Counter-OSINT: a guide to protecting your personal data

Оглавление

Counter-OSINT: a guide to protecting your personal data
Introduction
Why it is important
What will happen in the next chapters
Basic digital hygiene
Phone number
We share personal life and work
Using a virtual number
Email address
Separation of accounts
Down with subscription boxes, trash and spam
Disposable email mailboxes
Public Email Mailboxes
Forwarding mail from other mailboxes
Using a personal domain to create catch-all mailboxes
Using Bitwarden to generate email aliases
Last name, first name, patronymic, date of birth
Government agencies
Login via another site (Single sign-on)
Address and location
How to prevent address leaks
Using subscriber boxes
Password
Password managers
Check your passwords against leaks
How to come up with strong passwords
Signing in without a password
LessPass
Useful materials and links to sources
Photo
How to test yourself
How to remove yourself from face search engines
Face photo as biometrics

Photo metadata
Materials used and useful links
Database leaks and “probiv” (unauthorized data lookup)
Do this today
Check what has leaked about you specifically
You cannot delete your data from leaks
What usually leaks
How this differs between countries
Determining the source of a leak
Finding yourself in leaks
Using aliases/fake email addresses
Using different names for tracking
Canary tokens
Canary tokens
Difference from phishing and logger links
How to make leaks useless
Creating a new fake account
Fake links with commonly used identifiers
Sites for generating plausible data
Phone privacy
Contacts from the phone book
Installed applications
Materials used and useful links
Wi-Fi
Privacy of social networks and messengers
What this section covers
If your platform is not here
Facebook
Who can see your posts
How people can find you on Facebook
Used materials and useful links
Telegram
Privacy
VKontakte
Settings
Instagram
Privacy for developers
Exposing your email address
Linking a phone to an account is not always a good idea

Removing information about yourself
Deleting your own accounts
Deleting search results in search engines
Removing information about leaks
Screen sharing
Russia
Documents
Probiv (unauthorized data lookup)
Data leaks to public access
What to do
Ukraine
Documents
Probiv (unauthorized data lookup)
Data leaks to public access
Belarus
Documents
Probiv (unauthorized data lookup)
Public data breaches
Kazakhstan
Documents
Probiv (unauthorized data lookup)
Public data breaches
Identification Documents in Brazil: What They Are and Their Purpose
CPF — Individual Taxpayer Identification Number
RG — General Registry
CNPJ — National Registry of Legal Entities
RENAVAM — National Registry of Motor Vehicles
CRV — Vehicle Registration Certificate
Data Breaches: A Threat to Privacy and Security
Measures to Enhance Online Security
About this edition

Counter-OSINT: a guide to protecting your personal data

How to keep others from building a dossier on you. Written for Russia and the CIS, useful anywhere.

Edition of 17.11.2026.

The current version and other formats: counter-osint.soxoj.com/en/pdf

This work is distributed under the Creative Commons Attribution-ShareAlike 4.0 International licence (CC BY-SA 4.0). You are free to copy, distribute and adapt it, including commercially, as long as you give credit and release derivative works under the same licence.

Introduction

🚫 This guide **is not about anonymity**.

Anonymity is the complete concealment of information about yourself, including your identity. To make it impossible to understand who you are. Maintaining anonymity on the Web is difficult even for people from organized hacker groups. You should start with *privacy* - hiding information about your personal life. Maintaining privacy is easier, it’s like hygiene.

🚫 This guide **is not about resisting big brother and corporations**.

I have no goal to tell you how to become elusive and not let big companies make money off you. You are already in the system, you are already being used, you are already a product. And if you confidently object and consider yourself anonymous, you are probably in another system, maybe even a criminal one, and you are unlikely to learn anything new here.

✅ This guide is **about the value of personal information**.

Everyone is free to decide for themselves what to hide. I just want to show you how the data that you have not hidden is used, and how to stop this use. How to understand how valuable the information is that you are going to enter into the window and click the “Save” button. How not to sell your personal data at the price of a shawarma.

✅ This guide **is about privacy and counter-OSINT**.

You will learn about how people who collect information about you think. What they use and are guided by, what data is important to them. What they can do with this information (and do!).

And, of course, you will receive instructions on how to reduce the risks of losing your privacy to zero. In fact, it is a guide for newcomers to the world of personal counterintelligence.

Welcome!

▶ 🕵 Advanced level

Why it is important

It is difficult to stay out of the access zone in our digital time. A hermit can have an emergency phone, and a dog, although not every one, has an Instagram account.

The penetration of social networks and means of communication into our lives could be extremely positive if it did not lead to a lot of sad consequences. From calls from fake Sberbank employees with a request to dictate a password from SMS, and to collectors suddenly demanding to repay a loan issued on your passport.

In recent years, there has been a trend towards privacy and protection of user information: GDPR, CCPA, LGBD. The companies were obliged to take care of the safety of personal data and to prevent their leaks. But did they start collecting less information about us? Absolutely not. For them, our data is a source of profit.

But the tightening of legal norms for companies is not enough. You probably left a lot of “bread crumbs”, because it’s not the first year on the Internet. Old accounts, ads, public correspondence, photos. Following these traces, you can come close to you and use it for any purpose.

Interesting fact: in 2017, a journalist found the anonymous accounts of the FBI director in just a couple of hours. It was enough to get a tip about his existence, information about his son and about his thesis in theology.

A huge array of data about people, which can be easily collected by improvised means, has led to the popularity of OSINT, a methodology for collecting data from open sources. Often, this term now refers to means of spying on people, although initially it is an intelligence methodology. Any means can be used for both good and bad purposes — this should not be forgotten.

Therefore, it is important to have **Counter-OSINT** tools to protect your data and ensure privacy.

What will happen in the next chapters

Let’s analyze simple but effective steps that will make it very difficult for an outside observer to collect information about you. With specific points and actions.

The guide will be useful to a wide range of interested people — not only those who have heard something about OSINT, but also friends, acquaintances, parents. An investment of half an hour for thoughtful reading and conscious actions will bring peace of mind and protection from fraud, surveillance, harassment, blackmail.

At the same time, we will not neglect convenience. Many guides concentrate on protecting yourself to the maximum (even if it is not justified). We will proceed from the need to maintain **a balance between privacy and convenience**, in which the use of the Internet will not be complicated.

Let me remind you that OSINT is the collection of information from open sources. But, unfortunately, such sensitive data as databases of phone numbers, passport data and so on often get into the Network.

Moreover, in the Russian Federation, through “probiv” (unauthorized data lookup), you can get detailed information about the owner of a phone number, car, apartment from official state registers and databases. Unfortunately, many people are willing to provide access to what should be carefully protected for money.

We will take this into account: it is impossible to ensure complete anonymity and remove yourself from all registries, but it is possible to complicate the search process so much that an attacker will not be able to cling to the information.

Thus, the purpose of the guide is to teach how to protect publicly available information and complicate the process of finding other information about you.

Identifying important information

To understand which data is more important and what should be protected more, it is necessary to know modern realities adjusted for Runet. We will analyze this further, and to try to be objective, we use OPSEC.

The term OPSEC, like OSINT, came from American intelligence. It means the process of analyzing and protecting critical information.



Chatter - help the enemy!

To begin with, let’s list all the **primary data** that somehow reveal our identity, but *exist physically outside the Internet*.

- Last name, first name, patronymic
- Date of birth
- Passport data (series, number, etc.)

- Physical address
- Personal documents (driver’s license, etc.)
- Biometric data
- Other personal and identifying information

There is not much such data. But, having at least a part, you can pretend to be you and deceive third parties. For example, send a message to friends asking them to urgently transfer money due to a difficult situation.

At the same time, scammers will not necessarily be interested specifically in your identity. For example, they can buy a database and hundreds of “fresh” passports to link passport data to QIWI e-wallets to increase the limits on money withdrawal.

Any personal data may be used. For example, restoring access to social media accounts often requires answering a security question. Thus, knowing your mother’s maiden name or your favorite musician increases the chances of hacking you.

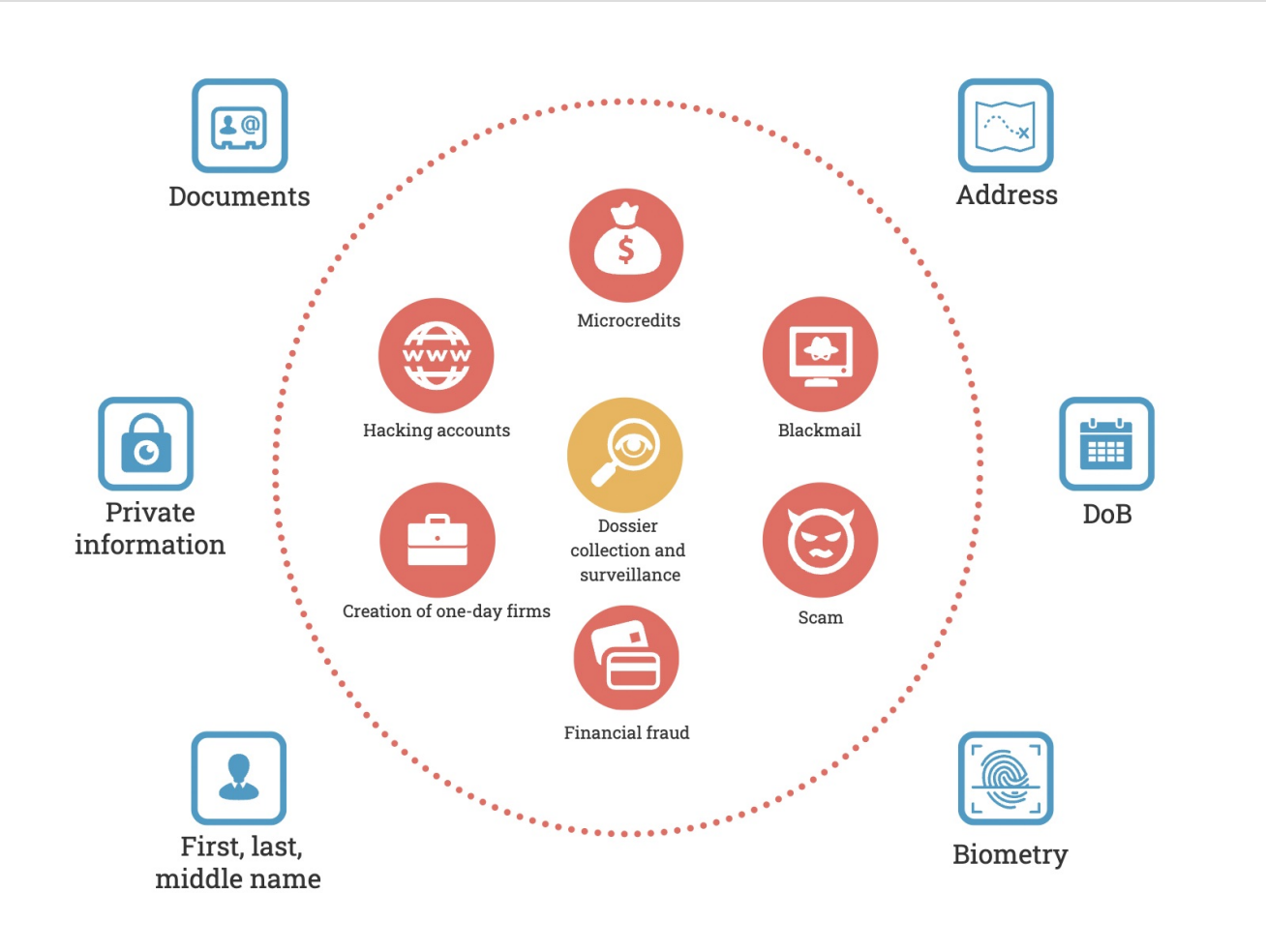
Interesting fact: a high-profile case occurred in 2012 — the capturing of 4 accounts of a person at once with knowledge of only the address, name and email. An elegant chain of access recovery — first using known data, then linking fake ones — allowed the attacker to first gain access to Amazon, GMail, Apple, Twitter, and then remotely erase data from the person’s devices.

Perhaps you were confused by the item “biometric data”, but, alas, their use has long entered our lives. Face search tools have long been common, which use the same technologies as for unlocking a personal phone through the front camera, as well as extensive databases from social networks. When you post your photo online, you leave an opportunity to find yourself.

Analyzing threats

In accordance with the OPSEC process, we will analyze who may be interested in such actions and how they can use information about us. Let’s

look at the popular cases of using primary data in the diagram below and try to draw conclusions.



What can be done with our data?

What can be done with our data? Surely you have noticed that most of the items are related to **receiving money**. I think the financial motivation of scammers does not require an explanation. The only thing to note is that money can be stolen not only from you, but also from other persons. In this case, participation in the criminal process becomes critical for us, where both the witness and the accused can be involved.

The benefits of collecting complete information about you, including access to correspondence, are less defined. This can be both domestic harassment, and espionage, blackmail, and so on. It is only clear that in most cases it is **causing personal harm and invasion of privacy**.

These threats are understandable and explainable, and in many cases regulated by law. It makes no sense to list articles related to financial losses, there are so many of them; and the collection of personal data is Article 137 of the Criminal Code of the Russian Federation. However, let’s face it: it takes a serious reason to go and force the initiation of a case on your own, and participation in such processes is stressful. Therefore, let’s return to the position already voiced above: our goal is to protect our data and avoid threats.

Obviously, knowledge of the primary data is not enough to conduct fraudulent schemes. These methods are based on social engineering and involve remote interaction through a call or messages. That is, we implicitly mean that our detractors already know our **secondary data, virtual identifiers** — phone number, email, social network account address. Thus, getting information about this data carries no less threat.

Each of the data types will be described in more detail later. In the meantime, let’s leave our attention on the fact that the more data falls into the wrong hands, the more serious the outcome may be. Hence the conclusion — the amount of data about you must be controlled, do not scatter them where it should not be and monitor their use.

Let’s talk about **digital hygiene**.

Basic digital hygiene

Let’s formulate our goal: to minimize the amount of data that can be collected about you in one place.

Don’t put eggs in one basket.

Why is it important?

Example 1

You are using the services of a company that spends too little money on security. At one point, they are **hacked**, and the entire customer base is in the hands of intruders: phones, postal addresses, names, surnames, your purchases. Almost always, such databases end up in the public domain as a result. As a result, your data will be available to everyone.

Example 2

You use the company’s services in a highly competitive business where the price of customer data is very high. Some employees leave for competing companies, **copying** their customer base. How this database will be used, and whether it will go further in the hands — there are no guarantees.

Example 3

You use the services of a company that collects the data of its customers to offer discounts and promotions. To do this, they send out advertisements using the services of another company. This company does mailing lists all the time, and is interested in having its own customer data. Therefore, the second company **accumulates** databases with the data of other customers, which can then be reused for other mailings.

Surely you have an objection: *is it really not controlled by the law in any way? They cannot legally use this data!*

Unfortunately, the legislation in the field of personal data processing (PD) does not keep up with the real state of affairs. Exchange of virtual (not physical!) data is difficult to track and stop. Moreover, the market for illegal PD exchange is so developed that big players are lobbying for its

legalization. In such circumstances, we cannot rely on the protection of the state or the guarantees of companies, and we need to be more conscious to what data and in what quantity we give to others.

Phone number

Earlier we said that a phone number is a **secondary** identifier. From the point of view of common sense, this is so: you can get rid of the phone, break the contract with the operator, or maybe buy 100 numbers, and then the curious will plunge into analytical paralysis, trying to figure it out.

