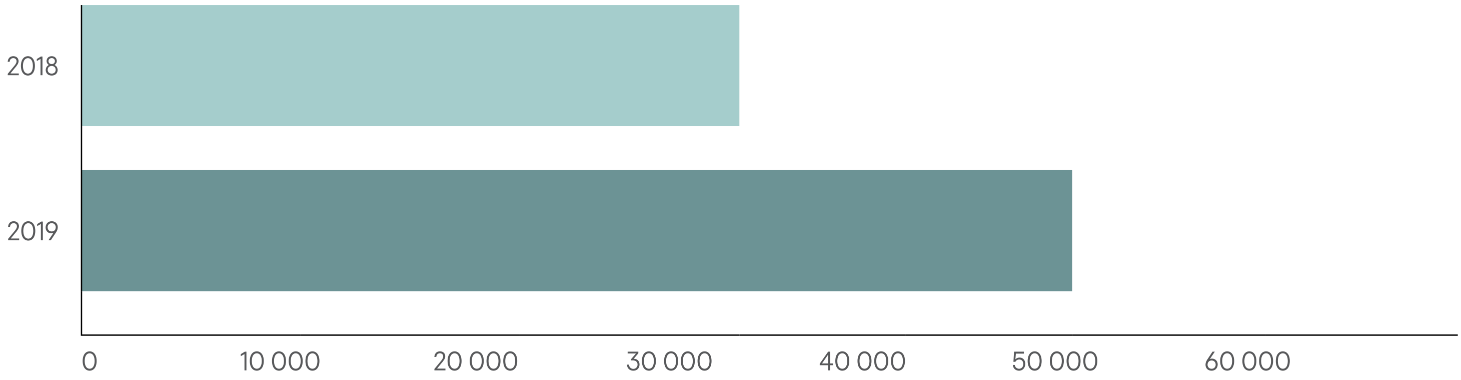
With smartphone users having on average between 60 and 90 apps on their device at any one time, it is clear that our reliance on apps for socializing, shopping and sharing information has increased. But these apps could also be a potential treasure trove for third-parties looking to gain access to our confidential and lucrative personal data.

The main reason for this often lies in the levels of restriction and permission settings on these apps. With so many apps on our devices – ranging from social media and communications platforms which we use every day, through to shopping, gaming and banking services which store financial credentials – it can be easy to lose track of what permissions and restrictions you put on each one.

Furthermore, the Android platform does not warn users about the risks associated with this or other permissions. The user often doesn't know that their location can be used for tracking and, that if they give an application access to the camera, it means it will be able to take pictures from the device at any time, without the user noticing.

For this reason, the use of threats, which rely on location tracking to steal data rose significantly in 2019. Kaspersky experts found that one such threat class – detected as Monitor – grew significantly, with the number of targeted users increasing from 33,388 in 2018, to 50,410 in 2019. Programs of this type can monitor smartphone activity (incoming and outgoing SMS messages, messenger conversations, track location, record call activity) and are not malicious programs. If such software were installed without user consent it could lead to personal information being misused.

Monitor Activity in 2019



Another notable player in the field of privacy violation is Ginp – a malware family, which deceives users by impersonating banks. When a victim opens their mobile banking app, the malware overlays a screen, which mimics the real app, asking for login credentials and stealing credit card data. This malicious deception is practically impossible to spot, unless an antivirus solution had been installed.

Despite the abovementioned examples showing just how easy it can be for malware to find its way onto our devices without us realizing – as simply as it can appear, the potential damage can also be easily stopped in its tracks. Checking the security settings of each app and setting your own restrictions – rather than just accepting all privacy permissions as standard – will put you back in control. The addition of permission checker controls will then alert you to the presence of such malware to help minimize any potential damage.

