Definitive checklist

How to protect your data online

kaspersky BRING ON THE FUTURE

Learn more:
kaspersky.com

Definitive checklist: how to protect your data online

Photos, uploaded documents, smartphone app details – data management is a continuous, daily event whether we realize it or not. But do we know where this data ends up, and could it be in the wrong hands? We need to learn how to share personal data responsibly - whether it is personal data that you have influence over, data controlled by other parties, or even information about others that you have access to. This checklist will show you how to take control of your data.

Information about you that you control

1.

Be conscious of which personal data you share and with whom, as well as how much you trust them

When sharing personal identification information (passports, IDs, medical insurance), make sure you understand which service or person you are sending it to and how much you trust this particular service or person. In the case of businesses, check in case there has been a previous data breach. Think every time before you give someone your documents. For example, sharing personal data with a real estate agent for a contract may be risky, while confirming ID details to a delivery service that requests it on behalf of customs is generally trustworthy.

This is especially important when it comes to sharing medical data (such as menstrual cycles, blood sugar, daily calories).

2.

Be mindful of who you share your data with and when

It is a good practice to keep track of third parties that you have shared your personal data with. This way, when you see the news about a leaked database around a service you have used, you can check if your data may have been compromised. A handy way to go about this is using a password manager as a catalogue of all the services with which you've registered. By controlling who you share your personal data with, you will think twice before sharing it.

Learn more: How to upgrade Discord security
Finding out what data apps really collect

3.

Think before you post. Be accountable for what you share. Every time. Even if your account is closed

Aside from sensitive data, a 'social portrait' can be constructed based on your posts and used against you. Make sure that you are ready to be accountable for whatever you have said online. Consider making your account private, but be aware that this does not make it fully hidden, and there are still a number of ways to expose what you have posted (for instance, your followers getting hacked).

Learn more: Protect your privacy online
Take control of your personal data

4.

Use abstract geotags, if any at all. Do not tag photos with specific locations that you visit regularly

Geolocation is one of the most sensitive types of data which can compromise you – by following the geotags, criminals can identify where you live, where your children spend time, which routes you take and when you are not at home. At the same time sharing geotags of places you travel to or attend rarely is generally safe.

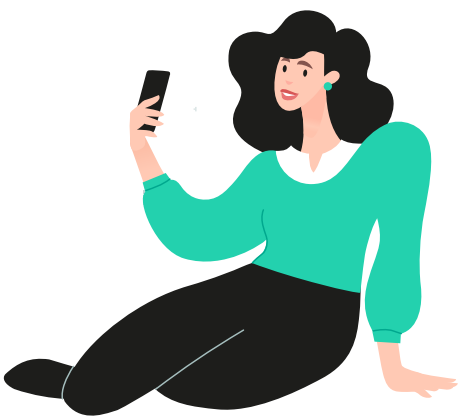
Set up your social media privacy settings with the help of Privacy Checker

5.

Make sure that you do not show your personal data on the photos you share

This should be an easy one, yet, looking at the hashtags #tickets or #flights we can see that so many people still share their personal data in photos – for instance, their flight booking numbers on a boarding pass. Any time this type of data is made public it has the potential to be abused—even if it's just by some ill-intentioned joker. In fact, a prankster once cancelled a booking of an unwitting user for fun by simply calling the airline using the booking number posted online and the name of the user. If you plan to share something about your travels, make sure that the photos do not contain personal data, just share the destination.

Learn more: **How to keep spies off your phone — in real life, not the movies**



6.

Understand which messengers are safe and which ones have end-to-end encryption

Personal conversations, which generally take place in messenger apps, are the most sensitive data of all. We use messengers to discuss very private and important topics, things that can identify our vulnerabilities. Therefore, it is crucial to understand how secure the messenger you are using is, and what kind of data – text or photos – can be shared with low risk. Know whether your favorite messenger app stores messages only on your device or in a cloud or server, from where they can be leaked. Consider other privacy options, for instance, whether the app informs you if the participant of a conversation took a screenshot of your communication, or try to send self-destructive messages.