But from the point of view of online platforms, the phone is the most convenient means of communicating with you and confirming your identity. Therefore, *almost all* use the number as a **primary**, a unique identifier.

This leads to an obvious conclusion. Almost any website knows your phone number and has its own information about you. The site can exchange this information (and does it!) with other companies - within the framework of services, for money, by barter.

Examples of such sites and platforms: - Authorization systems in public Wi-Fi (97-FZ) - Discount and discount cards - Authorization /verification in social networks and messengers

By combining all the pieces of information on your phone number from different places, you can assemble your portrait. What to do about it?

We share personal life and work

Almost all of us have work and personal affairs. Therefore, it is worth starting with the separation of these spheres of life.

Most large companies offer corporate communication to employees: either you take a new SIM card from the company, or a working tariff is connected to your personal number.

But even if there is no such possibility, **always** get a separate phone number. I have several arguments: - It will be impossible to link your accounts by numbers automatically, except through an agreement with the operator. And this is already a high level of protection! - With a separate phone, it is much easier to think in terms of privacy. You have a choice of

which number to link to SMS banking, and which one on the company's public website. - Work is work, it should be separated from rest and your personal life. And the second phone will only benefit. :)

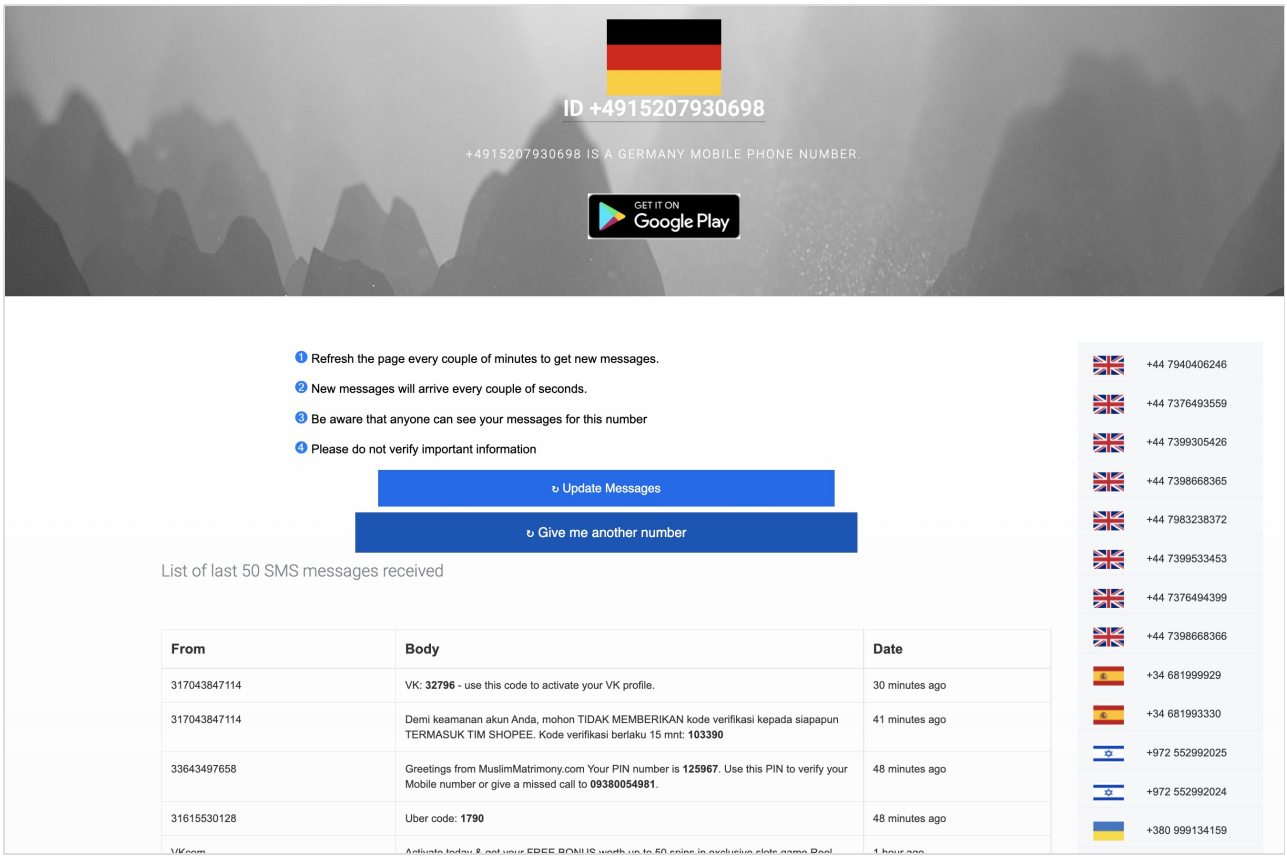
Using a virtual number

There are 3 segments of services that help protect your real phone number.

Services for one-time SMS reception

There are public websites that allow you to receive SMS from any sender. We will not list them, because they are simply Googled by the phrase `receive sms online`.

They use a small number of phone numbers at the same time, and often they already have accounts on different sites: testers, spammers, scammers. However, they can be used for authorization in public Wi-Fi networks. The only disadvantage of this approach is that you already need the Internet to access the public Internet. ☺

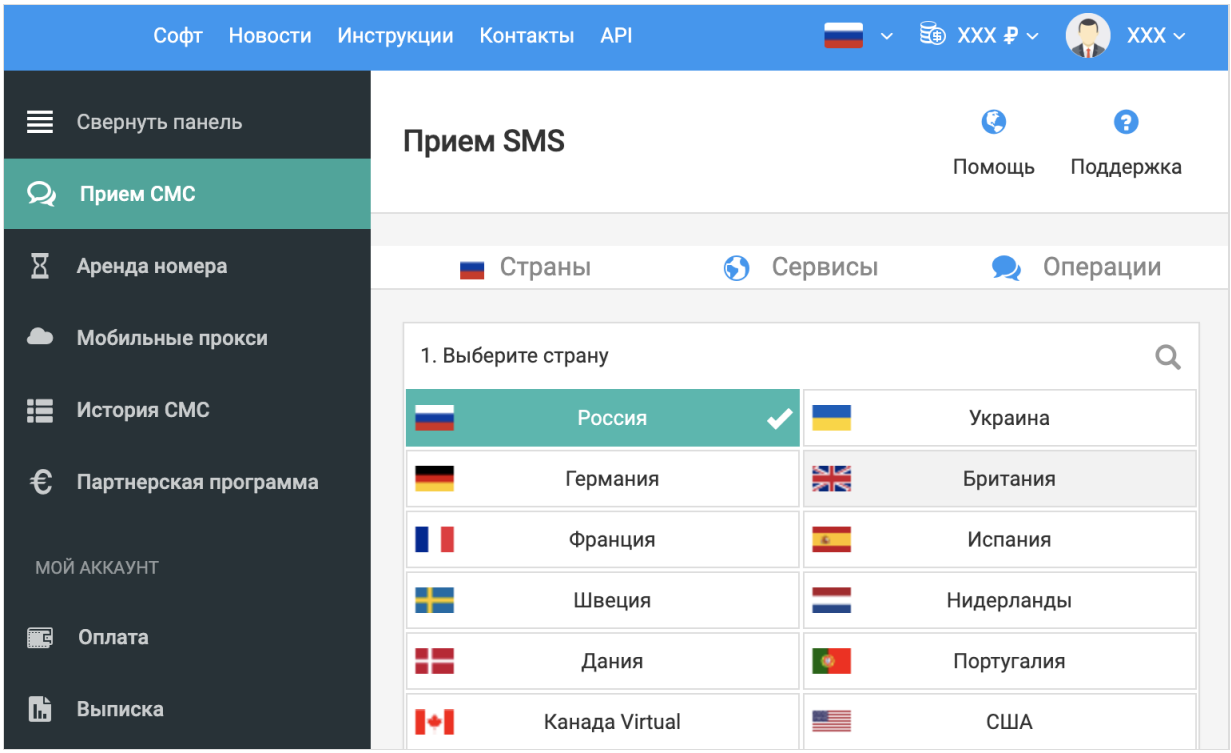


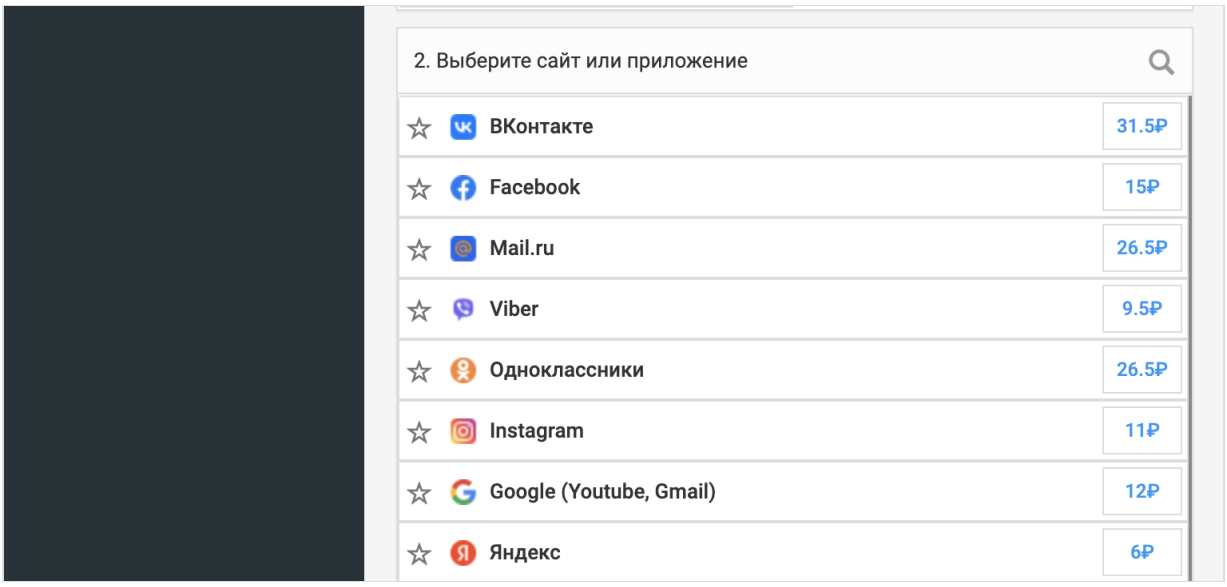
Of course, it is not recommended to use such services to obtain sensitive information and link it to your personal accounts, since anyone can see the

received messages and access codes.

And a little advice: before trying to use a number from any of these sites, you should pay attention to the time of receipt of the last SMS message (the table in the screenshot above). If this time is far in the past, then the number is no longer working, but it has not yet been removed from the site.

Services for receiving SMS for a specific site





The section will be updated

Permanent Virtual Phone Number services

Some carriers offer customers a **substitute number** for incoming and outgoing calls and SMS as a bonus to the main plan — without a separate SIM card. The substitute number works through the carrier's app and can be changed in a couple of taps, leaving the main number unchanged.

For example, in Russia this is offered by **T-Mobile** (T-Bank's MVNO, not affiliated with Deutsche Telekom): a substitute number is included in the base plan and can be changed from the app. Similar features are available from Yota, MTS («Second Number») and a number of foreign carriers.

The main rule: never save the substitute number anywhere — not in your address book, not in any profile. This lets you rotate it regularly without consequences: as soon as spam starts coming in, you generate a new one.

Typical use cases: - price requests from companies with «leave a request» forms; - registration on one-off resources (promos, giveaways, surveys); - access to public Wi-Fi with SMS authorization.

For a higher level of protection, the substitute number is worth combining with Hide My Email — together they cover most everyday registrations where your primary contacts are not actually needed.

⚠ **Weak spot — the human factor.** If you give your real name during registration, the chain of accounts tied to a single substitute number can still be linked. When using this scheme, use a pseudonym.

Email address

The email address was and remains the most common identifier for an account on the Network. You may not have a phone number, but you must have a mailbox - this is an unwritten rule.

The presence of an email in itself reveals some information about you. First of all, this is **alias**, the name of the box, to the left of the symbol “@”. The first and most obvious advice is not to choose your initials, surname and year of birth by name, unless it is a purely personal or work mailbox.

The second, but important tip is to carefully study the email provider. The most well-known free mail services “in pursuit” of email give you accounts in other products. This is especially true of Google and Yandex, as these companies conduct their business in a large number of other areas, and to provide you with a free box for what you will become passive consumer of a dozen other services – their bread and butter.

Separation of accounts

To make it more difficult to find information about you, it is recommended to use email addresses wisely, using the technical ability to create their variations. According to official standards, after the alias and before the @ sign, you can specify an additional suffix with “+”, e.g `nickname+facebook@google.com`. Emails to such an email address will be sent to the owner of `nickname@google.com`, but from the point of view of sites, it will be a completely different email address. Google, in addition, has a feature: any dots in the alias are considered optional and work as suffixes after the “+”.

There are several usage schemes: a unique email address for each service, a unique email address for each “personality”, or use only for some services according to a scheme known only to you.

Additional benefits of using suffixes and dots are described here. Also, you can check the tool mailto_analyzer for analyzing your email address exposure.

Down with subscription boxes, trash and spam

Separately, it is worth noting the habit of a large number of people to use a separate “garbage” mailbox for non-critical services and a variety of spam subscriptions. By itself, the separation of mailboxes is useful, but only if it is conscious (see above).

If you do not look into such a box, and the letters are lying there unread by thousands or more, then this is an important signal: figure out whether you really need this box. If not, then unsubscribe from all mailings and delete the accounts associated with it, to minimize the possibility of using this email address to collect information about you.

Disposable email mailboxes

There are a large number of services that provide one-time mailboxes for 10-15 minutes. They are good for one-time registrations on sites where you get to for the first time and most likely will not use them anymore. Here we will consider those services that are created on random domains.

Services that generate plausible-looking aliases (first name. last name):

- TemporaryMail
- MinuteInbox

Other popular services: - 10minutemail - TEMPMAIL - Mohmal

Public Email Mailboxes

Also on the Internet you can find services that make it possible to use **your alias** for a temporary mailbox. Such email addresses are convenient to use for services in which email should look plausible.

Examples of such services:

- Maildrop
- Mailsac
- templail+
- Yopmail - It also supports forwarding (see below)

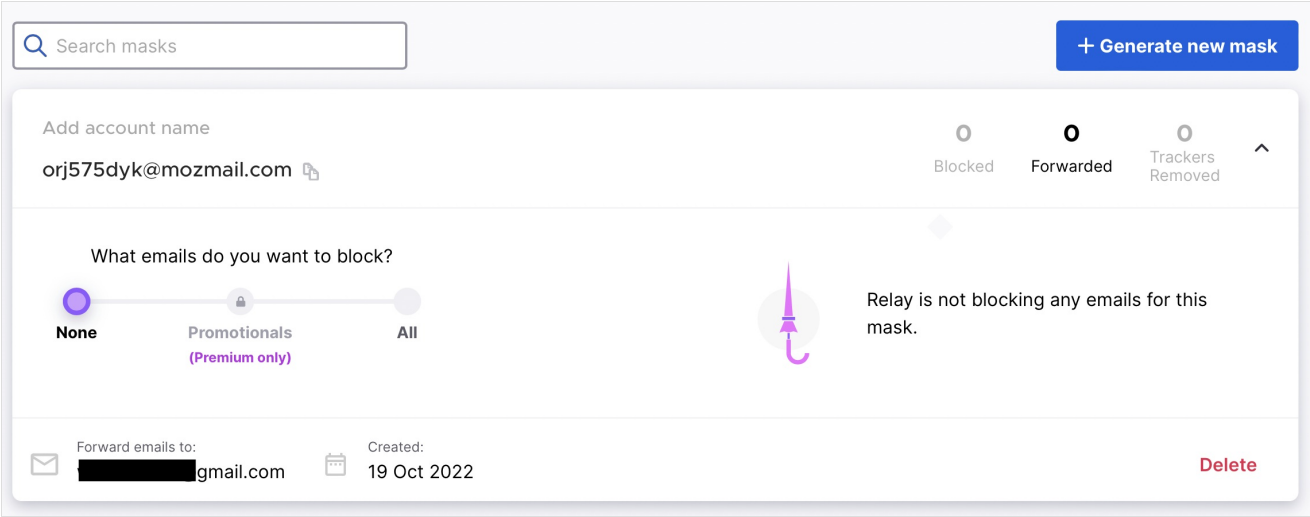
Forwarding mail from other mailboxes

Services that allow you to forward emails use so-called “masks” that allow you to hide your real email address.

