What to Do If Your Ex Is Stalking You With Technology

How your ex can track you, hack you, or just generally mess with your life... and what you can do about it!

By Linus Nyman & Laura Kankaala
Disobey Outreach

Disobey Outreach is a non-profit organization with a focus on helping at-risk individuals and groups with their digital privacy and security. One of our primary focus points is on helping victims of digital stalking or abuse by a current or former partner.

Disobey Outreach is an off-shoot of the annual Nordic security event Disobey. As a community and as an event, Disobey, held annually in Finland, seeks to foster a vibrant community of creators, makers, and breakers.

Linus Nyman (PhD) is a researcher with a fascination for privacy, security, and pretty much all things IT. He has spent many years in academia, both researching and developing and teaching courses at university. Linus enjoys trying to make learning fun (or at least not entirely painful).

Laura Kankaala is a security professional with a background in hands-on security. She has worked in a variety of security-related professions and fields, both on offence and defence. Her mission is to make information security knowledge available and understandable for everyone.

This guide was written using the open source software LibreOffice by The Document Foundation.

Contents

1. Who is this guide for?

If you believe your ex (or soon-to-be ex) might stalk you, hack your accounts, or otherwise use technology to harass you, then this guide is for you.

There are different ways your ex can use technology to mess with your life or keep track of you without your knowing about it. And the risks are greater if your ex has, or has had, physical access to your phone, computer, car, or home. Or if you have ever shared any of your online account passwords with them. Or if you use passwords or security questions that may be easy to guess. The list goes on (and on and on), but you get the picture: there are quite a few potential risks. In this guide, we will go over many of the ways in which technology can be used to stalk you or mess with your life – and what you can do about it.

If you aren't very tech-savvy, the topics might seem a bit daunting or even scary, at least at first glance. It can feel like there is too much to learn and that what will happen will happen anyway. As one member of a support group for victims of domestic violence once put it, "If my ex wants to hack my Facebook, he will." But the situation is not that grim. And that's a big part of why we wrote this guide: to show that there are simple steps you can take to reduce the risk and impact of this type of harassment. You don't need to be a technology wizard, and the basics aren't that hard to learn.

What we cover in this guide are the most common things someone might do to harass their ex with the help of technology. And we assume this person has moderate technical knowledge and will do things that either require no tools or just easily accessible ones. But we do have a section at the end that covers the situation where an ex is particularly tech savvy.

What do not cover is a situation where your ex has access to government, military, or police tools or databases or other high-end equipment. We also do not cover things that can't be solved by increasing your knowledge of security, such as revenge porn or your ex posting bad things about you online. For these situations, we recommend you seek further advice.

This guide does not cover what to do if there is a risk of physical violence. We are not psychologists or police officers – we can only offer advice regarding technology. Please contact a support group or the police if you fear violence. There are also shelters you can go to to escape a bad situation at home. We will not cover these topics, but the websites and phone numbers of support groups, shelters, and the police for your area can be found online.

Note: Please access the internet *securely* when searching for shelters, support groups, or any other similar topic online. We will cover how you can use the internet anonymously in section 7 of the guide.

Where is your digital life vulnerable?

For your ex to be able to access, for instance, one of your social media accounts, they can't just upload Evil Fairy Dust to the internet and magically gain access to your account. They need to find a vulnerability in your account's security – a way in.

You can compare account security to the security of a home: if there is a door or a window left open or unlocked, then that is a vulnerability in the security of the home. Similarly, in the example of your social media accounts, there needs to be a vulnerability that your ex can use – a virtual equivalent of an unlocked door or a key hidden under the doormat.

Generally speaking, you can find vulnerabilities in two places: the programs and the people. Just like a weak lock on a house door, a program might be vulnerable because of how it was designed. And, just like a person might be tricked into letting someone into their house, we as users create vulnerabilities through our actions and decisions.

In this guide, we will focus on the second type: vulnerabilities that result from our choices and actions. And the good news is that these vulnerabilities are often quite easy to fix. For example, your ex hacking one of your social media accounts is likely to be something as simple as them managing to guess your password. And weak passwords are a common vulnerability that you can sort out in minutes! (We'll show you how in section 2.)

But, an unfortunate side effect of making something more secure is that it usually also makes it less convenient to use. You need to keep this trade-off in mind when securing your digital life. The goal is to achieve a kind of sweet spot of having enough security without adding unnecessary inconvenience. In this guide, we go a bit beyond the steps people usually take to protect themselves but we have still tried to find a good balance with convenience. And we will focus on helping you take action in the areas where a little more security can make a big difference.

Common ways an ex can mess with your digital life

This guide will cover common ways an ex can mess with your digital life, focusing on four main categories: your online accounts, your smart devices, software designed for spying, and hardware designed for spying. Each of these topics has their own section in this guide, but first we'll cover them in brief.

Online accounts

Without ever investing a single penny in spy gear, your ex could try to gain access to your online accounts. Online accounts are basically anything you log into online. This includes things like your email, bank, and social media accounts, but also various services like calendars, "find my phone" applications, cloud storage services, and broader services like Google that (among other things) can track and keep a log of your location over time.

Your ex can use most if not all such accounts and services against you should they manage to get hold of your login information. This includes things like reading (or deleting) your emails, knowing who you are meeting and when, accessing (or deleting) your pictures, seeing a list of locations you have visited or people you have been in touch with, and knowing what search words you have entered into Google or what YouTube videos you have watched.

Online accounts, and how to secure them, are covered in section 2.

Smart devices

By smart devices, we mean internet-connected devices (as in the phenomenon called the "Internet of Things" or its abbreviation: IoT). All this really means is that the product has an internet-connected computer in it. It's hard to think of a product that now doesn't have a smart version. There are smart toilets, washing machines, security cameras, baby monitors, water bottles, underwear, mousetraps, etc. If you can think of it, someone has connected it to the internet.

Some of these products can be used for stalking, especially security cameras. However, even the smart products that can't easily be used to track you can still be meddled with just to mess with you and generally make your life miserable. For instance, if they get access, someone can remotely adjust the settings on your lights, thermostat, or other smart products in your home.

Smart, internet-connected devices, and how to secure them, are covered in section 3.

Spy software

The term software basically just means the programs and apps you use on your phone, tablet, or computer. In this guide we will focus on a group of spying software known as stalkerware, spyware, or spouseware. This software allows a stalker remote access to your phone, tablet, or computer, letting them see a wide range of things, like who you are in contact with and where you are physically located at any given time. These also sometimes come in the guise of being apps for parents to monitor the activities of their children, but they can be used in other ways.

Malicious software and apps designed to stalk you, as well as how to secure your devices, are covered in section 4.

Spy hardware

Hardware refers to a physical thing. Your phone is hardware; the apps on your phone are software. The kinds of spying hardware we will focus on in this guide are GPS trackers as well as hidden video cameras and microphones. We will go through some examples of available products, what they are capable of, and what you can do to try and detect them.

Spy hardware, and how to detect it, is covered in section 5.

Some special cases

The topics mentioned so far cover a host of basic threats. However, there are some situations that warrant special mention:

If your ex is unusually tech-savvy, this in no way makes your situation hopeless – you just need to be aware of some additional risks. This is covered in section 6.

If you are still living with them, then it is good to be aware of some additional ways they can spy on you, as well as how you can cover your tracks online and even use a computer without leaving a trace. This is covered in section 7.

2. Online accounts

Your online accounts are likely to be the easiest targets and the most vulnerable parts of your digital life. That's the bad news. The good news is that it is possible (and not even that difficult) to make your online accounts very secure.

To help you do this, the key security-related things we will cover in this guide are: passwords, security questions, and two-factor authentication. We will also briefly cover account privacy settings and how to avoid accidentally over-sharing information.

Passwords

You may have heard talk about the importance of a "strong" password, but what the heck does that even mean? A strong password is impossible (or at least absurdly difficult) for someone else to guess.