Learn more: **Telegram security and privacy tips**
What end-to-end encryption is, and why you need it

7.

Invest wisely in your smart devices. Cheap development often means higher data leak risks

Fitness trackers and smartwatches that we wear 24/7 are all tied to specific apps that gather your biometric data. While there are plenty of cheap devices, be aware – the less the developer has invested in the device and app, the lower the security can be. The basic rule is to consider the price, popularity of the device and how easy-to-use the application it is tied to, is. Look up information about the application that the tracker should be linked to, review any history of data leaks and read user reviews before purchasing. The same goes for smartphones, video cameras and baby monitors.

8.

Shop online in trusted stores. The fewer, the better.

The myriad of online stores offering more or less the same things may confuse us. But all stores have different privacy policies, some – none at all. The fewer online stores you use, the less information you share.

Information about you that you do not control

Browser activity

Every single step you take in your browser is traced by cookies and tracking URLs. And it's just cookies – there are myriad fingerprinting mechanisms used to uniquely identify a user online. This data enables organizations to create a detailed profile of you – and, no doubt, to cater advertising and enhance the user experience. But that comes at the cost of your data being vulnerable. It is therefore up to you to find the right balance between your privacy and improved user experience – with help from our tips.

1.

Opt for a browser that's built with privacy in mind or set up a plug-in that minimizes tracking

Tracking URLs meant for advertising are loaded alongside a webpage to trace your activity on top of the existing tracking executed by the web page. Install trusted privacy and security add-ons such as tracker blockers, ad blockers and security tools, and use plug-ins that cut off tracking links. For instance, Kaspersky products have a Do Not Track component that prevents the loading of tracking elements that monitor user actions on websites.

Learn more: How to tell if a website is taking your (browser) fingerprints

2.

Set up browser cookies to delete after each session

Set up browsing settings to limit cookies. This way you do not allow cookies to trace your web activity long-term and prevent them from creating a defined profile of you. Take into account the difference between first-party and third-party cookies: first-party cookies are meant to improve the user experience, making it more convenient to browse and create personalized recommendations for you.

They are generally safe. Meanwhile third-party cookies trace the same activity or the most interesting activities in order to create a profile of you and target ads to you - they might also trace your browsing history. Note that some browsers such as Safari, have now developed a more robust privacy policy in relation to cookies by default.

Learn more: Why you should try listening to your cookies

3.

Look for higher privacy settings in the browser's options interface

If you are ready to put some effort into protecting your data, both from a privacy and security standpoint, consider additional measures. For instance, Firefox Containers is a neat option for users to carefully segment portions of their online activity into separate boxes that keep data relevant to those segments separate from each other. Other options would be restricting which sites have access to your location data, microphone and webcam, and even which sites have JavaScript enabled.

More advanced users may consider disabling the WebRTC APIs if potentially leaking your IP address is an area of concern. Another option that usually is turned on automatically in most browsers that many users might want to turn off for added security is autosaving and autofilling of passwords. If the browser supports it, consider enabling the "HTTPS Only Mode" that automatically attempts to encrypt all HTTP traffic on sites (most of the web thankfully now uses HTTPS, but there are still outliers out there and it is better to be safe than sorry).

Many of these tasks can be done automatically with the help of browser extensions like **Privacy Badger**. It's the project maintained at EFF and is a free, install-and-forget browser add-on that works behind the scenes on users' browsers to opt them into higher privacy settings.

4.

Use incognito browsing

If you want to search for something, but do not want it to stay in your history, use incognito browsing windows. It limits the browser from tracing your browsing history and cuts off all the cookies, making your search private. This is especially useful if you are sharing your computer with others.