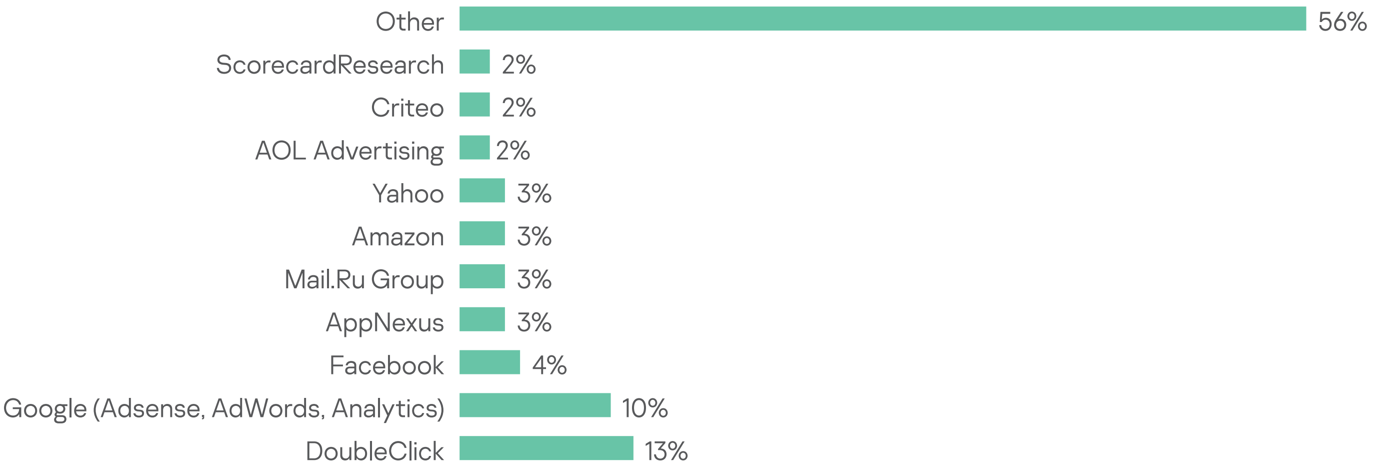
Data dead-end: stopping traces in their tracks

Many websites we visit every day collect information about what we view, how long we spend on each page, where we have clicked through from and where we go next. This might seem the norm nowadays and something we just expect will happen, but in tracking our movements, websites can learn an awful lot about us through analyzing and acting on our behavior.

And while this has its merits in ensuring the adverts and emails we receive are targeted and relevant, our information can end up taking a different turn, finding its way to data harvesters without our knowledge. Our social media channels can also be subject to manipulation by tracking our interests and serving us information designed to influence our opinions.

DoubleClick, Google (including services such as Adsense, AdWords, and Analytics) and Facebook are some of the most popular data trackers. Anonymized insight from our Do Not Track feature – an element of the Kaspersky Security Cloud solution which shields users against online tracking and data collection – shows that these services were detected on 13%, 10% and 4% of pages visited by Kaspersky users throughout the year.

Do Not Track triggers across the most popular trackers worldwide in 2019.



For Google owns the largest advertising network in the world at the moment – DoubleClick – and accumulates the most data about users from all over the world. Among its key services which process users' data, Google Analytics collects and provides visitor statistics to the website owner; Google AdWords is used for advertising purposes; and Google AdSense is designed for those who sell adverts on their own resources.

In addition to Google data collection services, the Facebook tracker is located mainly on the pages of social networks. Facebook also has another tool that we consider a separate entity – the Facebook custom audience. This is implemented in pixel format and embedded in pages, to track standard and user events, as well as conversions.

But this tracking doesn't have to be the case across every website we visit. There are tools available to stop online tracks from being followed and personal data made accessible to anyone for any means. In this way, users can only give up information which they want to share, when they want to share it, and not surrender everything just by browsing.