Here are some of the usual ways of guessing a password:

- ***Trying commonly used passwords***

  Unfortunately, we sometimes get a bit lazy when coming up with passwords, choosing something like "password" or some combination of letters of numbers that is easy to remember and type, like "123456". But these passwords are too basic and well known. Online, there are lists of the most commonly used passwords, which your ex can try on your accounts. So, passwords like "letmein" and "qwerty123" definitely would be called "weak" passwords, and they are really only useful if you want to keep your goldfish from accessing your accounts while you're out.

  So, you want to *avoid commonly used passwords.*

- ***Using what they know about you***

  Another approach your ex can take to guessing your password is to try things they know to be of personal significance to you. This is particularly important in a situation where your stalker knows you personally, but is also relevant regarding any information you may have shared on social media.

  So things like your cat's name, your name and date of birth, your favourite author or movie, and so on – these are all weak things to use as a password because they are easy (or at least far from absurdly difficult) to guess.

So, you want to *avoid personal information in your passwords.*

- ***Trying* all *the passwords***

  Although rare, the scariest approach someone can take to guessing your password is something called a "brute force" approach. A brute force approach basically means that you keep trying passwords until you happen upon the correct one. So, first they would try "a", if that doesn't work then they try "b", and so forth until they have tried every possible combination of every existing character.

  A single person trying all possible passwords by typing them in, one by one, would simply take way too long, even if your password is relatively short. There are computer programs that can automate this process, but they also have their limitations. Online service providers have added protections against automated programs, like freezing your account for several minutes after a certain number of failed attempts. And you'll have seen those "prove you are a human" challenges where you have to type in what you see in a box of blurry or squiggly letters and numbers.

  The situation where a brute force attack is a feasible approach is if your ex has managed to get hold of a leaked database of passwords for a site. It's bad practice for online services to store passwords in basic text form, so they store "encrypted" versions. Automated programs can be used to decrypt a list of passwords, but this is where the length and complexity of your password really make a big difference.

  If your password has been exposed in a leaked database, there is no way to protect yourself from an automated program eventually decrypting it so it can be used to access your account. But the good news is that, if you make your passwords long, then it will take a *reeeeeally* long time to brute force them. Like, billions of years long. (Yes, that was billions with a "b".) Although your ex could eventually manage to get hold of your password, you can take some solace in the fact that at least the sun will have fizzled out and our universe become uninhabitable long before that happens.

  So, *your best defense is still a strong password* – one that is unique and at least 12 characters long.

Making a strong password

How can you make a strong password? The short answer is: think of passwords as pass*phrases*, not pass*words*. Instead of using one word that you then add some complexity to (like mixing uppercase and lowercase letters and adding some numbers or special characters), come up with a sentence or series of words as your starting point.

Not only can short passwords (consisting one word with a bunch of special characters added to it) be difficult to remember, they are also less secure than long passwords. So, when coming up with a password, keep in mind that length is more important than complexity. The password “LoooongPasswords-TakeLongerToGuess” would take millions of years longer to brute force than the password “P@s5word” – even though the second password might seem more secure, with its special character “@” instead of an “a” and its sneaky use of a “5” instead of an “s”.

We aren’t saying that adding some complexity in the form of uppercase and lowercase letters, special characters, and numbers is a bad thing. It’s definitely a good thing. But the main goal is length. Once you have a long password you can then add some complexity to it to make it even more secure. Let’s take an example. One way to make passphrases easier to remember is to take them from your life or opinions. For instance, we could decide on the password “MyFirstBikeWasBlue”. Then we could add some complexity to it (while trying to not make it harder to remember) by modifying it to: “MyFirstBikeWas#Blue!”

One thing to be aware of regarding sentences as passwords is that there are computer programs that can try existing lists of song lyrics, combinations of words, etc. So try to alter your password in some way so that it isn’t taken verbatim from the lyrics of your favourite song. Spell some part of it phonetically, use some language less common than English, add some special characters, or other some such. This is a good idea even if your password isn’t taken from the lyrics of a song. Implementing this in our previous example, the password about our first bike being blue, we could change it to: MyFirstBikeWas#Bluu!

In short, make your password a sentence, and add in some special characters here and there.

Don’t re-use passwords

Remembering passwords is a pain, so many people reuse the same password for several different accounts. (We will cover how to remember long passwords in a bit.) The main reason why reusing passwords is a (very) bad idea is that, if someone gets a hold of one of your passwords, then they can access multiple accounts with it. Remember that stuff about vulnerabilities? Reusing passwords is like having one key for everything you want to lock: your home, car, bicycle, etc.

There are many ways someone can try to get a hold of your passwords, including sneaking a peek as you type one in, sending you an email that tricks you into revealing one, and more. But there is also another way that huge amounts of passwords fall into the wrong hands every year. You may have heard the term “data breach”. Basically, it means that, either by human error or poor security, a bunch of information that wasn’t supposed to end up on the internet ended up on the internet. This can be things like lists of people’s names, social security numbers, credit card information, etc. But it can also include email addresses and passwords. So, there is a risk of your passwords being exposed to the world through a data breach of an organization where you hold an account. But is this the only place you have used this password? One basic yet important way of limiting the damage from a data breach is to use a unique password for each account.

Ideally you should have strong, unique passwords for all of your online accounts. But if you think there’s a risk you aren’t going to bother with that (we know it’s a pain – but please do it anyway), then you should at least have strong, unique passwords for your important accounts.

Your email account is a good example. If your ex gets control of your email password they can then gain control of all other accounts that are tied to that email. You’ve probably noticed that “Forgot your password?” link on login pages. That link usually sends you a link to reset your password. And where is that link sent? To your email. Meaning, if someone gets a hold of your email login information, they can first change your email password so you no longer can access it, and then they can start going through various social media and other sites that are tied to that email account, changing all of your passwords. Securing your email is crucial – a weak email password makes all online accounts connected to that email vulnerable.

Security questions

The idea behind security questions originated back in the time before social media (believe it or not, there was such a time). A time when everything from where someone went to school to what they had for breakfast three years ago wasn’t on display for all the world to see. Security questions about your mother’s maiden name, the name of the street you grew up on, and the name of your first pet are all things anyone has a good chance of getting their hands on. But their chances of finding this information are even better if they know you personally or if you are active on social media.

The solution to more secure security questions is simple: just lie! Treat security questions like passwords. Make them unique. Meaning, never give the same answer to the same security question on separate sites – because your answer might leak in a data breach. And, equally importantly, make sure the answer has nothing to do with the question. (*What was my mother's maiden name*, you ask? Why, it was DogsJumpHigherThanCats#boingboing, of course!)

Two-factor authentication

As we have discussed, if someone manages to get hold of one of your passwords it can have really nasty consequences. This next topic, two-factor authentication (sometimes called 2FA or multi-factor authentication), is designed to protect your online accounts in a way that, even if someone managed to guess or otherwise get hold of your password, they still wouldn't be able to log in to your account.

The term two-factor authentication refers to the requiring of two different means of proving that you are, indeed, you. A common example of two-factor authentication is a bank card with a PIN (short for Personal Identification Number). To be able to access the bank account tied to the card you need to both have the physical card and know the PIN.

There are different ways to implement two-factor authentication for online accounts. A common approach is that, after having entered your username and password when logging in, you are sent a message containing a series of letters and numbers to your phone. The online account then asks you to type in the message text you have received. If you don't type it in, or if you get it wrong, then you are denied access to the account.

What this does is make sure that simply knowing someone's username and password isn't enough to let you access their account. An attacker will also need to access the second form of authentication. In the case of the example with a text message sent to a phone, the attacker would also need to have access to your phone (and be able to unlock the phone), and only then would they be able to access your online account.

Some forms of two-factor authentication are more secure than others, and text messaging is not the most secure method there is. But the important thing is to start by implementing at least *some* kind of two-factor authentication where it is available.