The principle of operation is very simple: - The mask address receives an email - The email is forwarded from this address to your real address

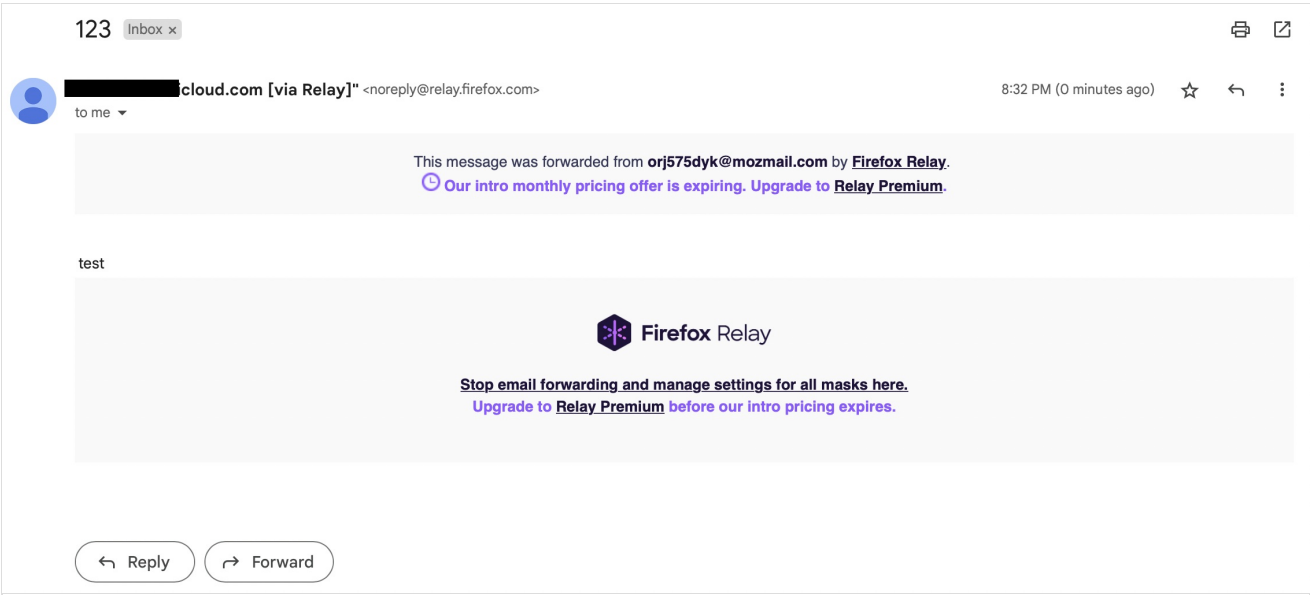
Example based on Firefox Relay:

First, a mask is provided that hides the real address.



firefoxrelay

Now, using this mask address, we can receive emails to our email address without showing it to the whole Internet.



relayedemail

Examples of services:

- SimpleLogin
- AnonAddy - generates addresses according to a template `*@ivanov.anonaddy.com`
- Firefox Relay - generates random addresses on the domain `mozmail.com`
- erine.email - makes addresses according to a template `*.ivanov@erine.email`

Hide My Email (Apple)

Apple offers **iCloud+** subscribers its own email-masking service called «Hide My Email». It is available from Apple ID settings on any Apple device and via the browser at iCloud.com, and is offered as an option in email fields when registering through Safari or via the system Passwords app.

One-time addresses are generated, e.g.:

```
6g662b5nbb@privaterelay.appleid.com
gains-unworn0x@icloud.com
argosy-07raving@icloud.com
```

Mail sent to them is forwarded to the «real» mailbox linked to the Apple ID; you can reply, and the recipient only sees the mask, not your real address. The forwarding address can be changed at any time, and unwanted masks can be deleted: after deletion, the flow of emails and spam to that mask stops immediately.

▶ 🥷 Advanced level

Last name, first name, patronymic, date of birth

Why is this information placed in a separate section? As a rule, the full name and date are enough to find a specific person, since the probability of two people matching all these data is very low.

Government agencies

There are regulations in various fields that oblige or encourage the publication of documents with personal data. On the one hand, openness in these areas helps transparency in the industry (for example, public procurement, lists of past/graduates), but we are more concerned that once we get into such a document, it will be difficult for us to leave it.

Russia includes the following: - lists of applicants at universities: they are often laid out with full names, the number of points, from the year of the enrollment order, it can be concluded about the age; - information about individual entrepreneurs, managers and founders of companies (USRLE/EGRIP); - public files of court cases: once you have committed an offense and even managed to justify yourself, you can be found by the case history; - public telephone databases: for the most part contain irrelevant information, but with reference to the house and apartment; - public registers of debts and pledges; - and so on.

The section will be updated

Login via another site (Single sign-on)

The modern architecture of authorization and registration in online services involves the active use of third-party “verified” accounts. For example, almost everywhere in the foreign segment of the Internet there is an opportunity to log in via Facebook, while in Russia, VK login is increasingly spreading. In some services, this is implied implicitly, for example, logging into YouTube through a Google account.

If you log in to a non-primary and public device in this way (for example, a TV or a game console), then there is a risk of disclosure publicly displayed information about yourself, for example, first and last name. To minimize this risk, it is worth renaming the account from “First Name Last Name” to something neutral, for example, “Account”.

Address and location

To begin with, we will highlight several criteria that it makes sense to pay attention to from the point of view of OPSEC.

These are: - geolocation: your real-time location, which most often leaks through digital channels; it can be both coordinates and the address to the apartment; - permanent registration address: what is most often called a “residence permit” is an anachronism of post-Soviet Russia, required in many state systems, but almost everywhere superseded by the following address - address of actual residence: the address at which you are “temporarily registered”, also required by various laws and acts to be able to provide you with various services.

Unfortunately, unlike in the USA, where your address = your mailbox, in Russia the address is strictly tied to physical real estate. Therefore, we cannot have tricks with “nomadism” as in Texas or South Dakota, where you do not necessarily have a place of residence. However, it is possible to use subscriber boxes, as described below.

How to prevent address leaks

- Do not publish photos in a “raw” form, files. They often contain information about the shooting location.
- If you use delivery, specify the minimum required amount of information in the standard address fields. The most preferable option is to specify only the house number and meet the courier outside. Write everything else (floor / apartment / intercom) in the additional information field — the courier will easily read it, but such unstructured information is less likely to get into the database with your address.

Using subscriber boxes

In Russia there is a single state operator of the postal network: Russian Post. It carries out most of the mail.

For delivery, the address of the person’s residence and their name are usually used, i.e., it is necessary to specify the full name, postal code, as well as the full address, including the apartment number. Ordinary letters or notices of registered letters/parcels are delivered by postmen up to the mailbox on the door of the house or in the entrance of an apartment building.

However, there is a possibility of anonymous mail delivery for the sender using post office boxes. This is a dedicated mailbox for mail in a specific mail division. Each box has its own number, online you can choose any unoccupied, for example, `777`. Also, under the lease agreement, it can be assigned an arbitrary name - this is a paid (and relatively expensive) service. The only disadvantage from the point of view of privacy is that to rent a mailbox, you need to create an account on abox.pochta.ru by specifying your phone number and passport details.

After signing the contract, you will receive the key to the mailbox, and you can open it at any time. But it is important to understand that the boxes are located on the territory of post offices, and access to them is regulated by its working hours. Therefore, it is more convenient to choose the largest branches where the subscriber department works around the clock. In Moscow, for example, this is a post office on Myasnitskaya Street, index `101000`.

How do I send letters now? As an address, ask your correspondents to specify only the postal code and the P.O. box number. Let’s take the examples above.

Canonical entry: `101000, P.O. box 777`

Or in short: `101000, 777`

And if you have assigned the name “Dump” to the box, then: `101000, Dump`

The rules for the delivery of shipments also apply to subscriber boxes. This means that only notifications will be sent to you for registered letters, and to receive them, you need to dictate the phone number to the employee of

the subscriber department, receive an SMS, and only after that you will be given a letter. But ordinary letters, of course, will be put directly in the mailbox.

Password

The main principle: **never use the same or similar passwords.**

For two reasons: - An email and password leaked from one site are often tried on others afterwards — your mailbox, Instagram, Amazon — and that is how accounts get broken into. Nobody has to be after you personally for that: hacked accounts are a commodity, and the market for them is large. - If your accounts and passwords surfaced in leaks, a shared password ties together even completely different emails and phone numbers. That is how journalists tied ten email addresses to one man (the story is in Russian).

The second reason matters more for privacy. A shared password links your accounts as firmly as a shared phone number: it works as one more identifier of yours. **Changing the password does not erase that link: the “email and password” record stays in the leak forever.** So never reuse a password you have already had somewhere, not even on a brand-new account.

Password managers

You do not have to remember a hundred passwords. You need to remember one — the one for your password manager.

A password manager is a program that makes up passwords, stores them and fills in the right one on the right site. **If your phone or browser offers to “save password” and you agree, you are already using one:** on an iPhone it is the Passwords app, in Chrome and on Android it is Google Password Manager.

Start with the one you already have: check which of your passwords have already leaked.

The one password you need to remember is, for a built-in manager, the password of your Apple or Google account; for a standalone program, its master password.

The account that holds your passwords now opens everything else, so give it extra protection:

- turn on two-factor authentication for it: signing in then takes a code as well as the password. Look for it in the account's security settings, and pick a method other than SMS codes if you can (why);
- set a phone passcode longer than four digits and do not type it where others can watch: **whoever knows the passcode and takes the phone can open every saved password.** On an iPhone turn on Stolen Device Protection (Settings → Face ID & Passcode): with it, away from home and work, passwords open only with your face or fingerprint, and the passcode alone is not enough;
- do not install cracked software on your computer: it can bring along a virus that pulls out your passwords — from the browser and from text files on your desktop alike.

A manager does one more thing, less noticeable: it fills in a password only on the site it was saved for. If you open a sign-in page and the manager does not offer the password, check the address: it may not be the site you saved. People rarely spot the difference between `paypal.com` and `paypa1.com` by eye, while the manager does.

A manager cannot protect a sign-in code: you type that in yourself. **Enter codes only on a site you went to yourself, not through a link in a message, and never read them out to anyone.** That is how Telegram accounts get hijacked: sign-in there is by code, and unless you have set a two-step verification password, the code is all a thief needs. Set one: Settings → Privacy and Security → Two-Step Verification.

A built-in manager keeps passwords in your Apple or Google account. Passwords from an iPhone will not show up on Android on their own — you will have to move them — and on a Windows computer you need Apple's iCloud for Windows app. A standalone manager is tied to neither Apple nor Google: it works the same on any phone and computer.

It is better not to keep passwords in the browser on a computer: a virus gets them out of there easily. Keep them in a standalone manager, where they are encrypted with the master password.

Of the standalone managers we recommend Bitwarden: its code is open, so any specialist can check how it handles passwords. The free version stores any number of passwords, works on any number of devices, can keep card numbers and notes, and generates both ordinary passwords and passwords made of random words. Checking all saved passwords against leaks at once is a paid feature.

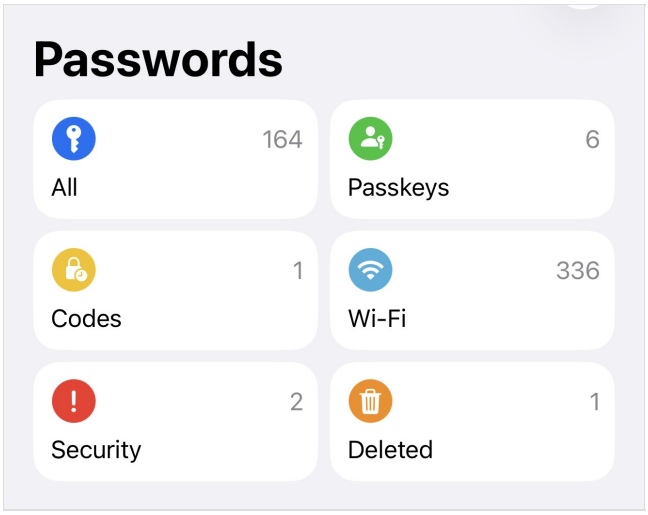
Passwords are stored on Bitwarden's servers encrypted, and only your master password can decrypt them — which is why it has to be strong. All saved passwords can be exported to a file, in case you ever lose access to the service. Unless you pick the encrypted format when exporting, the passwords in the file are in plain text: do not leave it in your downloads and do not send it to anyone.

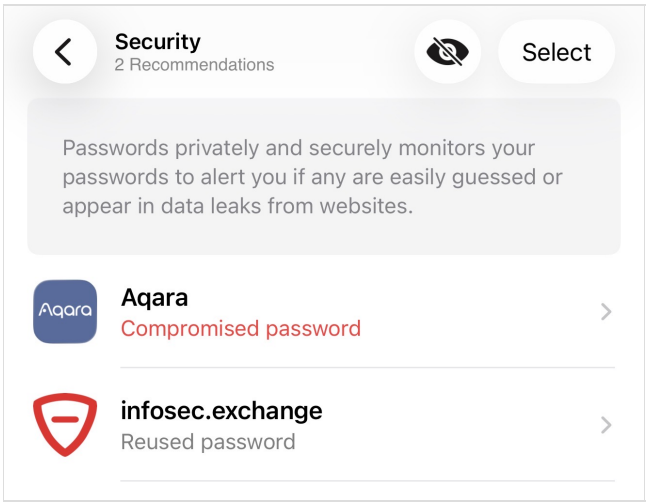
Write the Bitwarden master password down on paper and keep it at home. **If you forget it, nobody can recover it, Bitwarden included** — and all the saved passwords are gone with it.

If you do not want your passwords on someone else's servers, there is KeePassXC: it keeps them in a single encrypted file on your computer. You will have to carry that file to your other devices yourself, and on a phone you will need a separate app.