Keeping keystrokes safe from stalkerware

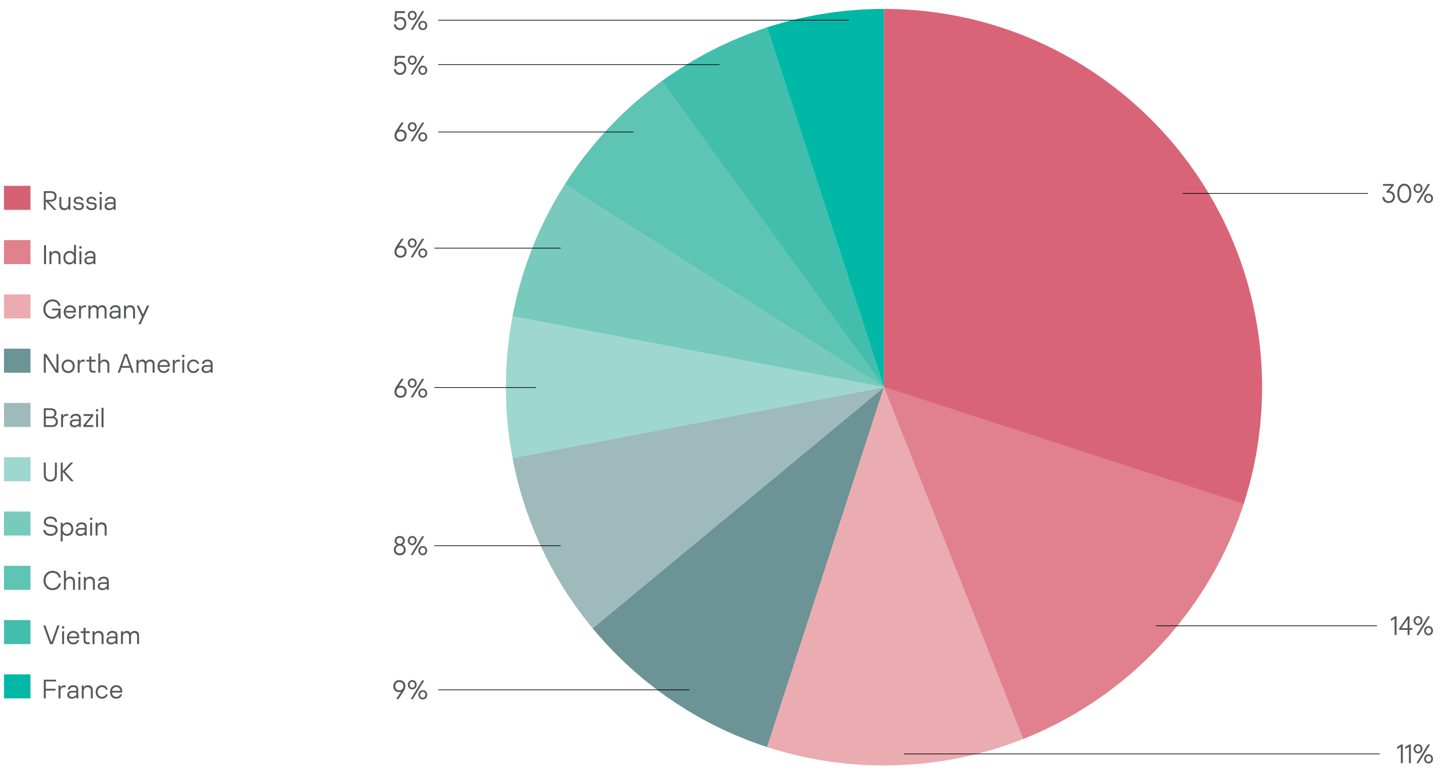
Much like the malware examples highlighted earlier, the presence of consumer surveillance technology (or 'stalkerware') on a device can easily go unnoticed until it's too late. Often promoted as a parental control tool or family tracker, these apps can have a much broader scope of application.

Stalkerware is installed without the device owner's consent, to secretly stream the victim's personal information – including images, videos, correspondence, and geolocation data – to a command server. This carries the danger of personal information being misused by third parties, such as the app owners. Almost all stalkerware is designed to monitor victims' actions, including keyboard activity, making it extremely effective in stealing information which the user is typing online, via keylogging tactics.

The low cost – sometimes as little as $7 a month – and ease with which it can stay hidden on a victim's device makes it an affordable way of monitoring someone's movements. Providing access to information such as a user's location, browser history, text messages, social media chats, and more, spyware can be extremely damaging for the often-unwitting victim.

To understand the potential extent of the problem, in 2019 alone, Kaspersky products detected 222,434 installations of stalkerware on users of Windows devices, with the top three most affected countries being Russia (40,912), India (18,549) and Germany (15,217). It is a global issue with growing consequences.