Help with remembering passwords

These days, most of us have dozens of online accounts, meaning we have a LOT of passwords to remember. And, in this guide, we are recommending that you don't reuse any of these passwords *and* that you make each one as long (and complex) as possible. How can you possibly remember them all? Not to fear – there are several ways you can solve this problem:

- **A password manager:** There are programs dedicated to the task of managing your passwords. Password managers will often have a feature where you can have them come up with long, unique passwords for you. Logging in to an account can then be as simple as the password manager automatically filling in your password, or you copying the password from the password manager and pasting it into the login site. Some password managers store your passwords (encrypted) in the cloud, others store them locally on the computer or smartphone you have the password manager installed on. The basic idea in both cases is the same: you only need to remember one password – the password to your password manager. And then the password manager will remember the rest of the passwords for you.

- **A list on a piece of paper:** Having your passwords written down on a piece of paper may seem like a bad idea, but that all depends on your situation. If your home is safe – if you live on your own or with people you trust – then having a list of all your passwords at home is a perfectly acceptable way to manage your passwords. You can add a bit of extra security by keeping your password list in a locked drawer or box, and keeping the key on your keychain. If you want to be extra cautious, you can avoid writing down the password for your most important logins, such as email accounts you can use to restore other accounts.

- **A list in a file on your computer (or phone):** Preferably the file should be encrypted with a long, unique password. And keep a backup of the file on a different computer or a USB stick – preferably one that you store outside of your home. These steps will protect your list in case you lose your device or in case of a fire or flood at home.

Account security and privacy settings

Broadly speaking, security is about protecting yourself from being hacked or tricked, and privacy is about the things we share – sometimes knowingly, sometimes unintentionally.

One example, that lies somewhere between security and privacy, is what your default settings are for storing files. For instance, where does your phone store pictures or video that it takes? Is it only on the phone's internal storage ("memory"), or are they also immediately backed up to the cloud? If you have things stored to the cloud, then you need to take extra care about securing the account that controls that site or service. In other words, make sure you have a strong password, enable two-factor authentication, and so forth.

You should also consider when an app or service gathers or shares your location information. If you post a picture to social media, but don't want others to be able to know where you are, make sure the site doesn't include or tag a location for where the picture was taken.

You can usually change at least some of the settings regarding what you want to share with others (or with the company behind the account or service). Check the privacy settings of your online accounts to make sure you aren't sharing more information about yourself than you are comfortable with, and to minimize the risk that you are sharing – or even storing – any unnecessary information that an ex can abuse.

Detecting access through login records

To help you know if someone has been trying to access your accounts, you can look at the logs that some online services allow you to see. Some services will show you a log of when and where your online account has been used. You can find things like where you (or someone who logged in as you) logged in from previously, and when that happened. So, you can see if your account has been accessed either from a location (like a city) you weren't in at the time, or if they have been accessed during a time when you weren't using that service.

To check these settings for Google, first log in to your Gmail or Google account (either via a browser or on a mobile device). Then go to Account settings -> Security. There you can inspect the following:

- Recent login events: determine if there are any suspicious login activities
- Devices that are logged in: verify if the list includes devices that shouldn't be there

You can also terminate any suspicious device or browser connections. Before doing so, take a screenshot or write down the devices for evidence in case you need it in the future.

Then go to Account settings -> People & Sharing. There, check the following:

- Location sharing: if location sharing is enabled, disable it.

Google Dashboard

If you have a Google (or Gmail) account, you should be aware that by default Google tracks and logs a lot of things about you. Things like what you search for online (if you use Google when you google), what YouTube videos you have watched, where you have been (if you have an Android phone or Google Maps app), and more. You can see (at least some of) the things Google tracks about you on something called "Google Dashboard". If you have a Google account, you can log in to your Google Dashboard at: https://myaccount.google.com/dashboard.

It is worth considering the benefits versus risks of having Google log all this information. Do you need this data stored about yourself? Consider the implications if your ex would be able to access your Google account. And note that you can delete the logs it has stored. You can also pause the logging of much of the information on the site, through Google Dashboard or under "data & personalisation" in your Google account settings. And, as noted earlier, this is an example of an online site that needs extra strong protection measures. If your ex manages to get hold of it, they will be able to access a *lot* of information about you.

iCloud

If your ex manages to get hold of your iCloud credentials, they can view anything you have stored in iCloud. Check to see which devices are sharing the iCloud account. This can be done in the iOS device's "Settings", and go to "Apple ID, iCloud, iTunes & App Store". The listing of devices shows a device's name and what kind of device is logged on to the iCloud account. If you see any unknown or suspicious device listed among the devices, take a screenshot of the phone to preserve a record of the suspicious device, then remove them. Then change the password on your iCloud account. For improved security, add two-factor authentication to your iCloud account (two-factor authentication is discussed earlier in this section).

Now, go through the rest of your accounts and follow this same approach to add additional security measures where possible.

3. Smart devices

Internet-connected versions of products are becoming increasingly common. Seemingly regardless of the product, companies are falling over themselves and one another to try to be the first to offer a so-called “smart” version of said product. And it looks like we’re heading towards a future where it will be increasingly difficult to even *find* versions of products that aren’t connected to the internet.

If all companies were great at security and also really cared about your privacy, then this trend wouldn’t be that concerning. But they aren’t. And they don’t. So it is. Which means you need to learn at least some basics regarding the security-related problems with smart products and how to secure them.

The security concerns related to smart products include both general security issues that everyone should be concerned about as well as additional issues that apply if you are worried about being stalked by an ex. We’ll cover these topics in four sections: security vulnerabilities, default passwords, privacy settings and data sharing, and others remotely accessing or controlling your devices. Then we’ll wrap up this section with a summary of things to think about when buying smart devices.

Security vulnerabilities

The security of smart products can be summarized in one (rather depressing) sentence: many – if not most – smart products aren’t very secure, and their security can get worse over time. This has to do with two things: software development and patches. It is very difficult to develop software that not only works but that also is secure. If the manufacturer lacks knowledge of security or needs to save costs, its products are likely to have security flaws. Furthermore, security is a constant battle between those who want to find vulnerabilities so they can exploit them for personal gain versus those who want to find vulnerabilities so they can “patch” them, meaning to fix or remove the vulnerabilities.

Smart products are notoriously bad at receiving patches. And even when a product does have a patch released, we as consumers are notoriously bad at actually updating our products. (Do you know anyone who has updated the software on their internet-connected toaster?) If left without updates, all smart products will eventually become vulnerable. So not only might your smart product have serious vulnerabilities or security flaws the day you buy it – given enough time without a patch, it (and any other such product) is guaranteed to eventually be vulnerable.

Default passwords

In the previous section, we talked about the importance of strong passwords. Now we get to the exact opposite of strong passwords: default passwords. A default password basically means whatever password a device comes with when you bought it. For example, common default passwords to unlock many SIM cards are “0000” and “1234”.

Default passwords for particular devices are relatively easy for someone to get hold of simply by searching online. And if you don’t change your default passwords, then you have left your device with a huge vulnerability – a very weak password. Some smart devices are made in such a way that you cannot change the default password. Which is, of course, an absolutely insane way to design a product. Unfortunately, there isn’t much you can do about that – except to avoid buying such products. Sadly, knowing which smart products to avoid isn’t that straightforward, and requires effort on our part: doing some research online to see what, if anything, has been said about the security aspects of a device before buying it.

Remote access or control

Being able to control a device via the internet can be handy. But opening a device up to the internet also means that anyone with an internet connection can try to control the device. Though smart homes are a reasonably new concept, there have already been stories about cases where smart devices in the home have been used for domestic abuse. A piece from 2018 in the *New York Times* by Nellie Bowles brings up several problems and concerns about smart products in the home being abused. Bowles tells of victims feeling like they are going crazy, as their appliances turn on and off by themselves, their smart locks stop working, their thermostats keep changing temperatures, and other problems.

If smart devices in your home are behaving strangely, then the first thing to try is simply to turn them off and then on again. (Which is the first thing worth trying – and often the only thing you need to do – when technology behaves badly.)

Another thing to consider is whether it was your ex who set up the device. If they have access to any smart devices in your home – if they have the password to manage it, then it is possible that they are behind any unwanted device behaviour. In such a case, first reset the machine (turn it off and then on again), and then change the password needed to control it. If the device is set up so that you cannot change the password – for instance, if you don't have the current password to it and the only option for resetting the password is through an email, and that automatically is sent to your ex, then you can either contact the manufacturer or unplug the device. An additional precaution you can take is to change the password on your router – the box that gives you your home internet connection.