Learn more: **Incognito mode Q&A**

Tracking by applications

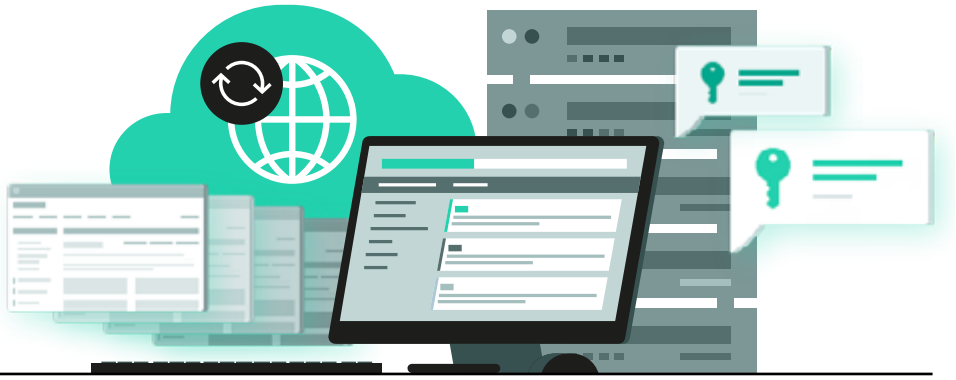
Mobile apps trace and gather your data the same way as web browsers. Even worse – we carry smartphones with us everywhere, so they know much more about us than we might suspect. There are two main ways to limit mobile devices gathering your information: minimize tracking and clutter the data with noise. Here is how:

5.

Use a basic VPN

A VPN fully encrypts the traffic from your device, keeping it safe and hidden from everyone, including your provider, even if you connect to public Wi-Fi networks. It can change some information about you and your device (for instance, your IP) and make it harder for organizations to trace you. It is important to consider that a VPN also gathers user data and therefore it is important to select a service that you can really trust. While a free version of a VPN will be sufficient to hide your traffic from a provider, it may also sell it to third parties. Select a service from a respected vendor with a data processing statement in place, for instance, Kaspersky VPN.

Learn more: How to protect your home Wi-Fi from nosy neighbors
How to choose a VPN



6.

Change the local region on your phone

Misinforming trackers about your location will help to confuse them and make it harder to create a correct profile of you. Set up a different regional locale on your OS and choose a third country for your VPN connection. For instance, select the German version of the iOS and a Finnish VPN connection. One of the issues you may face when using a locale change is trying to use a payment service in a country where this service is not supported. In such cases, just switch back to your local region, make a payment, and then switch again back the country of your choice.

7.

Set up specific access settings for each application on your phone

Use instruments that your OS developers have created to ensure applications only gain access to the information they need. Best practices includes allowing access to your location only while using an app, and limiting access to the microphone and photographs. Be wary of applications that request data they should not need to perform their functions.

Learn more: **With off-facebook activity, you have (some) control over your data**
Instagram's updated security and privacy settings

8.

Never install unverified applications

Unverified applications (apps that have not gone through an app store's verification process) often end up being adware – a type of software that floods your phone with advertising and gathers metadata about you. Even worse, the app you download may be malicious. For instance, it may contain spyware that gathers information about your location, your conversations in messengers or call log.