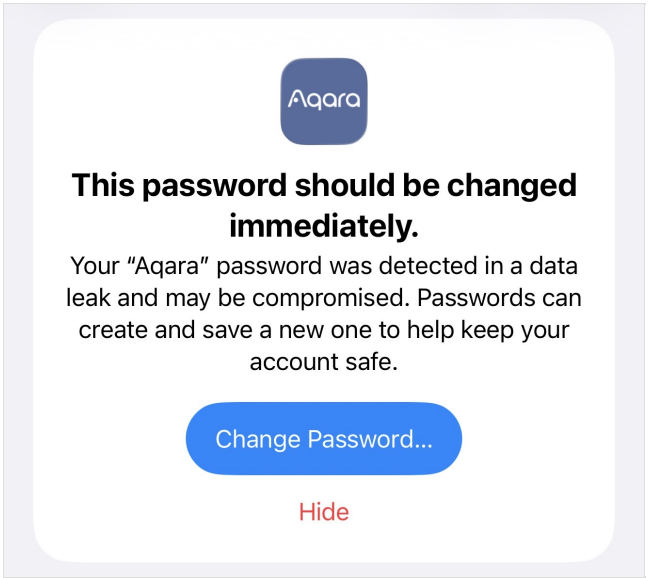
Check your passwords against leaks

A built-in manager checks this on its own. On an iPhone, open the Passwords app and go to Security; in Chrome and on Android, open Password Checkup in Google Password Manager. It shows **which passwords have already turned up in leaks and which ones you reuse on several sites.**





If a password has turned up, it is already being tried in break-ins. Change it everywhere you used it — the same section shows the list. Change your email password first: every other password can be reset through your mailbox. Then banks and government services, then shops where your card is saved. The rest can be changed gradually, as you visit each site.



Here is how: on the site or in the app, open the account settings and find the option to change the password. In the new password field your phone or browser usually suggests a random one — accept it, and it is saved. Afterwards check that the manager holds the new password, not the old one.

A password that is not saved anywhere can be checked at Pwned Passwords, a database of passwords from known leaks. The password itself is not sent there: the page turns it into an irreversible code and sends only the first five characters of that code. The codes of about two thousand other passwords start with the same five characters, and the service cannot tell which one is yours. If you would rather not type a password into someone else's page, just change it.

For what else about you is in the leaks, see the Data leaks chapter.

How to come up with strong passwords

"Eight characters, letters, digits and a special character" is a poor requirement: `P@ssw0rd` meets it.

A password is usually guessed not on the site itself but against a database leaked from it. The passwords in it are most often stored as hashes — irreversible codes — and a program tries variants until the code matches. How fast that goes depends on how the site stored passwords, and you cannot know that in advance. Sometimes the passwords sit in the database in plain text, and then there is nothing to guess.

Attackers try a short password in full, character by character. For a long one they take a dictionary — words and passwords from earlier leaks — and apply the usual rules to every word: **append a year, capitalise the first letter, replace letters with lookalike digits and symbols.** The closer your password is to that pattern, the faster they find it.

What to do: a password of random words

You only have to make up one password yourself — the one that opens the manager: your Apple or Google account password, or the master password of a standalone program. The manager makes up the rest: when you sign up

or change a password, it suggests a random one — accept it. The manager's own password, though, you will have to remember and type by hand, so build it from words. Until you have memorised it, keep it written down on paper at home.

The advice "think of three random words" does not work: people do not come up with random things. The words that come to mind are from one topic, from a recent conversation, or start with the same letter, and such combinations are guessed quickly.

So the words have to arrive ready-made. The Bitwarden generator hands them out — right on the page, with no sign-up; the phrase is put together in your browser and is not sent anywhere. Choose Passphrase there, and you get something like `decal-running-early-reflex-judicial-onshore`. What matters:

- take six words: every added word makes guessing several thousand times longer;
- keep the words that came up: replacing one with your favourite makes the password predictable. If you get a word you do not know, press again and take a whole new phrase;
- separate the words with hyphens or spaces.

Such a phrase cannot be guessed even by someone who knows which list the words came from: there are too many combinations to try in a human lifetime.

What not to do

Two tricks are recommended most often, and neither works. The first is replacing letters with lookalike digits and symbols: `password` as `p@ssw0rd`, `sunshine` as `5un5h1n3`. Password-guessing programs do this on their own: having taken a word from a dictionary, such a program immediately tries all those spellings of it too. The list of substitutions ships as a ready-made file with hashcat, the best known password-guessing program, and is switched on with a single option at launch.

The second trick is typing a word in the wrong keyboard layout: typed on a Latin keyboard, the Russian tongue twister `ехалгрекачерезреку` becomes `t[fkuhtrfxthtphtre`. Guessing dictionaries are converted to another layout automatically, and the trick is so popular that such passwords already sit in the dictionaries as ready strings. Kaspersky went through 231 million passwords from leaks, Russian ones among them, and called this trick popular (that summary is in Russian). **The leaked passwords include `gfhjkm` (the Russian for “password” typed on a Latin keyboard), `vfvf` (“mum”), `gfgf` (“dad”), and the reverse direction — `мдфв` from `vlad`.** The same study found that length alone does not save you: one in five 15-character passwords is guessed in under a minute if it was built from a familiar pattern and the site stored passwords in an outdated way — MD5 in the study.

Signing in without a password

A passkey is a way to sign in without a password. The site asks your phone or computer, and the device confirms that it is you — with your fingerprint, face or PIN. There is no password at all. The site keeps only a key it uses to check your phone, and nobody can sign in with that key.

What this gives you:

- **your key cannot be taken from a leak of the site** — the site does not have it. The old password still works, though: as long as it is valid, someone can sign in with it, so change it to a random one;
- **a fake page does not work**: the key is bound to the site’s address, and on a fake site the browser will not offer it. Such a site may ask for a password or an SMS code instead of the key — do not enter them where you normally sign in with a key.

There is a caveat. The keys are stored in your Apple or Google account, or in a standalone manager, and travel between your devices encrypted. That account becomes the key to everything else: whoever takes it over can get all your sign-ins at once.

Services also call other things “passwordless sign-in”: a code by SMS, or biometrics with the sample stored on their server. Then the sign-in is tied to your phone number or to a face template that is not in your hands. With a passkey, your fingerprint and face never leave the phone — just as when you open a banking app with Face ID.

Support changes fast, so check for yourself: look for “passkey” in the service’s security settings. A Google account is a place to start: it supports passkeys.

LessPass

What if storing passwords and syncing them between devices is too much trouble? There are password managers that store nothing at all. They suit those who do not want to keep passwords in anyone’s cloud.

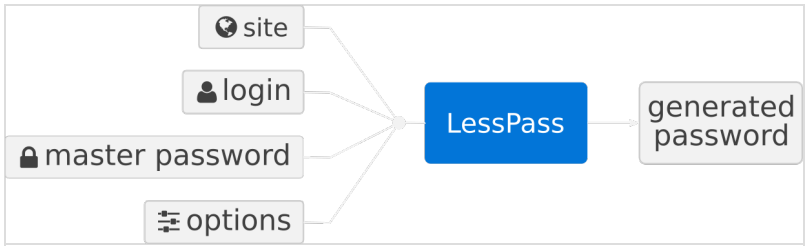
LessPass is the best known of them. It generates each password on the fly with a function that always gives the same result for the same inputs.

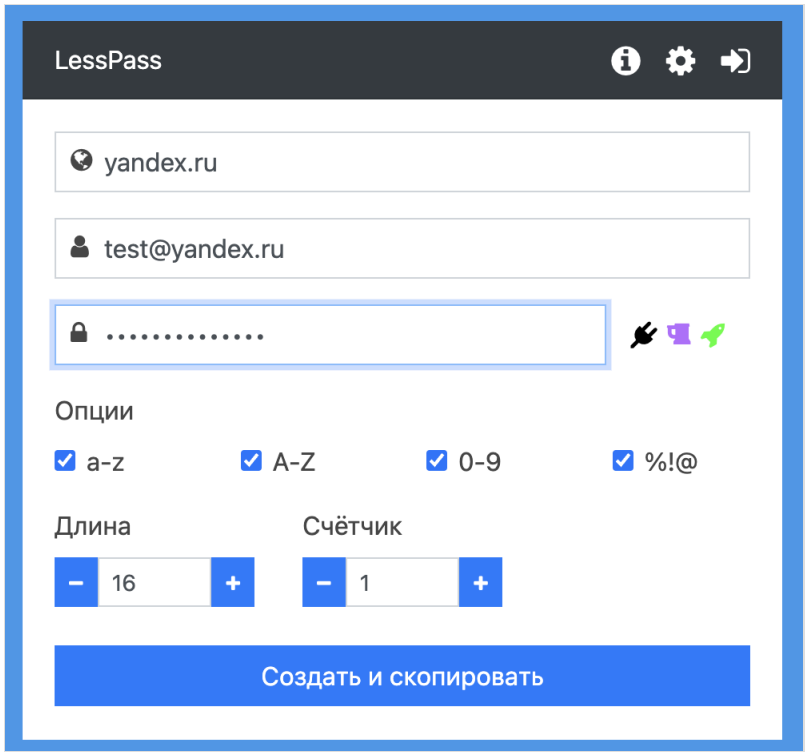
You tell the program: - your master password - your login on the site - the site address

It then generates your password without sending or saving anything. You can run the program on any device at any time and get the same password for that site.

This approach has a downside too. The master password cannot be changed on its own: change it, and all your passwords change at once. And if some site demands a password change or does not accept the generated one, you will have to remember which of the program’s settings you changed for it.

There is a risk as well. If the password for one site leaks in plain text, it can be used to guess the master password, and all the others are derived from the master one. So the master password here has to be as strong as for an ordinary manager.





Useful materials and links to sources

- Free LessPass password manager runs on a pure function (in Russian)

Photo

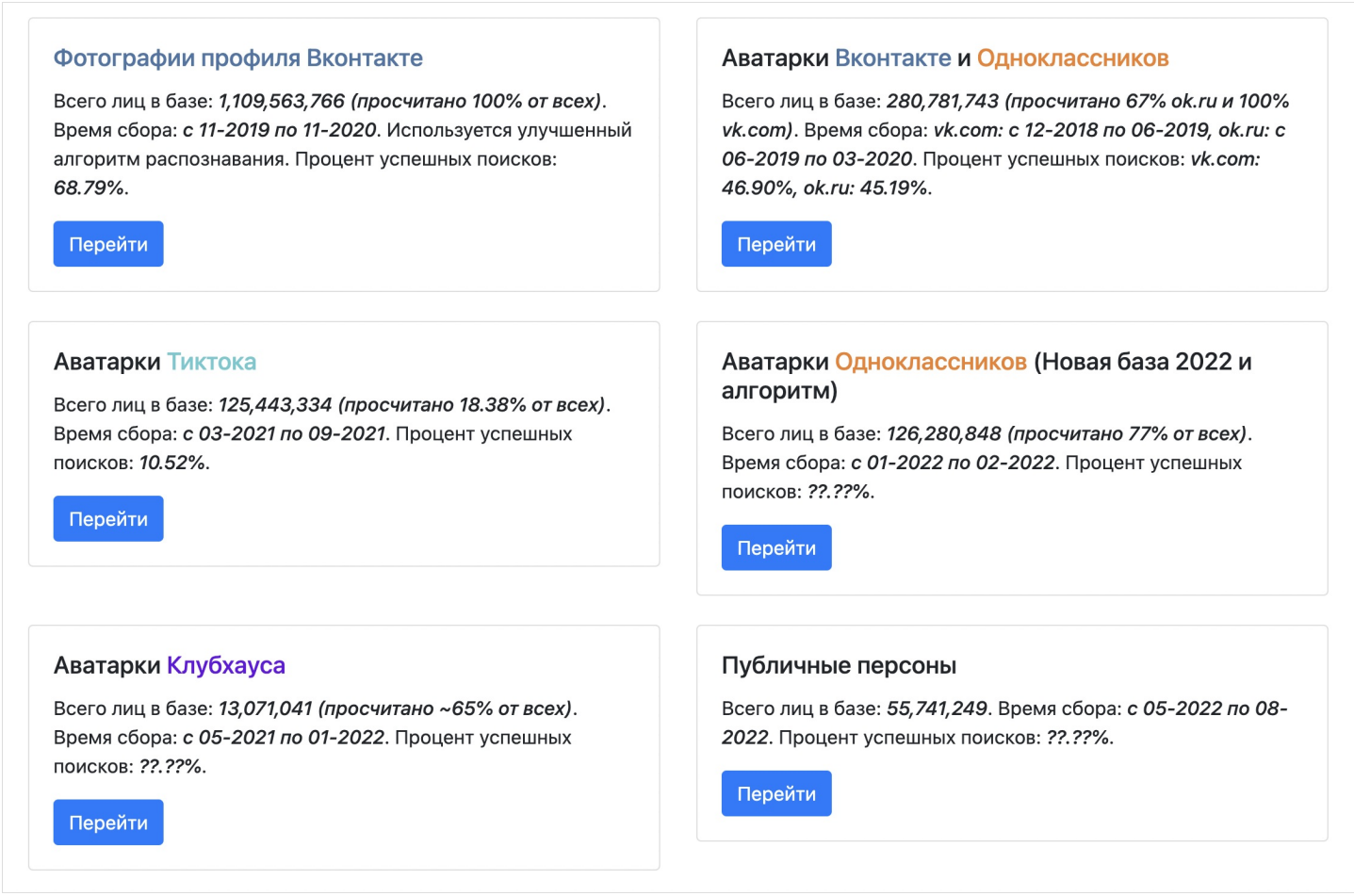
Unfortunately, photos (and any images in general) have long been easily recognized and indexed content. Search engines can search for similar photos, distinguish text, objects, and specific people on them. Social networks can recognize you in an arbitrary photo and put a mark there with a link to you even without your knowledge.

But, fortunately, in recent years, the trend towards privacy has intensified, and therefore social networks are introducing reasonable restrictions on recognizing people. General-purpose search engines refuse to do exact face search too: Google does not look up people by face as a matter of policy, and while Yandex searches for similar images and in practice often does find the person, it has no dedicated “search by face” feature. This reduces the likelihood of malicious use of such functions, but does not prevent the use of such technologies in general. Now recognition tools can be easily created independently or use freemium alternatives.

How to test yourself

In the post-Soviet space, you can still use Yandex. But it alone is not enough: below are the services that search for faces specifically, not for similar pictures.

If you have actively used social networks, you can find not only your account, but also photos with your face in the accounts of your friends, acquaintances or other people who are not even related to you. Of course, it is extremely difficult to delete such photos, and if you do not want them to link to you, then you should competently delete account.



Specialized face search engines

The niche abandoned by general-purpose search engines has been taken over by dedicated services. By definition they have no restrictions on searching for people — that is their entire point. It is worth checking yourself with each of them: their indexes are different, and an empty result in one says nothing about the others.

- Search4Faces — **free, no registration needed** (only its API is paid). Searches avatars and profile photos from VKontakte, Odnoklassniki, TikTok and Clubhouse — that is, exactly where PimEyes and FaceCheck.ID do not look. Its databases are outdated, most of the data was collected in 2022 or earlier, and this cuts both ways: an avatar you changed ages ago is still sitting there, but an empty result today does not mean you are not in it. The database is incomplete, and for an unfamiliar face the service often just returns people who happen to look alike.
- VK.watch — a VKontakte archive: profiles, their edits, friends, photos and comments, including the ones you deleted long ago. It has face search too, as a separate button. That is exactly what makes the service

unpleasant: deleting a photo on VKontakte does not remove it from an archive made earlier. Access is by paid subscription, and according to its own FAQ its subscribers include lawyers, recruiters and private detectives.

- Geometria — search over an archive of event photo reports: clubs, parties, city events. You upload a selfie and find yourself in other people's shots from events you simply attended without giving the photographer a thought. Face recognition is paid.
- PimEyes — indexes the open web: news sites, blogs, stock photo banks, forums. A free search will show you that matches exist, but the previews will be blurred; unblurred images and links to the source pages are available by subscription.
- FaceCheck.ID — positions itself as an "is this person a scammer" check, indexes social networks, police photos and public registries. The service shows its counter of indexed faces right on the front page: at the time of writing it is over 1.4 billion.