Privacy settings and data sharing

As if there weren't already enough things to worry about, another problem with smart products is that, like with social media accounts, the default settings on smart devices might make them give out more information than you care to share. Check the settings (or user manual) of your smart product to see what it shares by default, and what you can change about that.

There are (if you know where to look) a mind-boggling amount of things online that are supposed to be protected with a password but aren't. The controls for steel furnaces, security cameras, swimming pools and a whole heap of other things. So, at the very least, make sure your smart product requires a password to use it. (And also make sure it isn't the default password.)

Buying smart products

This might sound a bit odd, but the first thing to consider when buying a smart product is whether you actually need a product that can connect to the internet. Some products, like a home security camera, make sense to be able to access over the internet. Other products – toasters, washing machines and the like – are not likely to be as crucial to hook up to the internet. If you can find a version of whatever product you are looking for that doesn't come with an internet connection, choose that if possible.

The security-related trade-off to consider here is what the benefit is to you of being able to access the online features when you are away from home versus the risks or potential downside involved if someone were able to guess your password or access your device through some other vulnerability in it.

Another important thing to consider is how secure the product is – whether the manufacturer has taken the time to develop and implement proper security. You can check online for security-related reviews of products. And when buying a smart product, ask the salesperson about security. Two important questions are:

1. Can you change the default password on the device?
2. Does the product receive security updates?

And, once you have a new smart product in your home, the first thing you should do is *change its default password*.

In addition to being cautious when buying smart products, you can also improve your security even further by using commercial, off-the-shelf products. There are, for instance, routers designed to not only give you an internet connection (as routers do) but that also help secure smart devices by examining the internet traffic to and from them to see what should or shouldn't be let through.

4. Spy software

Spy software is designed to let someone remotely access your device without your realizing they are doing it. A general term for spy software is Remote Access Trojan, commonly abbreviated to RAT, but the specific type relevant to this guide are usually called stalkerware, spyware, and spouseware. In this guide, we will use the term stalkerware.

There are stalkerware programs designed specifically to stalk and keep tabs on someone without their knowing it. But there are also a host of similar programs that are designed (or at the very least marketed) to help people keep track of their children, loved ones, or employees.

The distinction between the two isn't as clear-cut as one might think or like. Programs marketed towards concerned parents have also been used to keep track of a partner. We have even found programs that offer advice on their homepage regarding how to hide the existence of the app on a phone, so that the owner of the phone won't realize it is installed.

What can stalkerware do?

If an ex manages to install spyware on your computer, they may be able to do things like access the files and documents on your device, access your browsing history, access your stored passwords, as well as change your device settings if there is no password set (or if the password is easily guessable).

Installed on a phone, stalkerware can give your ex access to things like the pictures stored on the device, your text messages, emails, call history, your contacts, give them access to the phone's camera and voice recording, and the geolocation capabilities of your phone (which is the feature that lets your phone know where it is – and by extension where you are).

Where would an ex buy stalkerware and how is it installed on a phone?

The more advanced versions of stalkerware – those designed to hide on the device and let a stalker snoop on all kinds of things – are sold and downloaded from the stalkerware vendor's own site. These kinds of programs shouldn't be available on official stores like the App Store (iOS) or the Google Play Store (Android). However, sometimes they are available on the official stores – at least for a while, until they are reported and removed.

However, there are plenty of apps on both the iOS and Android stores that offer some of the same features of stalkerware, like seeing a phone's real-time location, but which market themselves as being intended for legitimate uses (like keeping an eye on an aging parent with memory issues). These programs are available on, and can be downloaded from, the official App Store (iOS) or the Google Play Store (Android).

It is technically possible to design stalkerware so that it can be installed without access to a phone. For instance by sending the user a link to a file to download and tricking them into thinking they are downloading something benign. However, such cases seem to be the exception, with the norm being that stalkerware is downloaded directly onto the user's phone while the attacker has access to it. Meaning, the most likely scenario, if your ex wants to try to install stalkerware on your phone, is that they will do it when they have physical access to your phone.

Detecting stalkerware on your phone

It is illegal for someone to install stalkerware on your phone without your permission. If you have reason to believe your ex has installed such a program on your phone, and if it safe to do so, take your phone to the police. Before taking it to the police, put the phone in airplane mode so it will be disconnected from the internet. (For an extra layer of security, you can also turn off the phone or put it in a so-called "Faraday bag", if you have access to one). This way, your ex won't see that you are going to the police. And, in case the stalkerware app has some kind of remote delete function, it should also be impossible for your ex to use it if your phone is unable to connect to the internet.

But how do you even know if there is stalkerware on your phone? Unfortunately, antivirus programs do not always spot stalkerware. And even when they do, antivirus programs do not always flag them as malicious. Eva Gaupin of the Electronic Freedom Foundation is among those working to change this situation, so that more antivirus companies would both detect stalkerware and flag it as malware. However, since this is not yet the case, users need to be extra alert.

Regardless of the potentially incomplete nature of a virus scan, it is still a good idea to scan your phone with an antivirus program if you have access to one. Check all results carefully to see if there are any surprises or even slightly questionable findings. As noted, even if the antivirus finds stalkerware, it might not flag it as malicious. If the antivirus finds a program you aren't familiar with, check online for an explanation of what it is or does.

Here are some steps to help you detect stalkerware on your phone:

- Installed applications can be viewed in your phone's settings. (Android devices have all apps in one long list. On an iOS device, scroll down to the end: the last listing is for third-party applications that do not come with the default installation of iOS.)

- Go through the apps one-by-one to see if you recognize them. If you find one you don't recognize, it isn't necessarily stalkerware, but it might be. Look up the app online to verify its reputation and to find out what it is used for.

- If you find an app that appears to be stalkerware, take a screenshot or make a note of the name of the app. As noted, we recommend taking the phone to the police. But you can just uninstall the app if that is not an option or you don't wish to involve the police – and if there is no reason to fear a negative reaction from your ex if they are able to detect that it has been uninstalled. After uninstalling the stalkerware, update the device. If you want to be extra cautious, factory reset the device.

Other tips:

- A factory reset will delete your files, including pictures. Copy anything you want to keep over to another device or storage before doing a factory reset.

- Most stalkerware also consumes a lot of battery because of the continuous background processes monitoring things like location. So, monitor your battery life – it might give you a hint that something suspicious is going on.

- On Android devices, check whether "Unknown Sources" or "Install Unknown Apps" has been enabled. This setting allows apps to be downloaded outside of the official Google app store, which means they are *sideloaded* to the device. Stalkerware is most likely sideloaded directly from the internet in something called *apk* files and installed on the device. The default for this setting on most Androids is "Disabled" and you can disable it if it is enabled.

Jailbreaking (iOS) and rooting (Android)

If a phone has been "jailbroken" or "rooted", it means it has been altered to give the user more privileges – more things they can do with the phone – than they would have on a normal phone. Jailbreaking or rooting your phone would allow your ex to install more kinds of stalkerware or make it more difficult for you to find and remove stalkerware.

The two terms basically mean the same thing, but jailbreaking is used for iOS devices (iPhones and iPads) and rooting is used for Android devices. Let's take a look at each one separately.

Jailbroken iOS

A jailbroken device has been tampered with to give the user more access rights than with a normal iOS device. This can make it possible to do things you normally wouldn't be able to do, like accessing data, such as location, from other apps. It can also make it possible to hide app icons, like the icon for the spyware. And, jailbreaking can make it possible to install types of stalkerware that are harder to get rid of.

Actually, most of the stalkerware apps for iOS need to have a jailbroken device to be installed. And once there, they can be well hidden. You might not be able to detect them by inspecting the device via its user interface.

And even if you haven't jailbroken your phone, that doesn't mean that someone else who had access to your phone hasn't done it. Detecting whether an iOS device is jailbroken can be hard. However, there are some obvious signs of a jailbroken iOS device, such as the existence of certain applications.