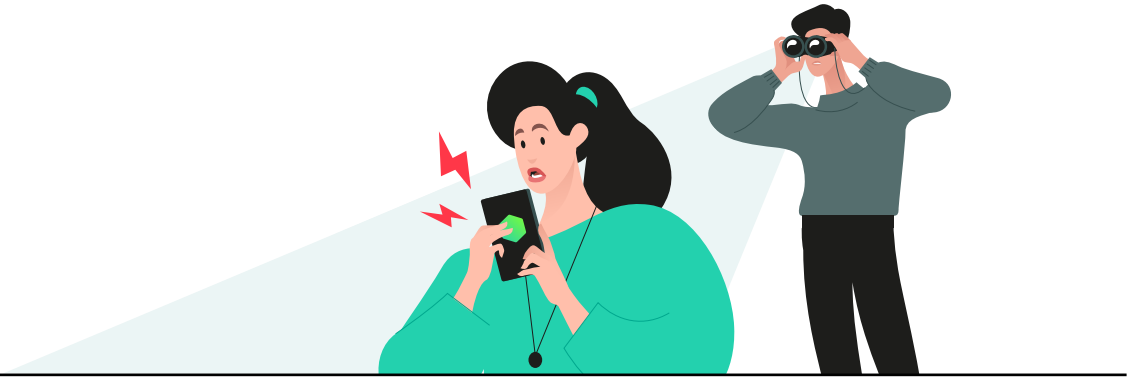
Information about other people that you have control of

Photos of other people, conversations, chats, phone numbers, and addresses – you often get access to other people's personal information. This also needs good care, and it is your responsibility to keep it safe. Here is how:

1.

Only share personal information after gaining consent from the people involved

Photographs of other people that you have taken may be considered innocent by you but could harm others. The same goes for screenshots of conversations, flight tickets you purchased together with someone else – pretty much anything that includes a third party and information that may identify them. Remember that you are responsible not just for your data, but for others' data that happened to become yours too.



2.

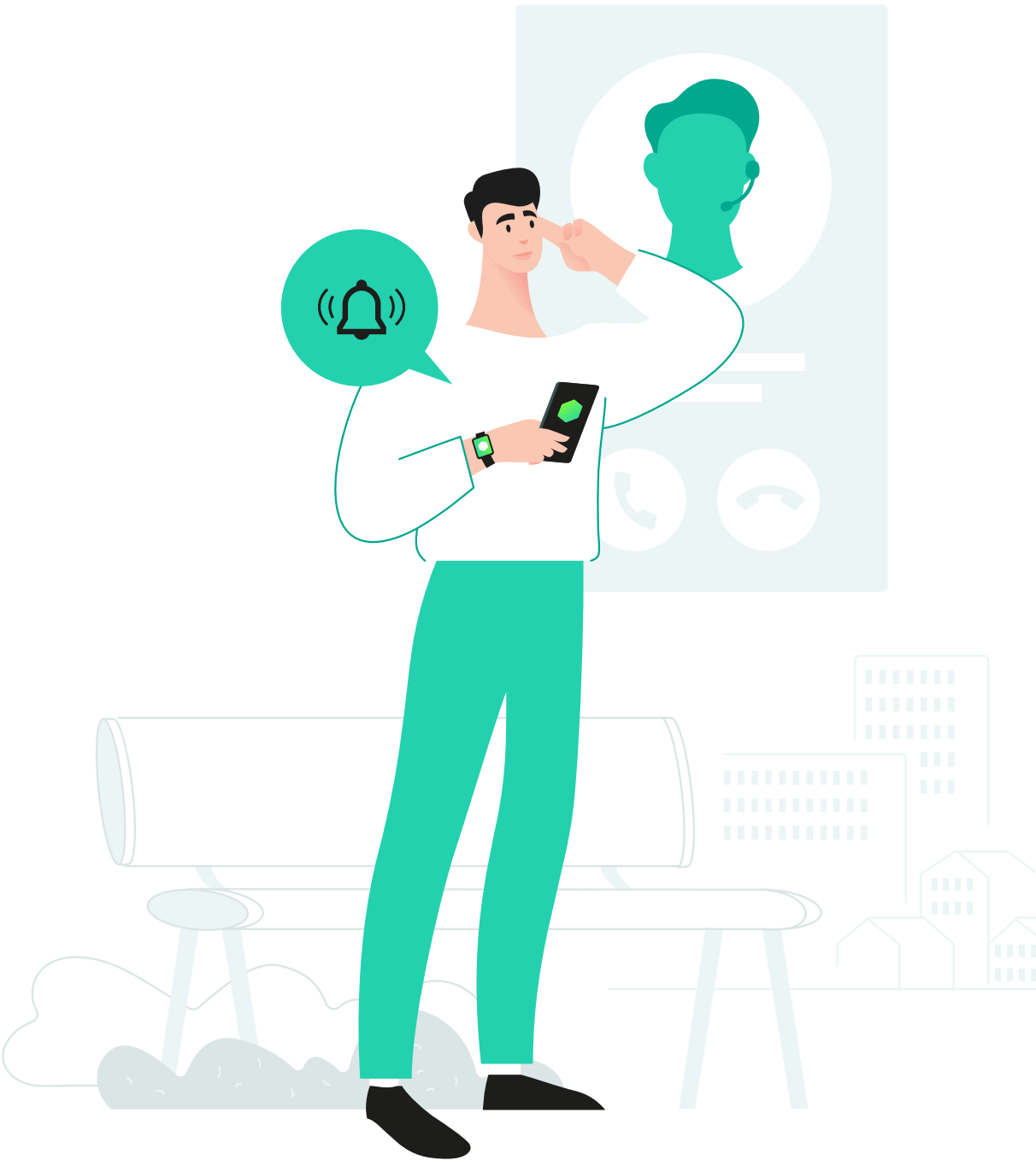
Treat other people's personal data like you would treat your own – with care