The last two find you where Yandex and the Russian archives do not reach: in other people's photo reports, on a conference website, in a sports club gallery, in a group photo from work.

And something common to all of them: by checking yourself you upload your face to a face search engine. It is a sensible trade — you learn what is already known about you — but it is still a trade.

How to remove yourself from face search engines

The terms vary a lot: from free removal by selfie in a minute to an email to an anonymous owner at gmail. And one service offers no such option at all.

FaceCheck.ID. Removal is free and, according to the service, instant: find yourself by searching with your own photo, mark your shots on the Remove My Photos page and confirm your identity with a selfie right in the browser.

PimEyes. The opt-out form requires several photos of your face from different angles and a scan of your passport or ID. That is, to stop being found by your face you have to hand the service additional photos of your

face and a document. They ask you to anonymize the scan by covering everything unnecessary, but whether the trade is worth it is still yours to decide.

Geometria. Here the path is lawful but paper-based: the operator is a Russian legal entity, OOO Geopromedia, and you can withdraw your consent to data processing by sending a scan of a written application to law@geo.pro, or the original by registered mail. Withdrawal deletes your account and the records containing your personal data, but not the photos themselves: they stay in the reports, and under the agreement the administration removes content solely at its own discretion.

Search4Faces. There is no form, but there is an email: the service states outright that you can request removal of your images from search results by writing to search4faces@gmail.com, and promises to reply within 24 hours. There are no guarantees beyond that promise — who owns the service is unknown, its domain is registered through a Bahamas-based privacy registrar, and the correspondence goes through an ordinary gmail mailbox.

VK.watch. The service does have a privacy policy, and it even describes the right to request deletion of your data by writing to support@vk.watch. But it is worth reading carefully: it describes subscriber data — email, billing details, technical logs, search history. Archived VKontakte profiles are not in the list of collected data at all, and there is no obligation to remove you from the archive either. The right to deletion here belongs to the one who searches, not to the one who is found.

Prevention is more reliable than any email anyway: the archive keeps the snapshot that was taken when it was collected, and changing your avatar after the fact is useless — that is the whole point of an archive.

The main thing: removal from an index does not remove the photo itself. It stays where it was — in someone else’s album, on an event website, in a news story — and the next service will index it again. Only removing the original source works reliably: delete your account or ask the site owner to take the photo down.

And these services are not all of them, only the ones visible from the outside. Clearview AI, for example, builds a similar index but sells access only to government customers, and there is no way to check yourself in it. There are other closed services that search an index of photos from social networks and even from messengers popular in particular countries — WhatsApp, Telegram and others. And there your profile photo is open by default: it is visible to anyone who came across your account in a shared group or found you by phone number, so closing it in the privacy settings is worth doing not only against people you know.

Face photo as biometrics

The section will be updated

Cloaking

To combat the tools for recognizing people in images, so-called cloaking is used. The essence of the method is to distort the photo in such a way that visually we perceive it as the original, but the programs did not see a person or a face there.

Methods for distortion can be both manual (blurring / retouching / distortion of individual parts of the photo) and automatic. Of the latter, special programs that use face recognition algorithms in the opposite direction can be noted, modifying the photo so that the search is not possible. An example of such a program: Fawkes.

Of course, such post-processing of photos or videos will not help proactively. To make it difficult to recognize faces with “smart cameras” in real life, original and not very good ways are invented, examples can be read from the links at the end of the page.

Photo metadata

The section will be updated

Materials used and useful links

- Big Brother is (so far) blind
- King’s new makeup

Database leaks and “probiv” (unauthorized data lookup)

It started back in the nineties: across the former USSR, state databases began leaking out piece by piece — passport records, address registries, registration data, telecom operator databases. Later came an enormous number of leaks from ordinary websites: shops, delivery services, forums, food delivery apps. And at some point services appeared that search all of it at once.

In this guide, “probiv” means exactly that — **the practice of looking a person up across many databases, websites and registries at the same time**. Not a single break-in, but an established industry that takes one phone number or name of yours and gathers everything that has ever leaked anywhere or sits in public view.

Do this today

Four things you can finish in an evening. The explanations come later in this chapter, but you can start with these.

1. **Look yourself up** by phone number and by email in leak-checking services. You will find out which databases you are already in — and that tells you what to fix first.
2. **Change any password you have reused.** In Russian leaks the password almost always sits right next to the login, so one exposed password opens all of your accounts at once.
3. **Turn on login codes** — two-factor authentication — everywhere it is offered. Then a stolen password alone is no longer enough.
4. **Set up a separate email address** for shops, deliveries and one-off sign-ups. Those are the databases that leak most often, so let the address that leaks be one that is not tied to your main accounts.

The rest of this chapter explains why it works this way, and what to do if your data has already leaked.

Check what has leaked about you specifically

Start by checking rather than reading: by phone, email or full name you can see which known leaks you are already in. The services for this, and the risk of each one, are covered in Finding yourself in leaks.

The key point from there: behind any online lookup there may be a wish to enrich your profile — to record the address your request came from, to link several of your searches together and work out who you are looking for. So searching the leak files themselves is safer than using someone else's website, even though it is harder.

You cannot delete your data from leaks

You can't. That is the unpleasant core fact of this chapter, and there is no way around it.

You can ask the popular services to remove your record from their search, and it is worth doing. But the database itself does not disappear: by the time a leak becomes public, dozens of people have downloaded it, it has spread to private services and closed bots, and recalling every copy is impossible. A removal request takes you out of one window, not out of the data.

There is a theoretical way to get deleted, and it is worth knowing about — if only to see who it is available to. People with high status, or those serving in the security services, get themselves removed from search results by pressuring the services that sell those results. But only people with leverage get deleted that way — and it has an awkward side effect: **the deletion itself works as a marker.** If a person shows up in one service and is missing from another, that reveals both which services clean their results and that someone came looking for that particular person. Some services make it even more obvious: instead of an empty result they state outright that the data was hidden by the user. To whoever is checking up on you, that is a finding in itself: you knew you were in such a database, and you paid to get out of it. And complete deletion still does not work: there are too many databases, and nobody can come to terms with all of them at once.

That is not a reason to do nothing — it is a reason to do something else.

What works instead of deletion

- **Work out where the leak came from.** Once you know which service gave you away, you stop feeding it new data, and you also see which of your traces are already linked together. How to find out — Determining the source of a leak.
- **Learn about the next leak before everyone else.** This is what canary tokens are for — a decoy address or a special link that lets you know the moment somebody starts looking for you. How to set them up — Canary tokens.
- **Devalue what has already leaked.** If ten plausible but false or borrowed contacts are attached to your name in the databases, the price of that record drops. Techniques — Making leaks useless.
- **Remove yourself from the services that trade in these databases.** Many of them have a removal procedure — see the summary below. How removal works at the probiv bots, and what to do if you are not ready to pay — Removing information about leaks.

Which services you can remove yourself from

Most of the larger services do have a removal procedure, but it looks very different from one to the next: a command to a bot in one place, an email to support in another, an application with a photo of your passport somewhere else, and a fee per row of your data in a few. Free routes are no rarer than paid ones, and they exist at the probiv services themselves, not just at the leak-checking ones.

The procedures and prices were collected in the autumn of 2026 and may have changed since, so treat the table as a reason to go and check rather than as a ready-made instruction. We give no addresses or links to these services: their activity falls under criminal liability in Russia. The table is reference material: it tells you whether a service has a removal procedure and what it costs, not where to look for the service. The last column answers a separate question: does the service tell the person who was looking for you that the data was hidden by you, or does it simply find nothing?

Service	How to remove yourself	Price	Hiding is visible

Service	How to remove yourself	Price	Hiding is visible
Глаз Дурова	the `/remove_me` command	free	no data
Overload	inside the bot	free	no data
VK InfoApp	in the app itself	free	no data
GetContact	hide your own tags in the app, one by one	free	no data
Leak OSINT	switch the Telegram language to a non-CIS, non-English one, remove through the bot’s menu	free	no
Avinfo	write to support	free	no data
vk.watch	a request by email	free	no data
Top100VK	a request by email	free	no data
Nebaz	a request through the feedback form	free	no data
Interesnoe	a separate removal page	free	no data
FIND HOMO	an email, the instructions are in the bot	free	yes
LeakCheck	following the instructions in their wiki	free	unknown
infotrackpeople	an application with a reason and a photo of your passport, up to 14 days	free	no data
Unamer	buy coins and run the removal command; those coins cannot be spent	400 coins	no

Service	How to remove yourself	Price	Hiding is visible
Detectiva	only Russian numbers can be hidden	1000 ₽	no data
Enigma	pay for the application and wait for review	1000 ₽	no data
TG Pulse	through the service	2000 ₽	yes, “hidden” and “not found” are different answers
Telescan	through the service	2000 ₽	no, but it notifies you when a hidden record is searched for
Funstat	partial hiding; full hiding is auctioned once a day	2500 ₽	depends on the type of hiding
Insight	hides itself once you top up the balance	3000 ₽	no
void	send the list of your data and wait for review	3000 ₽	no data
TeleSINT	buy the lifetime premium	4000 ₽	no data
Вектор	an application, wait for review	5000 ₽	no data
imsg	hides itself once you top up the balance	10,000 ₽	no
Eye of TON	through the service	150 USDT	no data
Dyxless	send the list of your data and wait for review; Russia and Belarus only	$300	yes

Service	How to remove yourself	Price	Hiding is visible
Шерлок	an application to hide, priced per row of data	$500	yes
Chat Crawler	through support	$1000	no data
Саурон	—	$2000 to enter the service	no data
Himera	the administration is against removal	—	no data

What usually leaks

It is not only logins and passwords. To show how much wider it goes, we will take one real database apart field by field, and then look at the rest.



image

This is only part of a single database — and hundreds of them have been collected across all regions of Russia.

What one row of a leak looks like

In the abstract, “personal data was leaked” does not sound frightening. So here is the actual list of fields from one database — the medical lab chain Gemotest, published on 1 May 2022:

```
name · sex · date of birth · place of birth · citizenship
passport · passport issuing authority
birth certificate · certificate issuing authority
SNILS (social security number) / INN (taxpayer number)
insurance policy number · insurance company
address · phone · email
link to a relative · customer number
record created at · record updated at
```

Stop for a second and look at what this set is. A person went in for a blood test — and a single row ended up holding their **passport**, **birth certificate**, **SNILS**, insurance policy, citizenship, place of birth, address and phone. That is enough to pass for you in a conversation with a bank or a mobile operator: these are exactly the details they ask for when verifying that you are really you.

Two of these fields deserve separate attention.

The link to a relative. Your leak automatically becomes a leak about your child or your parent, even if they never went to that lab themselves.

The created and updated timestamps. They show not only what is known about you, but when you came in — which reconstructs a timeline of your life.

And above all: this is a laboratory. Not a bank, not a government office, not a social network — a place you visit once to give blood.

Known major leaks

A few Russian databases that sit in open access. The last column shows the fields, which is where you see what actually ended up outside.

When	Source	Records	What was in the fields
July 2021	Delivery Club	1.8M	email, name, phone, address, **the network address of the computer** and **exact coordinates of the home**
2022	CDEK, two different copies	66.9M and 104.6M	email, name, phone, address, **apartment number**, **the name as registered with the tax service**, record creation time
February 2022	Yandex.Eda	~7M	names, phones, full delivery address, order comments
May 2022	Gemotest	31M	the full identity set (see the field breakdown above) **and medical test results**
2023	Rosreestr (state property register)	3.0M	name, address, phone, taxpayer number, passport
January 2025	Rosreestr	25.1M	the same plus email, date of birth, SNILS and **a link to a company**
July 2025	EMIAS, Moscow public health records	about 17 TB	patient data and internal databases

For scale: the January Rosreestr leak holds 25 million records. As of 2024, about 146 million people lived in Russia and about 13 million in Moscow. So that one database is twice the size of the entire population of Moscow.

Three of these fields are worth a closer look, because they change what counts as “personal data” in the first place.

Exact coordinates from a food delivery service. Not a text address that can be written imprecisely, but a point on the map accurate to the building entrance. Plus, in the same row, the network address of your computer — so both where you live and where you went online from.

Apartment number and the tax-registered name from a courier service. The delivery company kept not just an address but the apartment, and separately your name exactly as the tax service records it. That is no longer a contact detail for the courier, that is identification.

The link to a company at Rosreestr. A person, their passport, their property and their firm in one row. For anyone building a dossier this is the most valuable connection of all: it joins private life to business life.

Nobody knows how much has leaked in total

This is worth saying plainly, because you will meet the “how much” figure in the news many times, and it will be different every time.

Even the numbers for **one specific leak** disagree. Rosreestr, January 2025: the intruders claimed two billion rows, the news reported a published fragment of 82 million, and in the lookup services that database sits at 25 million records. An eighty-fold spread — for a single event. CDEK is similar: the news cited 19 and 25 million, while two different copies sit in open access at 67 and 105 million, labelled as “two versions of the alleged breach” — so even the fact itself is disputed.

The annual totals disagree just as much. For the same year, 2025, the state regulator counted slightly over 52 million leaked records, independent researchers put it between 145 and 767 million, and the relevant ministry announced that leaks had dropped thirteen-fold compared to the year before. The spread between the extremes is more than tenfold, and it is not anyone’s bad faith: the counting methods differ, and above all — **not every leak becomes known**.

There is one practical conclusion, and it is unwelcome: the absence of a news story about a leak at a service you use tells you nothing about whether your data leaked.

How this differs between countries

It helps to separate two different things here: how much data has leaked, and how people get access to it.

Russia against the global picture

A warning first: **different measurements give opposite answers to the question of where there is more.**

By one count Russia is first in the world in leaked accounts per person. By another the US is ahead, and by a wide margin: around 14.6 billion records against Russia’s 4.3 billion. France, which comes first in the first ranking, lands almost six times below Russia in the second.

The contradiction is not anyone’s mistake, it comes from **what exactly is being counted**. These tallies mix very different things: genuine breaches, hand-assembled password lists, the results of automated collection of public profiles, mailing lists and exports of public registries. They are not comparable in how dangerous they are, yet they all feed one counter. On top of that, it reflects the attention of whoever maintains the collection: English-language databases are gathered more actively.

Hence a conclusion that matters more than any ranking position: **“which country has more leaks” is a badly posed question.** The answer changes with the counting method. What matters for you is not your country’s rank but which specific databases holding your data sit in open access — and that is found by searching for yourself, not by reading statistics.

What is visible consistently is the structure, and it differs among neighbours. Russia and Ukraine both have finance and retail at the top, but Ukraine has **government databases** in second place and automotive ones in the top five. In Kazakhstan the top spot is shared by **government databases and education**. Belarus has the smallest collection of all, and it consists entirely of breaches.

The gap between Russia and its neighbours is enormous, but reading it as “Belarus is a thousand times safer” would be wrong: a small collection may simply mean the country has had less attention from the people who

assemble these databases.

And one figure that is more useful than any overall ranking: **in Russian leaks there are 89 stolen passwords for every 100 stolen accounts.** The password almost always sits next to the login — which is why reusing a password costs more here than it does on average worldwide.

Where these services get their data

The pile being searched has two sources.

State and corporate databases. The ones that have been leaking since the nineties, and the ones access to which is sold today — through a person with legitimate rights: an employee of an operator, a bank, a government agency. Most deals here are not technical attacks but betrayal: passport details and records from police databases go for **ten dollars a lookup and up**.