- Search for an app called "Cydia". This application is an app store for installing external applications on a jailbroken device and is a definite sign of a jailbroken device.
- Try to update the iPhone. If the update fails or gets stuck, the device may be jailbroken, because iPhone updates can sometimes fail on devices that have been tampered with.
- Use iTunes or iPhone to restore the phone to the factory defaults. In most cases, this will remove the stalkerware from the phone.

Note: If your device is jailbroken, some additional bad news is that in most cases a jailbroken iPhone has void warranty.

Rooted Android

A rooted Android device allows apps to access restricted features and private data locations on the device. This means that your ex might be able to access WiFi passwords, device functionalities like the camera and microphone, and data you have stored on your phone. A rooted device may also make it harder to remove any deeply ingrained stalkerware.

Many of the most invasive stalkerware require a rooted Android device. As such, a visual inspection of the device's user interface may not reveal the existence of stalkerware.

- Check to see if apps called "Kinguser" or "Superuser" exist. These apps are installed when the device is rooted and are a definite sign that an Android device has been rooted.
- Try to install an update to the Android device. If the download fails, the device may be rooted.
- It is advisable to do factory reset for the phone to reset applications and data on the phone. Some stalkerware has in the past been reported to survive even a factory reset. Monitor for further indicators of stalkerware.

Note: As with iOS, the warranty on a rooted Android device is usually void.

5. Spy hardware

The term “software” refers to a program or app. “Hardware” refers to a physical thing. Your phone is hardware, the apps on your phone are software. So spy hardware basically just means a device that is designed for spying on someone.

If you have ever seen a Bond movie you will know there are lots of devices that could be used to spy on someone. But James Bond is fiction. In the real world, the list of spying devices is thankfully much more limited, especially when it comes to those easily available online. And it is those kinds of devices, devices that are easily available online, that we will focus on in this section. More specifically, we will cover GPS trackers, hidden video cameras, and hidden microphones. We will also briefly discuss drones, but mainly to go over some reasons why drones aren’t likely to be a big risk for most people.

One important thing to understand about spy hardware is the difference between active and passive devices. Let’s start with that and then move on to discussing the different kinds of devices.

Active and passive devices

Hardware designed for spying can be either active or passive. Active means it can transmit the data it gathers, passive means it cannot. By way of example, a video camera that is hooked up to the internet is an active device. It can transmit the video it gathers over the internet to the person controlling it. A video camera that isn’t connected to the internet (and doesn’t have any other way of transmitting data) is a passive device. Rather than sending the video stream over the internet, it only stores the captured data locally on its own memory.

This distinction between active and passive is significant. It affects both the options of the person using the devices and our options in how we go about trying to find such a device.

- **Regarding the options – and limitations – for the person doing the stalking:** if someone has installed a passive device, say a GPS tracker on your car, then they will need to physically access your car again to retrieve the data the tracker has gathered. If they have installed an active GPS tracker on your car, they can access to the data over the internet without having to physically access the device.
- **Regarding your options when trying to locate a device:** a passive device can only be found by locating the physical device itself. An active

> device can be found this way, too, but it can also be found by looking for signs of data being transmitted. This won't tell you exactly where a device is (or even what kind of device it is), but it can give a heads-up that there is some hidden device transmitting data.

This stuff about looking for signs of data being transmitted might sound a bit technical. And it is – at least a bit. And it requires some additional hardware. We won't cover it in this guide, but will instead cover some ways to look for spy hardware that doesn't require any special devices or background knowledge. Next, let's discuss the types of devices themselves (all of which can be either active or passive).

GPS trackers

There isn't any exact data to be found regarding how common it is for someone to use a GPS tracker to stalk an ex. There was a case reported in Finland in January of 2020 of a guy who had hidden a GPS tracker in his ex's car, but such news stories are uncommon (at least in Finland). However, there is no way of knowing how many (or how few) GPS trackers are *not* found. One thing we do know is that GPS trackers are things we get asked about pretty much every time we speak with victims of digital stalking or abuse. So, if nothing else, we hope that covering them here will dispel any fears that may come from not understanding their possibilities and – more importantly – their limitations.

Before we get into the details of trackers, let's very briefly talk about what the heck "GPS" means and what it does. GPS stands for Global Positioning System. Basically, what a GPS does is tell you where you are by contacting satellites that are in orbit around the globe. GPS is used quite broadly, with smartphones being a common example of where you might find a GPS in use. Your phone uses its built-in GPS for features that use location tracking, like showing you where you are on a map.

There are ways an ex might be able to use the GPS in your phone to track you, for instance by infecting your phone with stalkerware, or by getting access to your Google Dashboard account (if you have it set up to record your locations). Your ex could also use a phone, hidden in your car, to track you. However, in this section we'll focus on GPS trackers – the devices that you can buy specifically designed for tracking.

Those are the basics of GPS. Now let's take a closer look at some of the capabilities and limitations of GPS trackers.

What can a GPS tracker record?

There are many different kinds of GPS trackers available. While they can all record location data, many can do a lot more. Consider a GPS tracker designed for use in a car: it could offer a complete map of all the places you have been, what routes you took to get there, what times you drove, and even how fast you were going.

Active GPS trackers, ones that can communicate information over the internet to the person who installed it, can also be set up to send alerts. One particular kind of alert to be aware of is something called geofencing. This allows a person to set a "fence" around a geographical area on a map, and then have the GPS tracker send an alert if the car leaves that area. So, if an ex were aware of your normal driving patterns (to the store, to work, to your hobbies), then they could set up a geofence starting outside that area. Then your ex would get an alert whenever you drove anywhere outside of your normal routine.

How long can a GPS tracker record for?

Basically, a GPS tracker can record as long as it has storage space and power. How much data a GPS tracker can store (data about where you have driven, when, how fast you were going, etc.) depends on the kind of device it is. Passive devices, devices that only store data on their own hard drive, are limited by their internal storage. These days, however, even a tiny USB stick, like one you could attach to the end of your key chain, can store huge amounts of data. So in practice, the real limitation is likely to be that of power.

If the GPS is hooked up to get power from your car, then it will keep running for as long as it can keep recharging itself from your car. If it isn't hooked into your car's power, then it needs a battery. And this battery, just like the battery on your smartphone, will need charging every so often. Which means your ex will have to physically access your car (again) in order to recharge the GPS. The battery life of common GPS trackers ranges from two days to a little more than two weeks. However, GPS trackers with large, external batteries have battery times of up to 6 months.

How can someone access data from a GPS tracker?

The answer goes back to the discussion of active versus passive devices. If someone hides a passive GPS tracker on your car, they will have to get hold of the tracker to get hold of the information it has recorded. If someone hides an active GPS tracker on your car, then they can access its data remotely, usually via an app or a website.

Where would someone hide a GPS tracker in a car?

There are different ways to hide a GPS tracker in a car. A key factor that affects the options is whether the person doing the hiding has access to the inside of the car.

- **Outside the car:** If they cannot get into the car, then the simplest option is that the GPS tracker is put in a magnetic box. This magnetic box can then be attached to any magnetic surface of the car. (To make it harder to find, it will probably be hidden somewhere underneath the car rather than visibly on the outside of it.)
- **Inside the car:** If they have access to the car, then they have some options. One option is to simply hide a GPS tracker (or a cellphone) anywhere they can find a suitable spot: underneath the seat, in the glove compartment, or using a magnetic box as described in the previous section. However, if they want to have a steady supply of power to the GPS tracker, then they will need to connect it to a power source in your car.

There are GPS trackers that are designed to be plugged in to your car, into something called the car's on-board diagnostics (OBD) connector. In older model cars, the OBD connector might be located under the hood of the car. More recent models, OBD-II diagnostics connectors, the type used since roughly 2000 onward (depending on country), are required to be within reach of the driver and are commonly located under the dashboard.

Another option is to connect the tracker to the car battery. However, anywhere it can be hooked up to power will do – in the case reported on in Finland that we mentioned earlier, the GPS tracker was hidden in a headlight compartment.