Top – 10 countries, which encountered stalkerware in 2019



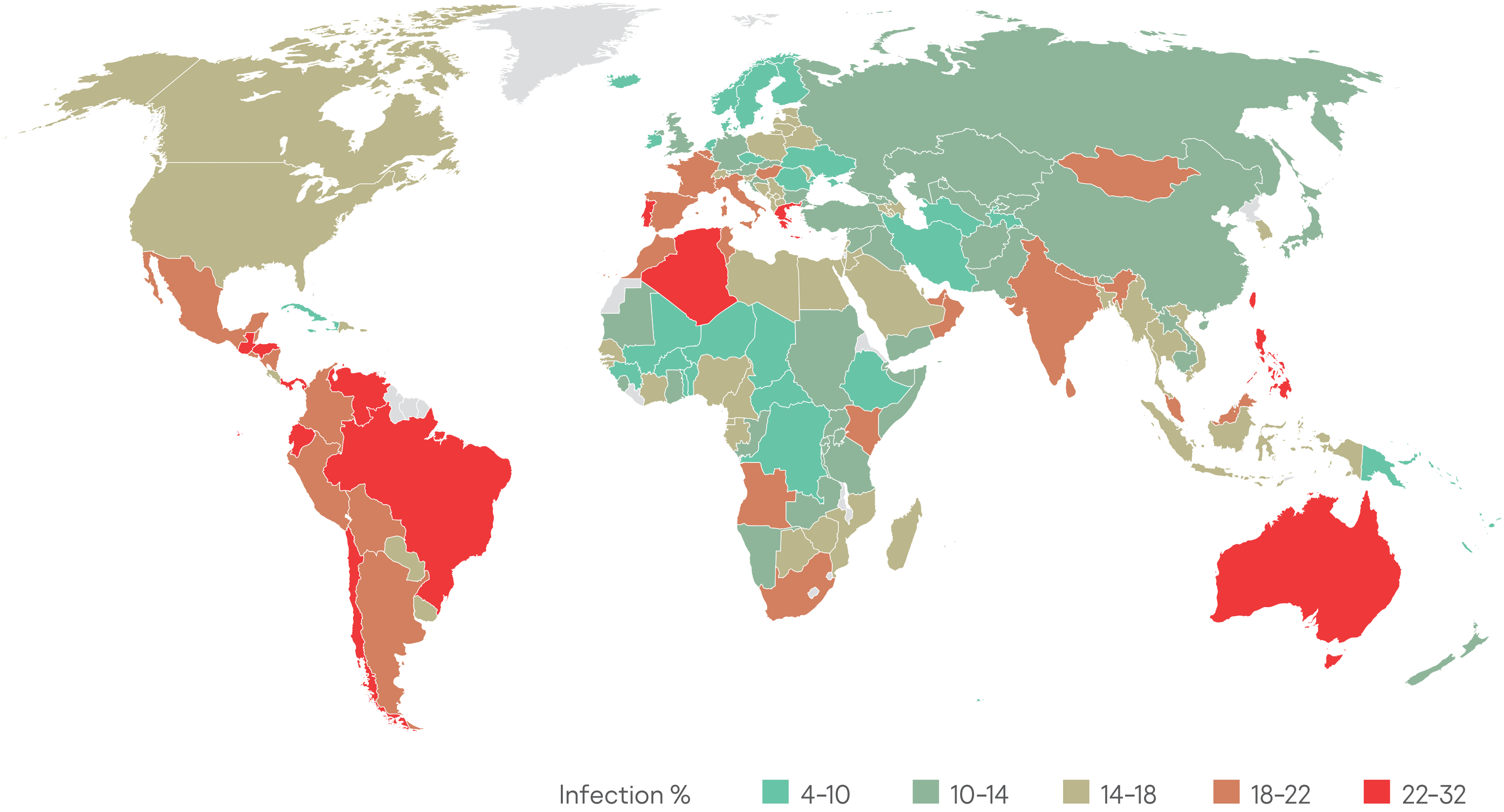
However, despite the potential impact that stalkerware can have on data privacy, it can be taken down in one fell swoop. To unmask the shroud surrounding stalkerware, users can start by easily defending against their keystrokes being recorded and images captured from their PC screen by using an on-screen keyboard.

Gone phishing: increased prevalence and pressure

Despite being one of the best-known forms of cyberattack, the social engineering tactic of phishing is still one of the most deployed worldwide. Preying on consumer interest in significant global events – from sporting fixtures including the football World Cup or the Olympics, to environmental and social disasters including the bush fires in Australia, and blockbuster film and TV launches including Game of Thrones and The Avengers – phishing attacks aim to dupe us into clicking on a malicious link or handing over personal details in return for a 'money can't buy' ticket or donation to a worthy cause.