It is telling how the attempt to shut this down ended: the campaign announced in Russia against the probiv market hit the security officials who were trading in it themselves, while the sellers moved abroad and carried on from there. The availability of the data did not drop.

Leaks from ordinary websites. There are more of these by volume, and they are what gives lookup services the chains of “phone — email — username — delivery address”. One online shop’s database is harmless on its own; ten such databases joined by a shared phone number map out a decade of your life.

The country Russia resembles in how this market works is India. The same thing happens there: not a break-in, but paid access through an intermediary with legal rights. In one documented case a company officially authorised to verify citizens’ identities let an access key out, and strangers used it for two years to check other people’s documents at six cents a query — with nobody noticing.

At the same time India is nowhere near Russia in sheer volume — 562 million records against 4.3 billion. Which means **the volume of leaks and the structure of the access market are independent things**: a country can leak less and still trade access just as freely. You have to defend against each of them separately.

What this means in practice

If you are in Russia or another country with a developed probiv market, the “don’t give away your data” defence works less well: the main databases are governmental and banking, and you are required by law to give your data to them. What remains is the second approach: watch which of your traces — phone, email, username, address — are linked to each other, and avoid letting them be glued into a single dossier.

What exactly is for sale in each country, and which documents work as the key to your dossier, is covered separately:

- Russia
- Ukraine
- Belarus
- Kazakhstan

Determining the source of a leak

Finding yourself in leaks

Many sites allow you to search for yourself by phone number, email, or even full name in information leaks and leaked databases. They should be used with caution, because any online search may have an additional purpose of data enrichment. For example, **collecting your IP address**, or linking several searches by the same person to **collect information about their social circle**.

Therefore, the preferred option is always an *independent search in leak files*.

But this can be difficult: you need to find the file (or many files if you need an exhaustive search), understand its structure, and perform an effective search.

If you choose the simpler way, I recommend using the following resources, in descending order of risk:

Well-known safe sites

The most well-known is Have I Been Pwned, maintained by a well-known security researcher and providing privacy guarantees.

Others: - https://monitor.mozilla.org/

Commercial alternatives

These often provide freemium access. You can find similar sites by searching for keywords like “check” or “leak”:

- https://leakcheck.io/
- https://checkleaked.cc/

Notifications

Some of the sites listed above also provide notification by email when a new leak containing your data is detected. If you lead an active online life, this type of service is highly recommended.

Using aliases/fake email addresses

Gmail and other major email services support special characters for creating aliases of your mailbox. Mail sent to an alias will arrive at your primary address, but you will clearly see the alias it was sent to in the “Recipient” field.

For example, `soxoj@protonmail.com` is equivalent to `soxoj+gitlab@protonmail.com`:



It is **strictly recommended** to use this feature on all sites where it is supported. Thus: 1. In case of leaks or spam, you will know exactly which service the leak originated from. 2. In case of targeted information gathering using your email, information from multiple sites will be less likely to be merged into a single dossier.

Of course, leak harvesting often involves email normalization: removing alias parts and cleaning up extras. Therefore, this only reduces the risk rather than providing complete protection.

Special mention should be made of providing email addresses **for receiving receipts** for online purchases.

> According to paragraph 2 of Article 1.2 of Russian Federal Law No. 54-FZ, the receipt must be sent
> electronically if the buyer has provided their phone number or email address before the payment.

This is exploited by major Telegram bots such as Eye of God (“Глаз Бога”): they store all your payment information and **add the specified email** to the data the bot provides.

Therefore, if you do not need a receipt, provide a deliberately incorrect email address that points to the source of the leak, e.g., eyeofgod@receipt.com. Alternatively, use the aliases mentioned above, which explicitly reveal where the address was registered.

Using different names for tracking

Besides directly searching for yourself in databases, you can proactively leave “beacons” that will help you quickly identify the site or company responsible for a leak. Most commonly in everyday life, this happens with spam calls that mention your name — for example, a name you provided on a classifieds website.

Websites have different approaches to the accuracy of account names. Some require that they match passport data (e.g., VKontakte), some only verify them for financial transactions, and most do not validate at all.

You can use the tricks listed below depending on the strictness of the service rules (ToS, Terms of Service). But before using them, I strongly advise you to study what sanctions are possible if you provide an invalid name, and assess these risks for yourself.

Use names/surnames that are consonant with or begin with the same letters as the site/company name.

This way, if that name is leaked in conjunction with a phone number or email, you will know where the information came from:

- McDonald’s: *Maxim*
- VKontakte: *Vova*
- Odnoklassniki: *Oleg*

Use variations of the name in Cyrillic or Latin

First of all, this applies to the full/abbreviated form of the name:

- Alexander
- Sasha
- Sanya
- Shura

Due to differences between languages, a name can have several transliterated forms. Even banks often provide the option of choosing the correct transliteration of names. For example, the name “Anatoly” can be represented as:

- Anatoly
- Anatolii
- Anatoliy

▶ 🥷 Advanced level

Canary tokens

Canaries are very sensitive to impurities of dangerous gases in the air. Therefore, for a long time the miners took them with them to the mines: if the bird stopped singing, it meant that it became dangerous to breathe air.

A similar principle is used on the Internet. Many companies use a warrant canary: a public statement that no one is surveilling their users, so that upon receiving a court order they can *remove* this statement. Thus, the company signals to users that the absence of surveillance is no longer guaranteed.

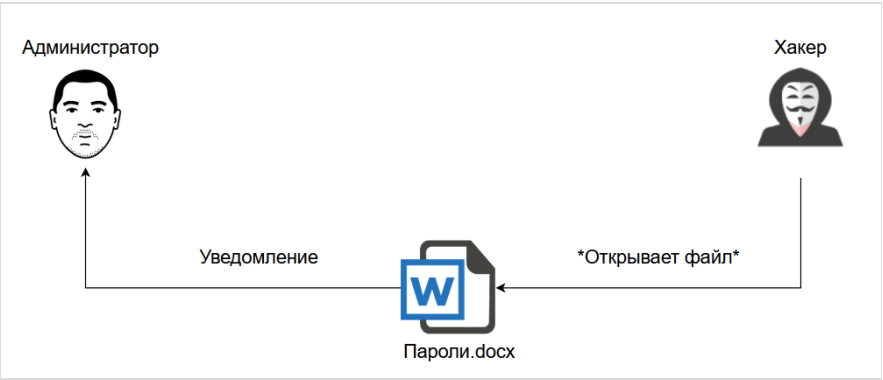
We are not going to hide from corporations, but from curious people. What can we do?

Canary tokens

You may have seen links in the biography on the VK page that lead nowhere (or lead to the application “Find out who is spying on you” or something like that). This is the simplest form of a canary.

There is a wonderful online service - Canary Tokens, which allows you to create your own canaries.

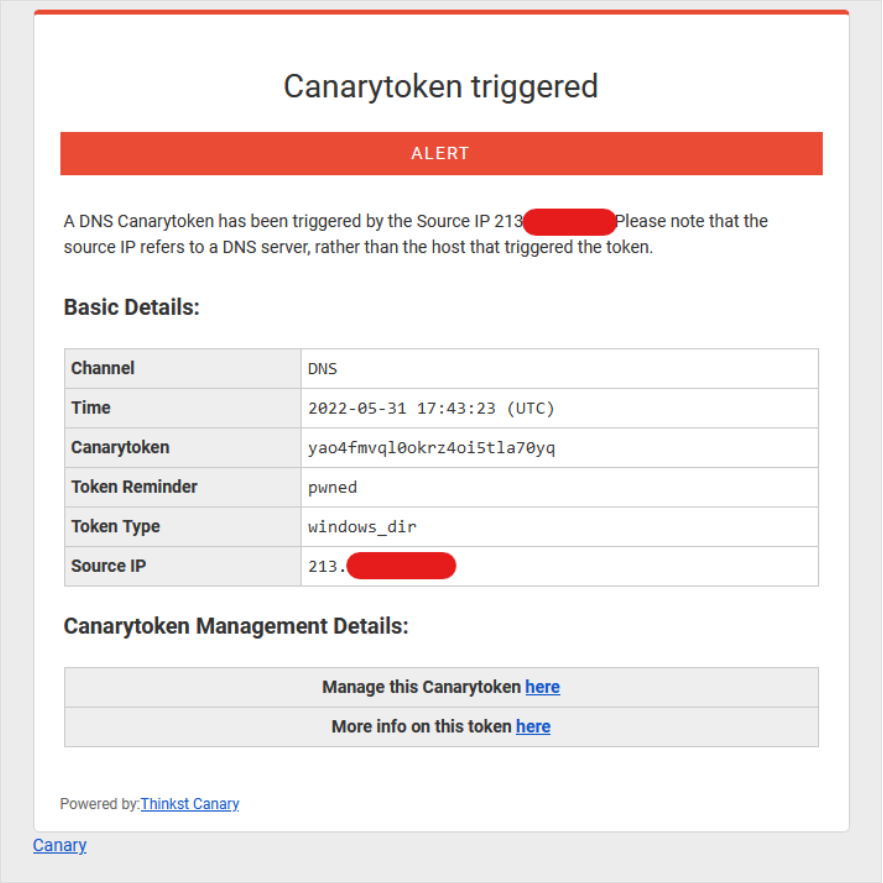
It allows you to create various kinds of canaries that we can use to detect curious employees of your organization or detect the compromise of your systems even before an attacker can perform some destructive actions.



What types can be generated and under what conditions will the notification be received: - URL token. When clicking on the link. - DNS token. When the domain name is resolved. - AWS keys. When using an AWS key. - Microsoft

Word/Excel Document. When opening the file. - Kubeconfing. When using Kubeconfig. - WireGuard VPN. When using the config. - Cloned Website. When cloning a website. - MySQL Dump. When loading a MySQL dump. - Windows Folder. When trying to open a folder. - Fast Redirect. When trying to visit the site, followed by redirection. - Slow Redirect. When trying to visit the site, followed by a slow redirect, to get more information. - Custom Image Web Bug. When viewing your picture. - Acrobat Reader PDF Document. When opening a PDF document in Adobe Reader. - Custom exe / binary. When running executable files. - SQL Server. When loading the SQL Server database. - SVN. When opening the SVN folder. - Unique email address. When sending mail to an email address.

Example of an email notification:



Difference from phishing and logger links

The section will be updated

How to make leaks useless

Is it possible to make leaks less useful when collecting information about you? Yes, although this is not guaranteed to help, it will only complicate the lives of those who collect data about you.

Let’s look at some resistance strategies that are suitable for cases when data about you has already got on the Internet.

Creating a new fake account

We create an account with identifiers that are used in active search based on data from leaks.

The section will be updated

Fake links with commonly used identifiers

Mail:

```
a@mail.ru
test@example.com
mail@mail.ru
1@ya.ru
work@mail.ru
work@bk.ru
work@list.ru
1234@mail.ru
test@test.ru
```

Phone numbers:

```
+79123456789
+79111111111
```

Sites for generating plausible data

- https://randomuser.me/
- https://www.fakenamegenerator.com/
- https://www.behindthename.com/random/

The section will be updated

Phone privacy

The topic of privacy on mobile devices deserves a separate large guide. User data is of too great financial interest for all vendors. And if there are moves towards privacy in the Western market (for example, Apple reduces the ability to collect data for all third-party applications, and Google improves access to applications with each version of Android), then in the Asian market (Samsung, Xiaomi and a lot of small vendors) user data settles in large quantities and uncontrollably.

What can be done with this in a short time and without complex manipulations like getting root or jailbreak? Unfortunately, the minimum is to keep track of which applications you install and what permissions you give them. Let’s analyze the most obvious cases.

Contacts from the phone book

Many applications have done their business only on access to the user’s phone book. The most sensational is GetContact, which has gone through a wave of Russian users. The principle is simple - a bunch of the contact’s name and phone number from your book leak to the servers, where they are combined into one database. After that, it becomes possible to find out the full name by phone number by requesting directly in the database. And sometimes a profession, and age, and anything at all. For example: “Ivan FSB”, “Alexander Client”, “Valeria Khrushchev 42”, “Masha Petrova Allegedly Model”. Now all this data can be easily obtained through Telegram bots.

Some other applications (for example, quite official ones like Sberbank) request access to the phone book in order to shorten the movements for transfers by phone number by a couple of clicks. At the same time, obviously, the contacts will be uploaded to their server anyway, and what will happen to them there is unknown.

Therefore, the first and obvious step towards privacy (both yourself and your loved ones and acquaintances) will be to restrict access to the phone book - we do not give it to applications on request, because they must

function without it (Sberbank does fine without it). Otherwise, we carefully study the application and look for alternatives if it unconditionally requires you to give your numbers.

Installed applications

Continuing the topic from the previous paragraph: applications for collecting contacts worked not only explicitly, but covertly, being introduced for money into other, free applications. Thus, a large number of inattentive people themselves merged their data, not paying attention to the fact that the next game from Google Play requests too many extensions. And few people read license agreements nowadays, alas.

Materials used and useful links

- List of alternative services and applications aimed at privacy

---

▶ 🥷 Advanced level

Privacy of social networks and messengers

This section goes through the privacy settings of several platforms, and at the end it gives the principles you can use to set up any other one.

I remind you that this guide is aimed at **hiding** your information from prying eyes on the Web. Unfortunately, almost everything you write in social networks and messengers is available to the platforms themselves. That is, a large number of employees of this company, law enforcement and other agencies that have the right to request this information, as well as sometimes a large number of other persons who semi-legally support the site's activities.

To fully protect yourself from the leakage of your personal information is not to use any platforms that do not guarantee end-to-end encryption and absolute security of your data, but there are extremely few such sites, and their prevalence among your friends and acquaintances is probably close to zero.

At the moment, let's leave aside thinking about whether or not to use big sites that earn money from you and are ready to sell your data. Let's take it as a fact that you have to use them, and let's set them up.

What this section covers

- Facebook
- Telegram
- VKontakte
- Instagram

If your platform is not here

The settings differ everywhere, but the questions worth asking are the same. Go through them in any social network, messenger or classified ads site, and you will close off most of what can be seen about you from the outside.

- **Who sees your whole profile.** Look at your own page from someone

else’s account, or from a browser window where you are not logged in: outsiders can almost always see more than you expect.

- **Who sees your list of friends and subscriptions.** People find you by it even when the profile itself is closed: a few matching names are enough.
- **Whether you can be found by phone number and by email.** This is a separate setting, and it is almost always on by default. Often your number reaches the platform not from you but from somebody else’s address book: they let the app sync their contacts, and you are already in it. **Do not sync your own contacts** — that hands the platform your whole address book and the connections between the people in it.
- **What a search for your name shows.** Check both the platform’s own search and an ordinary Google search.
- **Geotags.** Old photos and place check-ins add up to a route: home, work, gym, your child’s school.
- **Old posts.** Closing your profile today does not close what lay open for years. Many platforms can change the visibility of all past posts at once.

Facebook

Let’s discuss privacy settings in the most popular social network around the world - Facebook. As in other chapters, we remove accessibility and, if possible, set maximum levels, commenting on their purpose and associated risks.

To begin with, let’s analyze the privacy levels that Facebook allows you to set for your information and publications.

- **Available to everyone / All** - information will be seen by all Facebook users, and all Internet access will be open to search engines.
- **Friends** - only your friends will see the information.
- **Only me** - the information will be displayed only to you. *Maximum privacy!*
- **User Settings** - Flexible customizable list of who can and who can’t see the information. Both individuals and categories of “Friends” and “Friends of Friends” are available.