To find a GPS tracker in your car, you can look for anything that doesn't belong. If you are familiar with cars, then you can also look for things connected to the car's wiring that aren't supposed to be there. If you aren't familiar with cars, ask a friend or a repair shop to have a look. Repair shops will be able to lift the car up to get a good look underneath it. If you find a GPS tracker (or spy hardware of any kind in your car or home), contact the police.

An additional option, when concerned about the possibility of a GPS tracker – and, more specifically, an *active* GPS tracker – is that you can search for a signal being sent by the tracker. However, this is a more technical method that is beyond the scope of this guide.

What do GPS trackers look like?

GPS trackers are usually quite small – about the size of a phone charger (with or without the cable). If you type in “GPS tracker” on Amazon, eBay, or any similar store website, you will see a wide range of devices are available. Some have magnets built in to their cases so they can be attached underneath a car. Others may have slots or wires so they can draw power from a car’s on-board diagnostic (OBD) connector or battery.

Some other ways to track a car

Newer cars tend to have navigation systems that can keep track of where the car has been. If you have such a car, check its settings to see what it stores and how it can be accessed, and make changes as needed.

Cars can have dashboard cameras, often called dashcams, that capture video as they drive. Dashcams also commonly track where they have been, meaning where the car has been. Some dashcams may also feed this information directly to the cloud. If you have a dashcam, check its settings to see what information it gathers, how it stores it, and how someone can access it. (For instance, if you want to store dashcam information on the cloud, make sure the account it is accessed from it is password protected – with a strong password, of course.)

There can also be other cases when you car can be tracked. For example, parking apps for certain parking places in shopping malls or event venues may have cameras that read the license plates of incoming cars. The apps for these places can notify you – or anyone who has your license plate number registered in their app – when you arrive and leave a certain parking place.

Hidden cameras

Hidden cameras (sometimes called “nanny cams”) are built into various everyday devices. You can find shops that sell video cameras hidden in things like alarm clocks, phone chargers, DVD players, stuffed toys, and even electrical outlets.

Some cameras have motion detection, meaning they only record when there is movement in the area, which saves storage space. How much video a hidden camera can record depends on the size of storage it comes with, but one common example has 32GB of storage, which means it can record about 200 hours of video.

As with GPS trackers, hidden cameras can be either active or passive. An active camera needs an internet connection. The commonly available ones connect to

WiFi, rather than having their own internet connection through a built-in SIM card. This means that the camera needs to be able to access a nearby WiFi signal.

If you live in a home that you have previously shared with your ex, then an active spying device, such as a hidden camera, could be connected to your own home internet connection. A simple way to disable any active spying devices (either a camera or microphone) is to simply change the password for your home internet connection. That way, any device relying on your internet connection – including ones you don't know about – will need your new password to continue to have access to the internet.

As a side note, surveillance devices that record both video and sound are commonly illegal to sell. Sadly, they nonetheless don't seem that hard to come by.

Finding a hidden camera

One common element all the different kinds of hidden cameras share is that they need a lens through which the camera can capture footage. So the easiest way to look for a hidden camera is to look for the lens. More specifically, to look for light reflecting from the lens. The basic idea is the same as if you were to shine a light on a mirror or a window: you would be able to see the light reflecting off it.

There are special devices (or flashlights) that are designed for this purpose, as well as special apps you can download. However, you can also try it with a regular flashlight or other light source you have available. Turn off the lights in your home and then shine a light around to look for light reflecting somewhere you wouldn't expect it to. The lenses are really small – as small as the round lens on your phone's camera – so look for a fairly tiny reflection.

As with other active devices, you can also look for signals it sends. In the case of an active camera that is connected to your WiFi network, you can examine the devices connected to that network to see if there are any devices that you do not recognize. There are programs available that will let you see what devices are connected to your WiFi network. This can also be done through your router's web interface (check the documentation that came with your router for more information).

If you just want to immediately kick off any unwanted devices on your network, you can do this quickly and easily by changing your internet password, meaning the password on your router. But, if you want to check your router for any unwanted devices (which can be done on the router's website – check the router's documentation for the web address), you should do that *before* changing the password and, thus, kicking such devices off your network.)

If you do find a hidden camera (or spy hardware of any kind), contact the police.

Hidden microphones

Much like cameras, microphones can be built into everyday products, including things like pens, pins, and buttons. Like with cameras and GPS trackers, there are both active and passive hidden microphones, as well as mixes of the two. In other words, there are microphones that can transmit audio over the internet, that can store audio on the device, and that can do both. Sound requires less storage space than video, so a passive microphone can usually record for a longer time than a camera.

Finding a hidden microphone

As with GPS trackers and cameras, a passive microphone requires you to find the actual device. An active microphone, when sending data, can be detected by finding a signal of it transmitting data. However, that will only give you a clue that there is a device, not tell you exactly where it is.

An active microphone is likely to use a nearby WiFi to connect to the internet. An easy first way to address fears of hidden microphones is to change your internet password, meaning the password on your router. You can also examine the devices connected to your home internet network (your router) to see if there are any devices that you do not recognize. If you find a hidden microphone (or spy hardware of any kind), contact the police.

Based on our experience, hidden microphones (and hidden cameras) are not as common compared to GPS trackers. Nonetheless, if you are concerned about being recorded, a commonly recommended trick to make life difficult for potential eavesdroppers is using background noise. (Sometimes this background noise is called “white” noise. This refers to a type of background noise meant to make eavesdropping particularly difficult.) What this means in practice is that you play something else in the background – it can be music, the sound of crashing waves, static, etc. That will make it more difficult for an eavesdropper to hear what you are saying.

A brief note on drones as a means of tracking you

Sometimes people ask about the possibility of an ex using a drone to follow a moving van in order to see where someone will be moving to. In theory a drone could be used to follow you, or a car, around. But there are technical limitations which would make that very difficult. Chief among them is battery lifetime – how long the drone can fly before needing to be recharged.

Small drones have batteries that need recharging within minutes. The bigger the battery, the bigger the drone needs to be to carry its weight. But even the most expensive drones on the market have a flight time of much less than an hour. (There are drones that can fly for several hours, but they are military drones and have a wingspan that is at least the size of a car.)

Another concern for someone wanting to track you with a drone is the distance over which they can control the drone. To be able to steer the drone, they need to be within range of it. As with battery lifetime, the control range of drones varies. Cheaper models have a range of only a few hundred meters or less. More expensive models can have a range of over 10 miles. But unless you are moving only a short distance, the person controlling the drone would still have to be in a car of their own, following somewhere not too far behind you in order to be able to keep steering the drone.

6. If your ex is unusually tech-savvy

There are some additional ways an ex can stalk you, hack you, or generally mess with your life if they are a bit more tech-savvy. However, the situation isn't as daunting or scary as the term "tech-savvy" might at first make it seem. We are primarily talking about something that you will have been exposed to several times before: someone trying to make you think they are someone else. This is commonly done to trick you into clicking on a link or giving away your login information for some online site. This kind of tricking people into things online is a phenomenon commonly known as phishing, but more broadly it is known as social engineering.

In addition to some phishing attacks, we will also cover another thing a tech-savvy ex could potentially try: spying on you by spying on your internet traffic. To do this, they need to be on the same network as you, meaning they need to have access to the same internet connection that you are on. This is more likely in a scenario where you are still living with them (a situation which is covered more in-depth in section 7), but is technically also possible if you use public WiFi.

Phishing – and how to spot a trick website

Phishing means trying to trick you into giving away valuable information. In traditional phishing, this will often be about something like trying to trick you into giving thieves your online account login information.

People who try to trick you into giving them valuable information will try to make you think that you are giving the information to a legitimate person or site. One way to do this is to make the site look trustworthy. This is commonly done by creating a site that looks like a legitimate login page (which looks just like whatever account they are trying to scam you into giving away your login information for) and then trying to get you to log in to it. Since the page only looks real, but actually isn't, what happens when you log in on it is that your login information is sent to the bad guys scamming you.