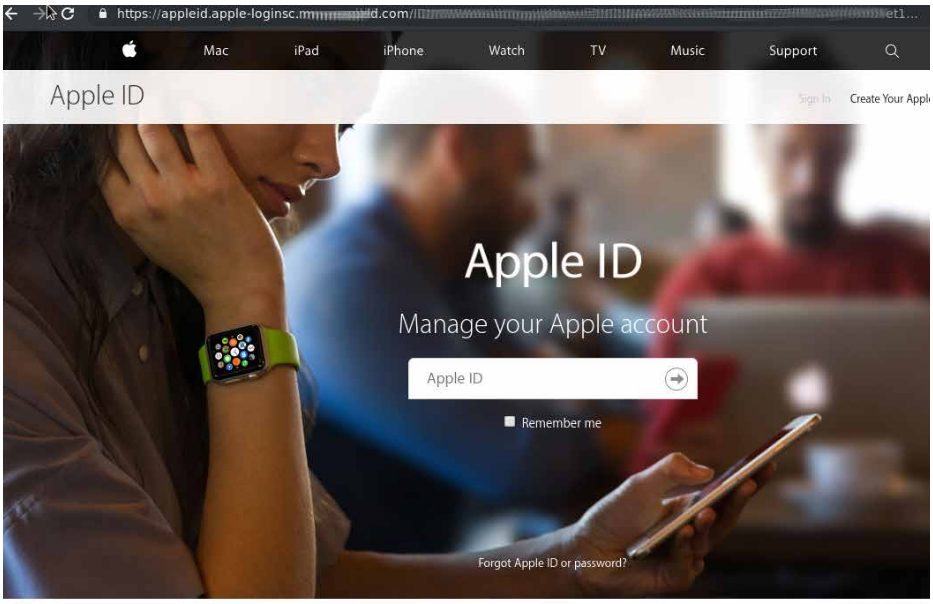
With cybercriminals coming up with ever more enticing and legitimate-looking ways to try and convince us into handing over confide ntial data, phishing can be a cause for concern when it comes to ensuring we don't divulge something to someone we shouldn't. In fact, our figures suggest that the level of phishing attacks grew significantly in the past 12 months, with our Anti-Phishing system preventing, on average, 38 million attempts to direct users to scam or fraudulent websites – every month. This figure represents that 15% users were targets of phishing attacks.

Geography of phishing attacks



The level of phishing attacks grew significantly in the past 12 months.

Examples of phishing page: Apple website



https://appleid.apple-loginsc.[redacted]d.com/[redacted]

Apple ID

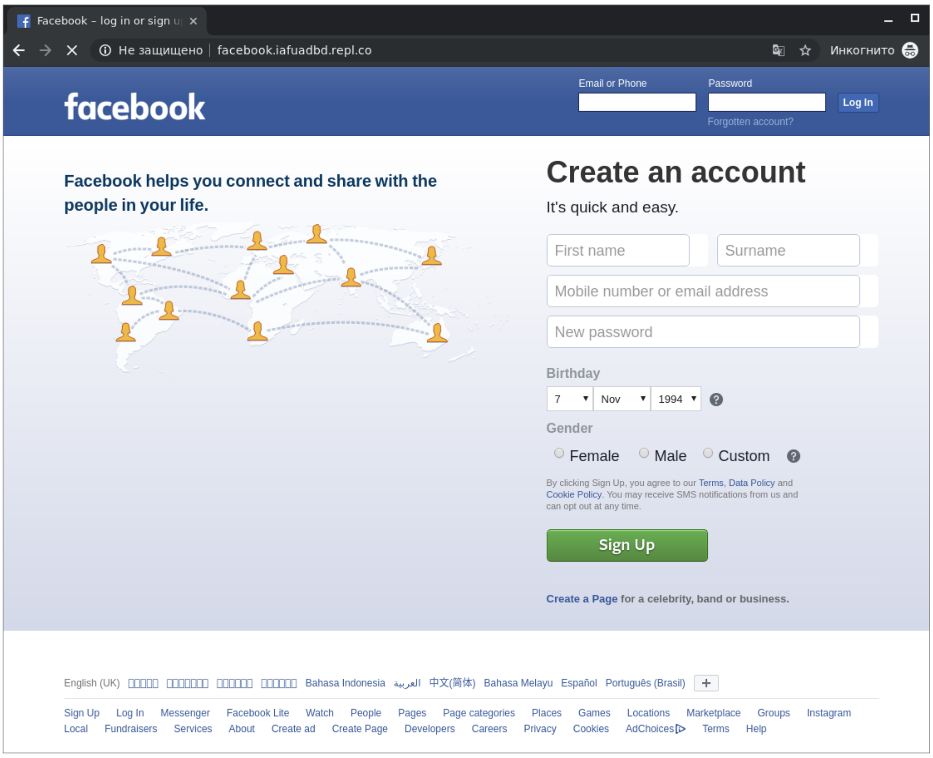
Manage your Apple account

Apple ID

□ Remember me

Forgot Apple ID or password?