Also for “Friends and Subscriptions” there are additional visibility levels of “Friends other than…” and “Certain Friends”, which are variants of the latter.

Important note: The “Friends” level suggests that you can trust this group of people more, but do not underestimate the possibilities of social engineering. You can confirm the request to add a friend of a person similar to your friend without much hesitation. Which in fact will not turn out to be such, but will be added solely for the sake of obtaining your private information.

Go to the section “Settings and privacy” => “Quick privacy settings”. We open the first card “Who can see your publications” and sequentially disassemble the screens with settings.

Who can see your posts

Profile Information

- *Email address* and *Date of birth* - in fact, these data identify us, we put *Only me*.
- *Hometown* and *City of residence* - if they differ, then third parties can easily link information about you in your youth/before moving with current information. In this case, it is also recommended to put *Only me*.
- *Education* - similar to the previous paragraph (this information may be issued by your native).
- *Work* - usually does not represent a secret if it is a public work. Depends on your situation.
- *Who can see the friends list in your profile?* and *Who can see the people, Pages, and lists you subscribe to?* - information about the social graph potentially makes it possible to learn a lot about you from the above indirectly. Surely you have friends and colleagues, college classmates, and school classmates. Therefore, we also put “Only me”.

Publications and stories

- *Future posts* - determines which value will be set by default for new posts. Allows you to avoid accidentally publishing a post with incorrect privacy settings. It is recommended to set “Friends”.
- *Stories* - they are visible only 24 hours, but not only on Facebook, but also in Messenger. We do not neglect the risks of finding out information about us through another platform, so we put up “Friends”.
- *Restrict access to old publications* - **important setting**, which makes it possible to massively change the visibility settings for all old publications. Click “Restrict access” and confirm your decision.

Blocking

In this section, you can add people to the blacklist. This is not our goal right now, but if you are concerned about privacy, knowing about a specific suspicious profile, block it here.

How people can find you on Facebook

This section in the “Quick Privacy Settings” **is very important to us** - it allows you to “break the connection” between your phone and mail and account.

Friend Requests

As mentioned above, the addition can be initiated only in order to see your private data.

Phone number and email address

Both settings are set to “All”. This means that you can be found by phone number and email address via the built-in Facebook search! Of course, we put “Only me”.

Search engines

This setting is enabled by default and allows indexing of your profile. Turn it off and thereby prohibit finding our profile in search results by name Google, Yandex, etc.

Used materials and useful links

- Habr - Privacy Settings Facebook VS OSINT

Telegram

Let’s move on to the privacy settings in the messenger, which is considered one of the most private - in Telegram. As in other chapters, we remove accessibility and, if possible, set maximum levels, commenting on their purpose and associated risks.

Go to the settings, the “Privacy” section. Let’s start with the subsection of the same name.

Privacy

Telegram makes it possible to flexibly manage whitelists and blacklists for access to your data. For items in this subsection, you can hide information from everyone or show it to everyone, or use your contacts list. It is also possible to add point-by-point exceptions in the form of individual accounts or all people belonging to certain groups.

Contacts at the moment in Telegram are considered not only those accounts for which you know the phone (as it was earlier), but also accounts manually added to the contacts of the application. Therefore, you should not rely too much on the contact list in the settings - at least, there may already be extraneous numbers in your phone book, and it is easy to add contacts inside the application by mistake. Therefore, it is recommended to make an audit of the phone book or not share access to it at all. For more information, see the section accesses for mobile applications.

Phone number

We set the option “Who sees my phone number” to “Nobody”, otherwise any Telegram account in any chat will be able to see your phone number.

We also see that there is an option “Who can find me by number”. This is one of Telegram’s most valuable privacy settings. It was added solely because of the mass protests in Hong Kong and the discontent of the protesters because of the ease with which the police could disclose their numbers.

Unfortunately, so far this option has no “Nobody” value. We put this option

in “My contacts”, and now only accounts from your contacts will be able to add you by phone number. At the same time, we remember the limited trust in the contact group (see above).

Last activity

There is a feature in the platform - restrictions on the time of the last activity (was N minutes ago on the network) act in two directions. We set the value to “Nobody”, but remember that at the same time you will not be able to see the activity of other accounts. Fortunately, specific people can be added to exceptions if necessary and removed after verification.

Groups and channels

Permission to add you to groups and channels has a limitation - you can’t ban everyone, but you can only allow your contacts. There are also separate point bans for the option.

We set the option to “My contacts”. At the same time, we remember the limited trust in the contact group (see above).

Calls

Anti-spam in Telegram works well, so calls from spammers are quite rare. Also, fortunately, the call itself does not disclose any information about you if Peer-to-peer mode is not enabled. In this mode, Telegram establishes a direct connection from your device to the interlocutor’s device, and it becomes possible to determine the IP address.

We set “Who can call me” to “My contacts” if you are ready to manually add accounts to contacts and monitor their “cleanliness”. We set the “Peer To Peer” option to “Nobody”.

Profile Picture

When this option is enabled, other accounts lose the ability to see your avatar. This rather useful option is also limited by the access level of contacts, but can also be enabled manually for specific accounts.

We set the option to “My contacts”. At the same time, we remember the limited trust in the contact group (see above).

Forwarding messages

From a certain version, Telegram learned to remove the link to the author for forwarded (forward) messages. Thus, even if your message is copied to another chat, it will be impossible to access your profile through it. Previously, this allowed tracking accounts that left at least one message in any chat.

We set the option “Who can link to my account when forwarding messages” to the value “Nobody”.

VKontakte

The section will be updated

Settings

General

The “Profile Settings” block. Turn on the “Hide gift block” option.

Privacy

For **all settings** in the lists below, we first set “Only me”, if necessary, add people through the options “Only friends”, Some friends” or “All friends except…”.

My page

- Who sees the basic information of my page
- Who sees my saved photos
- Who sees the list of my groups
- Who sees the list of my audio recordings
- Who sees the list of my gifts
- Who sees my hidden friends

In the “Who is visible in the list of my friends and subscriptions” block, select all friends and all subscriptions.

Entries on the page

- Who sees other people’s posts on my page
- Who can leave entries on my page
- Who sees comments on posts
- Who can comment on my records

Photos

- Who can tag me in photos
- Who sees the photos in which I was marked
- Who sees the location of my photos

Go to the control panel “Marks on the photo” and remove all the ticks: - Recognize me in the photo. VKontakte algorithms will offer you photos, where you can mark yourself - Show your friends recognized photos with me. Friends will see photos of you in the feed and will be able to tag you. Only you can confirm the mark. - Recognize friends in my photos. Algorithms will prompt you to tag friends in your photos - Show the block “Is that you in the photo?” in the feed. A block will appear in the feed where you can confirm or delete the mark - Show the block “Is this a friend in the photo?” in the feed. Artificial intelligence will find your friends in the photos and offer to mark them

Contact me

“With whom to establish a direct connection in calls” - select “Friends only”

“Who can find my profile when importing contacts” - select “Nobody”

“What is visible instead of my photo when importing contacts” - select “Picture with a letter”

Stories

- Who can see my stories
- Who can answer my stories with stories
- Who can send opinions to my stories
- Who can see congratulations for me in the stories

Other

“Who can see my page on the Internet” - select “VKontakte users only”

“What updates do my friends see in the news” - we remove all marks

“Profile type” - “Closed”

“Who sees the number of my steps in VKontakte Steps” - choose “Only me”

“Who can see my activity in games” - choose “Nobody”

“Who can see my activity in mini-apps” - select “Nobody”

Application Settings

The section will be updated

Instagram

The section will be updated

Privacy for developers

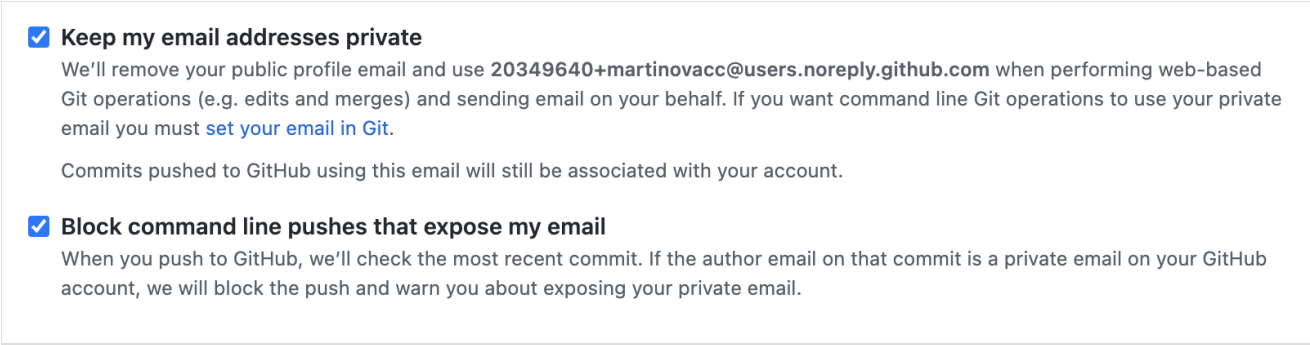
Exposing your email address

When working with program code and version control systems such as git, there is a risk of exposing your personal email address. This often happens when working with personal/work projects on the same device at the same time.

To avoid this, check the correctness of global settings or settings in the directory of a specific repository:

```
git config --global user.name
git config --global user.email
```

GitHub provides the ability to hide your email from the interface and block the “leak” of the main email address linked to the account:



Email Privacy Settings in GitHub

This section will be updated

Linking a phone to an account is not always a good idea

Do not use confirmation via phone number where it is not necessary.

2FA is used to enhance security. Use an additional factor to log in to the site when you realize that an account on a particular site is important to you (correspondence, purchases, finances), and that you will consciously confirm the login every time.

However, if there is a choice of what exactly to use for confirmation - a phone number or *something else* - then use something else. Companies are interested in knowing your number: sending you SMS, verifying your identity, linking it with other sites. Just as easily, they will give out part of your number when trying to log in to your account or when your friend gives the app access to their contacts.

It’s also a bad idea to link someone else’s phone. For example, linking your grandmother’s phone to your Google account because Google for some reason required you to add a phone. Knowing your account, it will be possible to get part of your grandmother’s phone number through, for example, access recovery.

Where are information leaks about your accounts possible at all?

- Login form. For example, the service may respond with the messages “a user with such an email does not exist” and “you entered the wrong password”, which clearly confirms the presence of an account with your mailbox.
- Registration form. The site will not allow you to register an account for a phone that is already in the system: “this phone is already in use.” And if it’s not there, then a notification will most likely be sent to the phone.
- Access recovery form. Most often, some data is entered, for example, the account nickname, and the service responds with something like `A new password has been sent to iva*****ov@mail.com` or `We sent an SMS to a number`

`ending in 93`. Or asks you to enter an email, and then writes “if such an account exists, then we have sent a notification.” And Meta (Facebook) only needs to know the account ID.

In all these places, there may be a leak of the second factor (phone number) that you link to your account.

Removing information about yourself

Deleting your own accounts

Before deleting, find what to delete. A single username usually turns up more accounts than you remember yourself: old forums, services you signed up for once, sites that registered you automatically through your email. For a quick self-check there is the Maigret bot — it looks up accounts by username across thousands of sites, with nothing to install.

Despite the fact that the Internet remembers everything, deleting accounts remains one of the strongest means against basic intelligence on you. It seems that this is a trivial topic, but there are several important nuances:

Before deleting: 1. Request the service to **export your personal data** under GDPR. This will help in the next steps and give you an understanding of what the service knows about you. 2. **Rename your account**, delete/change photos, wait a few days. This is necessary so that indexer sites and search engines have time to update the information about your account, and subsequently you cannot be found by its latest copy. Also, do not forget that from now on you cannot leave any comments and messages publicly. 3. All old comments/tweets/messages **should preferably be deleted**. There are mechanisms in social networks and messengers that allow others to reach you even after deletion: mentions (a link to your profile that looks like a name), authorship marks, reposts/retweets. It’s worth getting rid of all such leads. 4. Update the search results by asking them to reindex your **modified page** (Google) and wait for a while so that other systems that save information from social networks will also receive a new version of your account.

After that, the account can be deleted using the platform’s built-in tools.

Deletion request

Not all services allow deletion through regular means. Or it is hidden so deep that it is impossible to find. Fortunately, there are auxiliary sites with information on how to delete your account.

- JustDeleteMe - an excellent directory for platforms, gives links and a description of the necessary actions, shows the complexity of removal. The creators also have related sites JustGetMyData and JustWhatsTheData to fulfill paragraph 1 above.
- AccountKiller - removal instructions for a large number of sites, mainly Western.

Even if you couldn’t find the removal instructions for the site you need, don’t despair. There is always the option to write to support and request the deletion of your account under GDPR.

Deleting search results in search engines

Google offers a number of different forms through which you can request the removal and updating of content in search results.

- Removing outdated content from search - well suited for pages that need to be reindexed (see above point 4 about deleting accounts).
- Google Personal Data Deletion Request Form
- New request form for deletion of personal data

Removing information about leaks

Brief instructions for deleting your data from popular services - Have I Been Pwned, Leakcheck, IntelX, etc.

To make requests to services that are interested in storing your data, you need to prepare a complete list of all the information that you want to clean up. It should include: - nicknames - phones - emails - addresses - car license plates - government identifiers (passport number, social security number, taxpayer identification number, full name, etc.) - any data from leaked database records

Removing yourself from people-search bots

Earlier this guide contained step-by-step instructions for deleting your data from specific Telegram bots — with their addresses and the items in their menus. We no longer give those: the activity of such services falls under criminal liability in Russia. What is useful is something else — how the removal procedure itself works, and that is below.

On 9 December 2024 article 272.1 of the Russian Criminal Code came into force — it criminalises the unlawful collection, storage, use and transfer of personal data, and, separately, the creation and maintenance of resources that distribute it. Telegram began deleting such bots, and the services began changing addresses and disappearing from search.

In late February 2025 Eye of God, the best known service of this kind, suspended its work: its creator explained that he was waiting for the legal situation to become clear. But the industry did not end there: services of this kind are still running, and most of them do have a removal procedure — a summary of them is on the page about leaks.

How to remove yourself where it is still possible

If you have found out that someone is searching for data on you, try to obtain the bot’s message itself or its report: the report leads you both to the service’s website and to the Telegram bot. Then look inside for the option to delete your own data — it hides in a section like “Account” or “Profile”, and sometimes it is not there at all and the only way left is to write to support.

A free procedure is not a rarity: at some services it is simply a command to the bot or an email to support.

But **removal often does cost money**, and the price reaches hundreds of dollars for a single row of your data. The wording one of the large services uses to explain this is worth reading in full:

> *The service is expensive, because hiding data is an exception to the principle of free access to information. When privacy is a luxury.*
>
> *We are obliged to provide the option — and we have provided it. We are not obliged to make it affordable — and we have not.*

In other words, the removal mechanism exists in order to fulfil an obligation, and the price is set so that nobody uses it.

It happens more gently, but still not for free: another bot lets you hide only the country your account is registered in, and only with a paid subscription that also includes bulk searches and higher limits.

What to do if you are not ready to pay

The legal lever appeared together with that same article 272.1: the activity of such services falls directly under criminal liability, and you can demand that the processing stop and the data be deleted by filing a complaint with Roskomnadzor — through its electronic reception or the public services portal.

But the lever has an unpleasant property, and it is better to know about it in advance: **the complaint has to name the operator** — who exactly processes your data. And the surviving services are anonymous, so there is nothing to name.