Follow the same principles with other people's data as you would with your personal information that you can control. Only upload personal data of third parties to reliable resources, do not show it to other people and consider how this data may be used.

3.

Always warn others about recording a conversation

Besides covert recordings being universally unethical and disrespectful to the participants of the conversation, in some countries they are also illegal.



4.

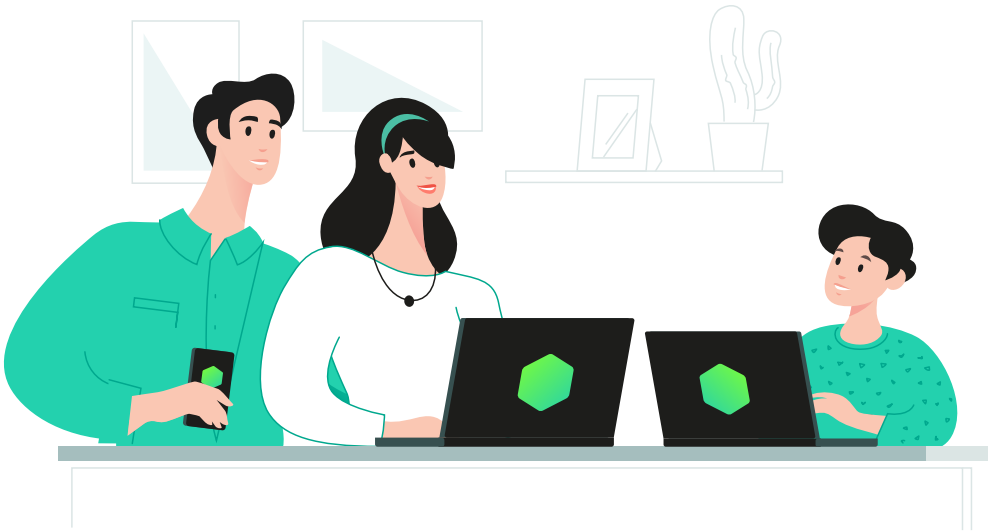
Do not share information about your family relations or close connections in public social media accounts

Personal connections reveal more than you think – they show which people mean a lot to you and hence make you vulnerable. This information may be used not just against you, but against your close connections too.

5.

Talk to your friends and family about treating your data right

Have conversations within your community to set some data hygiene standards for each other, and remember to check in with each other if, and when, anything relating to personal data leaks happens. There has to be a level of trust within your trusted network about how data is shared externally.



www.kaspersky.com

kaspersky

GBD-7837 Q1/21 V1