Examples of phishing page: Facebook website



Facebook – log in or sign u ×

Не защищено | facebook.iafuadbd.repl.co

Email or Phone

Password

Forgotten account?

Facebook helps you connect and share with the people in your life.

Create an account

It's quick and easy.

First name | Surname

Mobile number or email address

New password

Birthday

7 ▾ Nov ▾ 1994 ▾ ?

Gender

○ Female ○ Male ○ Custom ?

By clicking Sign Up, you agree to our Terms, Data Policy and Cookie Policy. You may receive SMS notifications from us and can opt out at any time.

Create a Page for a celebrity, band or business.

English (UK) □□□□□ □□□□□□□ □□□□□□ □□□□□□ Bahasa Indonesia العربية 中文(简体) Bahasa Melayu Español Português (Brasil) +

Sign Up Log In Messenger Facebook Lite Watch People Pages Page categories Places Games Locations Marketplace Groups Instagram Local Fundraisers Services About Create ad Create Page Developers Careers Privacy Cookies AdChoices Terms Help

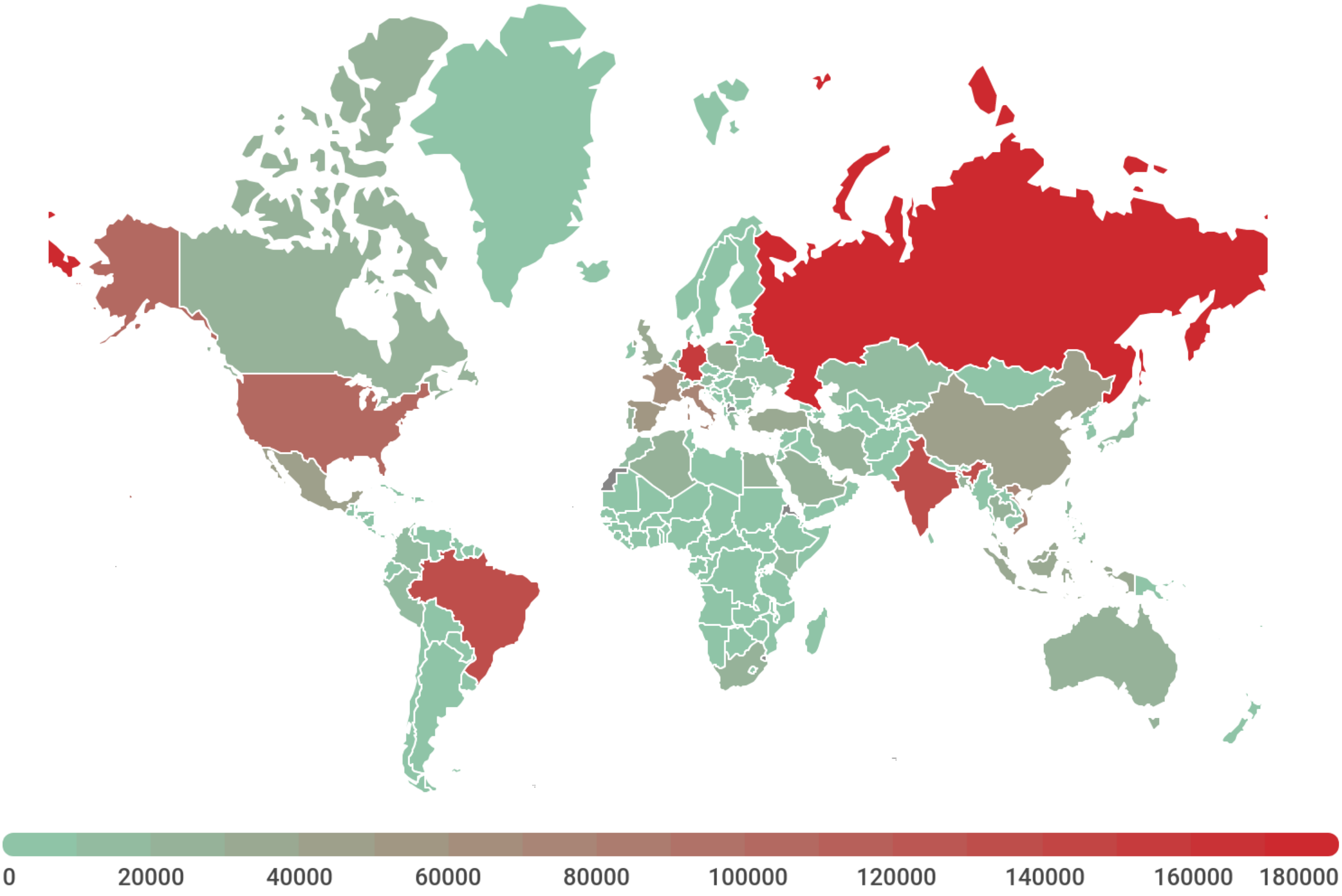
But despite this high number, users are wise to the tactic and putting measures in place to stop attacks in their tracks. This includes being vigilant and thinking twice before clicking on any suspicious looking links, as well as deploying anti-phishing tools to defend against attacks attempting to steal your money, from getting through, or to stop users unwittingly inputting information into a phishing site.