Why would an ex do this? As mentioned earlier, one goal with trying to trick you could be to get hold of your login information to some online site. However, they could also try to trick you into downloading malicious software onto your computer or phone. Or to trick you into entering your current address or phone number.

The basics of guarding against an ex trying to trick you with a phishing site are the same things to keep in mind regarding phishing sites in general.

- **Check the URL (the website address)**
  The URL, or Uniform Resource Locator, is the address of a website. Phishing sites can look identical as far as the site content goes – they can mimic real sites perfectly. By only looking at the content of a site there is no way of knowing whether it is a real site or a phishing site. But phishing sites can't fake the website address, the URL.

  Scammers will often try to make their website address look like an official site. This can be done, for instance, by slightly misspelling the name of the site they are trying to mimic. Or, by including a popular site name, like google, in the scam site's URL.

  Fortunately, such scams are easy to spot if you know how to look for them. When checking a URL, start at what is called the "Top Level Domain": the .com, .org., etc. And then read to the left from there. The name or word immediately to the left of the "dot" is the site you are visiting.

  So, if you are on a page with the address: google.scamsite.com, then – even though it says "google" in the URL – you are on a page belonging to the site scamsite.com. (And, similarly, if you are on a page with the address scamsite.google.com, then you are on a page belonging to Google).

- **Avoid clicking on links**
  A common method of tricking people is to send out an email saying something along the lines of "Your account has been compromised (or hacked). To secure your account, you need to change your password." And then there is a link to what appears to be a login page. As noted earlier, this is most likely a scam. However, if you think there is a reason to believe it might be a real email, then you can avoid the risk of it being a phishing attack simply by visiting the site directly – in other words, by typing in the site's address in the URL, rather than by clicking on the link.

  So, say Random Company Inc. sends you an email saying you need to change your password, and includes a link. If you believe it might be a real email, then instead of clicking on the link, you enter Random Company Inc.'s website address into your browser.

  Another tricky thing about links is that they can be made to look like they will lead to a different site than they actually lead to. So you can't trust the link to take you to the site it looks like it will take you. If you are using a computer, you can check where a link actually leads by hovering over it with your mouse.

An example of a time when you might want to click on a link would be if you know to expect it. Like, for instance, if you forgot a password and have requested a password reset. Then you will know to expect a link to a password reset site.

- **Don't download things if you aren't absolutely certain what they are**
  Careless downloading is a spectacularly effective way of filling your computer or phone with harmful applications, including spyware or ransomware. Like with clicking on links: if you know what you are downloading and believe the site to be trustworthy, then go ahead.

  Be extra weary of downloadable content that is delivered to you via any form of email or messaging app. If anyone whose identity you cannot prove (for example by calling them and knowing who they are) asks you to download anything via Facebook messenger message, it is better to ignore the message than to download.

- **Don't click on "enable content" or "enable macros"**
  If you get a file that doesn't look right – for instance that has text which is impossible to read – and you get a notification that you need to "enable content" or "enable macros" in order to read the file, don't do it. Enabling macros (sometimes just called content) in typically a Microsoft Office file (Word, Excel) will allow the computer to run a program that has been embedded in the file you have received. This program, it is safe to assume, will be malicious.

  There are cases where you would need to enable macros, but if you aren't familiar with what macros are, and aren't absolutely certain that the file is legit, then don't click enable.

Email and phone number "spoofing"

Not only can websites be made to trick you into believing that they belong to some particular company even though they don't, email addresses and phone numbers can also be altered.

There are websites online that let people send emails so that they look like they come from whatever email address the sender wants it to look like it comes from. You can send an email that looks like it's from any address you can dream up. So, if you get an email that looks like it's from a friend's email (or from the police, or the president, or whomever), then it might be from them – but it might also be something called email spoofing: altering the sender's email address to trick the person getting the email. Well-established email service providers, such as Gmail, may be able to flag suspicious emails for you.

So, if you get an email that looks like it's from a friend or someone you trust, but the email somehow feels off or they ask you for personal information, then remember email spoofing. Call or send an email to your friend and double-check that it actually came from them.

The same is true of phones. It is possible to spoof a phone number, so that a call or text message looks like it's from a different number than it actually is from. The more tech-savvy your ex is, the more skeptical you need to be of emails and text messages. If a friend sends you an email or text message that seems odd, call them directly to make sure it came from them.

Fake public WiFi access points as a means of spying on your internet traffic

Things like surfing the internet and sending emails may seem like they happen invisibly – you type in something in your browser and, presto, you visit a website. However, this doesn't happen at all as invisibly as it seems. Whether surfing the web, sending emails, watching streamed content, or doing whatever else you like to do online, there is a lot of data being sent and received. This data is sent in the form of little collections of information called "packets".

If I want to watch cat videos, my computer first needs to talk to the computer that has the cat videos and tell it I want to watch them. This traffic – between our computer and the sites we visit and services we use – passes through a bunch of different places on its travels. What we are concerned about in this guide is, specifically, any chance your ex might be able to snoop on that traffic – something called "packet sniffing".

Exactly what your ex would be able to see depends largely on how much of your internet traffic is encrypted, which again depends on things like what sites you visit and what apps you use. A general example would be that they could see what websites you visit, but a worst-case scenario (if nothing is encrypted) is that they can see everything, including being able to read any emails you write or receive. Such a worst-case scenario is unlikely, as an increasing amount of websites, email providers, etc. have begun encrypting traffic. However, generally speaking, you still want to avoid allowing your ex to snoop on your internet traffic.

If you aren't living with the person you are worried about, then the main risk of them snooping on your internet traffic has to do with public WiFi access points. It is safer to not use public WiFi and to instead use your phone's own internet connection. If, for whatever reason, that is not an option for you, then you should be aware of a risk (or vulnerability) with public WiFis: WiFi access points can also be spoofed.

Your favourite coffee shop might have a public WiFi called, say, “CoffeeShopWiFi”. And if you log on to that then you will be using the coffee shop’s WiFi. Then again, maybe not. The problem here is that there is nothing stopping anyone from creating a public WiFi access point and calling it whatever they want. Your ex can create a WiFi connection and call it “CoffeeShopWiFi”. Technically, this isn’t difficult to do: they just need a device that can share its WiFi – a router, a phone, a laptop, etc. However, this device will need to be in range of whatever device you are connecting to the internet with – and WiFi has quite limited range.

There are several factors that affect the range of a fake WiFi access point, but in any case the range will be short. Your ex would either need to be in the same room as you are, or somewhere very close by. They couldn’t set up a fake WiFi in their own home, since the WiFi range wouldn’t reach your device in the coffee shop.

There are a few other things to bear in mind regarding WiFi scams. If your favourite coffee shop has a password-protected WiFi, they will have the password listed somewhere. And your ex can add the exact same password to their fake WiFi connection. This way, you will feel even more certain that you are logged on to the coffee shop WiFi, even though you aren’t.

This scam is made even more difficult to notice if you allow your phone or computer to connect automatically to publicly available WiFi networks. Then, even if you aren’t anywhere near your favourite coffee shop, if your phone notices what it believes to be the coffee shop WiFi within range, it can still automatically connect to it.

So, if possible, use your phone’s own internet connection. And if you are out on the town and need to connect your laptop or tablet to the internet, then you can set up your phone to grant internet access to those devices. Meaning, your phone can help your laptop or tablet connect to the internet. This is called using your phone to create a WiFi “hotspot”. (Note that when you use your phone to create a WiFi hotspot for another device to use, you will be using your phone’s data.)

- Exactly where the settings to enable hotspotting can be found are likely to vary depending on what phone you have. But it will be something along the lines of first choosing “Settings”, then “Network and Internet”, and then “Hotspot and tethering”.
- When you enable hotspotting on your phone, it may automatically generate a password or it may by default allow anyone to use its internet

connection. If your phone doesn’t automatically generate a password, add the password requirement yourself. To do that, look for an option called something like “Set up WiFi hotspot”.

With that done, find your phone’s WiFi network using your laptop or tablet and enter the password to connect to it. Now you don’t have to worry about an ex listening in on your internet traffic!