So the realistic order is this: remove yourself where the procedure exists and is free — that happens at the people-search services themselves, at the leak-checking ones, and at operators like GetContact below. For the rest, assume the data has already spread, and work with the original source — the leaks these bots are built from.

Disabling search for your number in GetContact

In GetContact, it is possible to disable the display of names known by your number at will, or disable the search entirely.

To do this, follow this link and log in via messenger, then turn it off.

It should also be noted that in this section of the site you can track search queries by your number. If you disable the search, this feature is lost, as well as receiving notifications about searches for you from the app. However, when you log in to the GetContact application again, this feature is restored.

Visibility Settings

Visibility settings

You don’t want to appear in search results? We would like to share with you some tips that may affect your decision.

By unlisting from search results, you won't be able to do the following:

* Enterprises, banks or similar business corporations and individuals may want to see the person they do business with in Getcontact in order to know them better. Not being visible in Getcontact may result in worries in such cases.

* You won’t be notified when your phone number is searched by other Getcontact users.

*You will not be able to see the tags other Getcontact users will create for you in the future.

Search visibility: On

Are you sure you want to unlist from search results?

Please note that it can take up to 3 hours before changes take effect and your phone number will be visible again in search results when you start to use Getcontact with the same number.

No Yes

Screen sharing

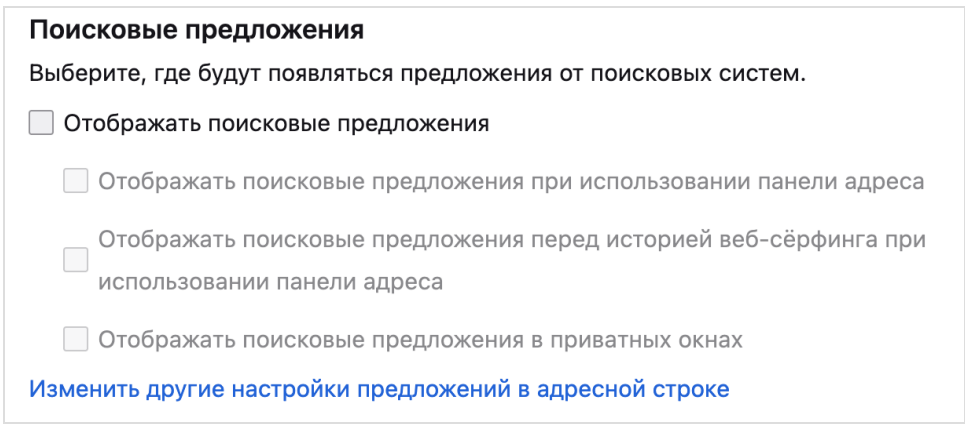
During the post-COVID, remote work became the norm. A lot of people call up with colleagues in specially designed applications for this: Zoom, Microsoft Teams, Google Meet, and so on. One of the essential attributes of such applications is the function of showing your screen: to show the interlocutor something, you make your desktop or individual windows visible, for example, the browser.

Of course, this carries with it the risks of disclosure of sensitive information. Let’s leave aside the fact that you purposefully show something, consider only random consequences:

- Correspondence and messages in messengers and social networks (in pop-up windows)
- Open browser tabs or bookmarks
- Auto-completion hints in all input windows (especially in the browser address bar)

The latter category may carry the greatest risk: when you enter a symbol by symbol, the browser will try to offer you something from the history of a recent visit, search queries or bookmarks that has at least some overlap with the characters (even if they are similar letters anywhere).

To disable this behavior, you can uncheck all the boxes in the Firefox sections “Search / Search Suggestions” and “Privacy and Protection / Address Bar”.




Панель адреса
При использовании панели адреса предлагать ссылки
из журнала посещений
из закладок
из открытых вкладок
из ярлыков
из поисковых систем

Russia

Everyone in Russia has a passport, a SNILS and an INN. Any of these numbers works as a key: it is used to link data about you held by different government agencies, and sometimes to restore access to an account. Below are those identifiers, the services that obtain data unofficially, and the leaks that affected Russians; read it not as a reference but as a list of what is better not to give away without need.

Documents

All the identifiers listed below can be used to find the owner.

Individuals

- **Passport number**
- **SNILS** - *insurance number of an individual personal account*
- **INN** - *taxpayer identification number*
- UIN – *unique identifier of accruals*

Legal entities

- OGRN - *main state registration number*

Transport

- Car number
- OSAGO policy number - *compulsory civil liability insurance*
- STS number - *Vehicle registration certificate*
- VU - *driver’s license*

The main government service is Gosuslugi. Access there can be restored through any of the first three documents of an individual, while revealing part of your mobile phone or mail. It is not recommended to enter SNILS or INN into your personal account without an explicit need.

Probiv (unauthorized data lookup)

What services for obtaining data through employees are available in Russia?

- Data from mobile operators: Beeline, Megafon, MTS. Call details, location (the so-called “Flash”).
- PFR (*Pension Fund of Russia*). SNILS, statement from the personal account of the insured person (SZI-6), date of death, current place of work, maternity capital.
- MVD (*Ministry of Internal Affairs*). Databases IBD-R, IBD-F, Rospasport, Stream, Migrant, Highway, Frontier.
- GIBDD (department of the Ministry of Internal Affairs). Cards, fines, restrictions, list of cars, vehicle cards (vehicles), VU.
- FNS (*Federal Tax Service*). SNILS, accounts, EGRN, EGRUL, 2NDFL, purchase and sale books, archive extract, declaration, affiliation, insurance premiums, debts.

Data leaks to public access

In December 2021, there was a leak of the program code of the regional website Public services. The federal website has not been affected, but there is a possibility of data leakage from it.

In February 2022, there was a leak of the Yandex.Food delivery database. The names and surnames of the clients, telephone numbers, the full delivery address of the client and comments on the order were published. There are almost 7 million unique numbers from Russia and Kazakhstan, dates from 06/19/2021 to 02/04/2022. To check their data, enthusiasts have raised the service https://saverudata.info/.

Other leaks

- FOMS - *compulsory medical insurance fund*
- UFMS
- PFR
- SNILS of citizens

What to do

Keep a separate number for deliveries, classified ads and sign-ups. Every database in the list above has a phone number in every row — and the number is exactly what such databases are joined by. A separate number does not make you anonymous: it is registered to your passport too. What it does is keep your orders and ads from being glued to your bank and government accounts through one shared field. More on this — phone number.

What the “flash” (“вспышка”) from the list above is. It is a one-off answer to where a phone was, based on its last activity on the network: not a route and not a point on a map, but an approximate radius, and only while the phone is online. It is sold not on the darknet but openly: detective agencies advertise it as an ordinary search service, next to call records. There is no hacking of your phone involved — the data comes from the operator’s side, and shop employees are convicted for selling such printouts under articles 138 and 183 of the Russian Criminal Code. Your phone’s settings do not protect you from such a purchase, so assume that your movements and your list of calls can be bought.

Ukraine

Ukrainian documents and some of the government services are gathered in the Diia app, so access to it is access to everything kept there. Below are the numbers you can be found by — passport, IPN, driving licence — and the leaks that affected Ukrainians. Check whether you are handing these numbers out where they are not needed.

Documents

All the identifiers listed below can be used to find the owner.

Individuals

- **Passport number**
- DRFO - *identification number of an individual*
- RNOCPP (IPN) - *registration number of the taxpayer's registration card*
- VU - *driver's license*

Government services: - Diya - electronic public services portal

Legal entities

- EDRPOU - number in the Unified State Register of Enterprises and Organizations of Ukraine

Probiv (unauthorized data lookup)

This section will be updated

Data leaks to public access

In January 2022, information appeared about a leak in the database of the Diya service. Despite the assurances of the authorities that the leak was fake, enthusiasts confirmed its origin.

To find out whether your data is in this leak or in any other, use the methods from "Check what has leaked about you specifically".

Belarus

Belarus has few public registries, but its state databases — the passport system, the traffic police, the Ministry of Internal Affairs — have already ended up in outsiders' hands after hacks. Below are the numbers you can be found by and the leaks that are known about. Assume that this data about you is no longer a secret, and do not use it as security answers when recovering access to your accounts.

Documents

All the identifiers listed below can be used to search for a person.

Individuals

- UNP - *Payer's Registration Number*

Probiv (unauthorized data lookup)

The section will be updated

Public data breaches

In 2021, hackers claimed access to AIS "GAI-Center", AIS "Passport", to the USB database and "Riots" of the Ministry of Internal Affairs of Belarus, as well as about hacking the database of employees of the IC of Belarus. Only some data were publicly available, but journalists were also given the opportunity to check the personal data of specific people and analyze the array of personal data of 1.4 million deceased residents.

In February 2022, the Yandex.Food delivery database was leaked. The names and surnames of customers, phone numbers, the full address of the customer's delivery and comments on the order were published.

A total of 206 thousand unique numbers from Belarus, dates from 06/19/2021 to 02/04/2022. To check their data, enthusiasts have raised the service https://saverudata.info/.

Kazakhstan

In Kazakhstan the IIN is asked for almost everywhere — in government services, in banks, in shops — so a single number makes data about you from different places easy to join up. Below are the numbers you can be found by and the leaks that affected Kazakhstanis. The less often your IIN goes where it is not mandatory, the fewer such joins are possible.

Documents

All the identifiers listed below can be used to find the owner.

Individuals

- INN - *individual identification number*
- RNN - *registration number of the taxpayer*

Juridical persons

- BIN - *business identification number*

Transport

- GRNZ - *vehicle registration plate*
- SRTS - *vehicle registration certificate*

Main public service - Electronic Government of the Republic of Kazakhstan.

Probiv (unauthorized data lookup)

The section will be updated

Public data breaches

In the summer of 2019 , during the presidential elections , there was leak personal data of 11 million Kazakhstanis from the CEC (Central Election Commission).

In February 2022, there was a leak of the Yandex.Food delivery database. The names and surnames of the clients, telephone numbers, the full delivery

address of the client and comments on the order were published. There are almost 7 million unique numbers from Russia and Kazakhstan, dates from 06/19/2021 to 02/04/2022. To check their data, enthusiasts have raised the service https://saverudata.info/.

Identification Documents in Brazil: What They Are and Their Purpose

Brazil, with a population of over 210 million people distributed across 26 states and a federal district, uses various identification documents to ensure the identification and exercise of the rights and duties of citizens and businesses. These documents vary in terms of their purpose, scope, and validity.

CPF — Individual Taxpayer Identification Number

The CPF is a crucial document for identification with the Federal Revenue Service of Brazil, the agency responsible for administering federal taxes. It consists of 11 digits, including two verification digits. The CPF is mandatory for all Brazilians and foreign residents in the country and is required for a wide range of financial operations, such as opening bank accounts, applying for credit, and filing income tax returns.

Furthermore, the CPF is essential for access to social programs, such as Bolsa Família, and for participation in public examinations, selection processes, and enrollment in educational institutions. The CPF number can also be printed on the identity card or national driver’s license.

RG — General Registry

The RG is an identification document issued by state public security agencies. It consists of a sequential number followed by the acronym of the issuing state. The RG contains information such as name, date of birth, parentage, photo, signature, and the bearer’s fingerprint. In addition to serving as an identification document, the RG is valid throughout the national territory and can be used as a travel document in Mercosur countries.

It is important to note that the RG is often required in situations such as opening bank accounts, obtaining official documents, and participating in public examinations. Obtaining an RG is also linked to the mandatory military enlistment for men over 18 years of age.

CNPJ — National Registry of Legal Entities

The CNPJ is a document that identifies a company with the Federal Revenue Service of Brazil. It consists of 14 digits, including two verification digits. The CNPJ contains information such as the corporate name, trade name, address, economic activity, and share capital.

For companies, the CNPJ is essential as it is required for conducting commercial activities, issuing invoices, hiring employees, and complying with tax obligations. Additionally, it is used for obtaining credit, opening business bank accounts, and participating in public bids. The CNPJ number can also be printed on the business operating permit or the Simples Nacional card.

RENAVAM — National Registry of Motor Vehicles

The RENAVAM is a document that identifies a vehicle with the National Department of Transit (Denatran), the agency responsible for coordinating state transit authorities. It consists of 11 digits and contains information such as make, model, year, color, license plate, and chassis number.

In addition to being mandatory for all vehicles in circulation, the RENAVAM is essential for vehicle transfers, payment of vehicle-related fees and taxes, obtaining annual licensing, and performing services such as property transfer and change of municipality.

The RENAVAM number can also be found on the Vehicle Registration and Licensing Certificate (CRLV) or on the Denatran portal.

CRV — Vehicle Registration Certificate

The CRV is a document that proves vehicle ownership with the state’s Department of Motor Vehicles (Detran) where the owner resides. It contains the same information as the RENAVAM and also serves as a document for transferring vehicle ownership.

In addition to the functions mentioned above, the CRV is essential for the sale or purchase of used vehicles, as it formalizes the transfer of ownership, ensuring that the transaction is registered and legalized. Therefore, it is

important to keep it in a safe place and not carry it with the vehicle.

Data Breaches: A Threat to Privacy and Security

Concerns about data security are of global significance, and Brazil is not immune to incidents of sensitive information leaks that can have significant impacts on the privacy and security of its citizens.

Mega Data Leak of CPFs: Two Years Later, Questions Remain Unanswered

In January 2021, the largest data leak in Brazil's history occurred. Approximately 223 million Brazilian CPFs were made available for free on an internet forum, with a hacker selling information related to these individuals, including address, phone number, email, credit score, salary, income, and much more.

There is no tool available to check if your data is included in the file, and it is likely that such a tool will not be developed. The Supreme Federal Court (STF) ordered the removal of the "Fui Vazado" website, which allowed checking by CPF to see what types of data were present in the mega leak.

Measures to Enhance Online Security

Protecting your personal data on the internet is crucial to prevent fraud, identity theft, and other issues. Here are some measures you can take to enhance your online security:

- **Manage your passwords:** Use strong, unique, and hard-to-guess passwords for each service you use. Change passwords periodically and do not share them with anyone. Consider using a password manager to store and generate secure passwords.
- **Avoid sharing sensitive information on social media:** Refrain from disclosing data such as address, phone number, CPF, RG, income, location, and daily routine. This information can be exploited by criminals to impersonate you or track your movements. Adjust the privacy settings on your social networks.

- **Recognize and avoid scams:** Avoid clicking on suspicious links, opening unknown attachments, and providing personal data on untrustworthy websites or in emails. Many scams use phishing techniques to deceive you and obtain your data or install malware on your device. Use antivirus software and a firewall to strengthen your protection against threats.
- **Exercise caution in online shopping:** Make purchases only on trusted websites and verify that they use the HTTPS protocol, indicating a secure connection. Avoid using credit or debit cards on unknown or suspicious websites; opt for virtual cards or online payment services to protect your banking data.
- **Be wary of public networks:** Avoid using public Wi-Fi networks or shared computers to access services that require your personal data, such as email, banking, and social networks. These networks may be monitored by attackers or contain malware. If you must use a public network, consider using a VPN to encrypt your traffic.

Protecting and being aware of data security is fundamental in the digital age, where personal information is increasingly interconnected with our daily lives. By adopting proactive online security measures, you contribute to safeguarding your privacy and preventing potential cyber threats.

About this edition

The book is built automatically from the source text of the guide, which lives in an open repository. Content and typos are fixed there.

Edition of 17.11.2026.

The current version and other formats: counter-osint.soxoj.com/en/pdf

If you are reading an outdated copy, the latest one is always at that address.