Password protection

Nowadays most of us have too many passwords that we need to change often, for many sites or applications. But we often forget that we need a secure way to keep them organized, and also try to find an efficient way to sync them across multiple devices and keep them secure.

Thus, the use and reliance on passwords to access our accounts and apps make them a prime target for those looking to gain unlawful entry. In fact, the value of passwords as the key to unlocking our confidential data led to a 72% rise in 2019, of users hit by malware designed to harvest consumers' digital data – also known as password stealers. In the second half of 2019, we also saw an increase in the prevalence of AgentTesla (Trojan-PasswordStealingWare): one-in-five users encountered this type of stealer.In other words, in 2019 we noticed an increase in password stealer activity.

Despite the rise in attempts to steal our passwords, users can follow simple steps to ensure they can continue to use their apps and online services without fear of being watched or their passwords infiltrated. As well as minimizing the risks through not sharing passwords with family or friends, installing regular updates and patches on your devices and using a password manager solution to securely store passwords and personal information will ensure complete protection from the latest malware and threats.



Conclusion and recommendations

Our solutions are designed to give individuals additional peace of mind and the confidence to continue to socialize, shop and share online in a secure environment.

Data privacy should not be something we have to fight for, it should be a given right. Everyone should feel safe when using their devices and the internet, without worrying that their data could be at risk at every turn. There is no substitute for vigilance, and the old adage of 'it seems too good to be true' when an enticing email lands in your inbox out of the blue is certainly a good rule to live by.

Here are some simple steps which users can take to ensure their data remains safe and information protected.

- Start managing your digital footprint: keep a list of your accounts and regularly check if your data has become publicly accessible.
- 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.
- Do not share passwords or personal information with friends or family, as they could unwittingly make them vulnerable to malware. Do not post them on forums or social media channels.
- Do not click on a link in an unsolicited email or if you are unsure if it is legitimate. Check the provenance and authenticity of an email by visiting the website directly first, before clicking on a potentially malicious link.
- Never store unfamiliar files or applications on your device, as they could harm your privacy
- Check the list of applications on your device to find out if suspicious programs were installed without your consent.

Through the Kaspersky Security Cloud solution, we can help users protect their privacy in several ways:

- The Permission Checker feature for Android allows users to see what applications have access to a device's camera, microphone, location and other private information and restrict some of them if necessary.
- Account Check feature (available for Kaspersky Security Cloud) 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.
- To prevent the loading of tracking elements that monitor your actions on websites, enable the Do Not Track feature.
- Online communication with friends and relatives can be protected by using Kaspersky Security Cloud's On-Screen Keyboard. This quick launch feature will defend against malware that captures key strokes when you type in your login details and passwords in various websites. This will allow you to add another level of protection of your online accounts.

- The Anti-Phishing feature defends users against phishing sites or emails that try to steal your money or identity, ensuring you only open legitimate emails and visit valid websites.

- Kaspersky Password Manager (included in Kaspersky Security Cloud) securely stores all account and app passwords in one place so you can set 'strong keys' without having to remember multiple different combinations. Not only does this ensure the security of passwords, but provides fast and easy access to the websites, apps and accounts you use most often.

For more information about how Kaspersky Security Cloud can help protect your online privacy, visit the product page.

2020 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.