There are some additional precautions worth taking, like encrypting your internet traffic using HTTPS and, if possible, using a VPN. These precautions will be discussed in the next section.

7. If you are still living with them

This section is for people who are still living with the person they are concerned about. We will cover what kinds of activities will leave a trace that this person can find, and how to use a computer or surf the web without leaving a trace.

This section does not cover what to do if there is a risk of physical violence. We are not psychologists or police officers – we can only offer advice regarding technology. There are support groups, as well as the police, you can talk to if you fear violence. There are also shelters you can go to to escape a bad situation at home. We will not cover these topics, but the websites and phone numbers of support groups, shelters, and the police for your area can be found online.

Note: Please access the internet *securely* when searching for shelters, support groups, or any other similar topic online. We will cover how you can use the internet anonymously in this section of the guide.

Spying on your internet traffic through your home internet connection

In the previous section, we covered risks related to public WiFi and packet sniffing. If you are still living with the person you are worried about, then there is also a risk of them spying on your internet traffic over your home internet connection. Since they will be able to use the same internet connection as you, they will be on the same network and can (if they are tech-savvy enough to do it) log and look through all of the internet traffic that goes through your home WiFi connection.

As with public WiFi access points, a simple solution is to use your phone as an access point to the internet for anything you don't want your partner to be able to see. However, there are some other precautions worth considering – things we recommend to people regardless of whether they are concerned about the person they are living with.

Encrypting your internet traffic: HTTP, HTTPS, and the browser add-on "HTTPS Everywhere"

Your computer talks to the internet (or, more precisely, with the computer – called a server – that has the content you want to access) using a computer language (or, more precisely, a protocol) called HTTP (or, more precisely, Hypertext Transfer Protocol). You do not need to remember or even understand any of that – the important thing to remember is that HTTP is is not encrypted.

Meaning, if your partner can access that unencrypted communication, they can know a lot about what you do online.

Thankfully, an increasing number of websites offer encrypted connections. This is done using something called HTTPS (note the additional “S” on the end – think “S as in Secure”). HTTPS encrypts the communication between you and the site you visit, making it impossible for your partner to read or understand.

There is a free add-on you can get for many browsers that will make sure you always use an encrypted connection when possible. This add-on is called “HTTPS Everywhere”, and it is developed and maintained by a non-profit called the Electronic Frontier Foundation. HTTPS Everywhere is available for Chrome, Firefox, and Opera browsers. You can read more about HTTPS Everywhere, and download it for free, at https://www.eff.org/https-everywhere.

Note: it is important to remember that HTTPS does not hide the fact that you have visited a site. Once more, for emphasis: HTTPS encrypts your traffic with a website, but does not hide what sites you visit. So, even using HTTPS, if the person you are living with is monitoring your internet traffic, it is still not safe to visit sites that they might react negatively to your visiting (for instance, a site about domestic abuse or stalking).

Virtual Private Networks

HTTPS protects content you view on websites from being snooped on, but it doesn’t hide the URLs you’re visiting from anyone using the same network. In other words, they can see you visiting *example.com,* but they cannot see what you see on *example.com* nor can they see your credit card number if you submit it on the website.

For additional security, you can also use something called a Virtual Private Network, usually referred to as “VPN". A VPN commonly does two important things to improve both your security and privacy:

1. A VPN encrypts your traffic. This means that someone on the same network as you will be able to see that there is internet traffic, but won’t be able to see what it is.

2. A VPN sends all your internet traffic through the VPN provider’s own server (or computer) first, and then on to the site you want to visit. In practice, this means that the website you are visiting won’t know that the traffic it is receiving is coming from your computer.

Normally, a website will get a lot of information about visitors, including what browser they are using, what operating system you are using, they will see something called your IP-address, which will give them a reasonable approximation of where you are physically located, and more. These concerns aren’t particularly relevant to this guide in particular, unless you are visiting a website hosted by your ex or the person you are concerned about. However, if you can afford one, a (reliable) VPN is always a good investment for anyone concerned about privacy. VPNs are available for smartphones, computers, and tablets.

Note: All your traffic will pass through the VPN provider. So, don’t do an online search for “free VPN” and randomly pick one. Choose a VPN you have reason to trust – one by a reputable company with a good track record.

Surfing the web anonymously

Our advice on anonymous surfing depends on who you want to hide your internet traffic from. We will cover a few different scenarios, from easy to challenging.

Your only concern is your ex, you do not live with them anymore, and they do not have access to your computer or phone

In this situation, it will be very challenging for your ex to spy on your internet traffic at all. (Except perhaps in unusual cases, like that they work for your internet provider, the police, the government, or some such.) The main things to think about here are:

- That your online accounts are secure. If your ex has access to, or manages to hack, for instance your Google account, that can give them access your Google search history, watched YouTube videos, location, and more. (See section 2 for more on securing your online accounts.)

- Remember the discussion about public WiFi access points, and that it is safer to browse the internet using your home WiFi or your phone’s WiFi. And consider installing HTTPS Everywhere on your browser and getting a VPN.

Your only concern is the person you live with, and they have access to your computer or phone

As we discussed in the beginning of this section, a tech-savvy person can monitor the network traffic to and from your home internet connection. So, the main things to think about here are:

- You can use a VPN to encrypt your internet traffic. However, if you are using your home internet connection (for instance surfing on a computer or tablet), then even with a VPN, this person will still be able to see that you have been active online. You can avoid this by using your phone.
- Set your browser (the program you use to access the internet) to browse in “private”, “guest”, or “incognito” mode. This feature is available (under different names) in most browsers. In this mode, your computer won’t save your browsing history or cookies from sites you visit. The site you visit will know you have visited it, but someone examining your phone later will not – as long as you have closed the site. (Note: any files you download in this mode will not disappear when you close the browser. How to securely delete files is discussed separately later in this guide.)
- If this person has access to your online accounts or manages to hack them, they can still know a lot about what you are doing. (See section 2 for more on securing your online accounts.)
- Rather than using your own computer you can use a friend’s computer, a computer at the public library, a computer at a shelter or support group, etc.
- A further option regarding secretly using the internet is to use something called TAILS, which we will cover in the following section.

You don’t want anyone to be able to see your internet traffic

If you don’t want to take any chances regarding your internet traffic, then the Tor browser is the option for you. You may have heard the term Tor in connection with stories about illegal activities. Let’s start our discussion of Tor by clarifying some potential misunderstandings.

The Tor project is the nonprofit organization behind the Tor browser. The Tor project consists of several different products and tools. Among those tools are those that enable people to manage websites anonymously (you may have heard of the “dark web”, which refers to such sites). People involved in illegal activities are among those interested in hiding their internet traffic and maintaining anonymous websites, and are thus among the many users of Tor products.

However, the sensationalized picture of Tor as being solely linked to such users leaves out the many other uses for Tor and the many other types of users who benefit from it. People and groups like journalists, whistle-blowers, dissidents in oppressive regimes, and victims of domestic violence or a stalking ex. All of these people have good reasons to be extra careful about their anonymity online.

The Tor browser is a browser with a focus on anonymity and anonymous communication – making sure no-one knows what sites you visit. This is the tool we recommend for this situation. Note, however, that the Tor browser itself will be visible on your phone or computer. You can hide what sites you visit, but not that you have Tor installed. If that is a risk you cannot take, then see the coming section on TAILS.

Note: Hidden (or dark web) sites do not show up on normal searches made with the Tor browser. You will not accidentally stumble upon any illegal sites – at least not any illegal sites you wouldn't stumble upon with any other browser. The Tor browser works just like the search engines and browsers you normally use, and you will get the same kinds of search results and be able to visit the exact same websites with the Tor browser as you do with whatever browser you are using now. (To get to the hidden sites you may have heard or read about you need to know the exact address to type in the address bar. And they are long, nonsensical addresses.)

Using a computer *and* surfing the web anonymously with TAILS

TAILS (short for The Amnesic Incognito Live System, in case you were wondering) is an operating system developed by security and privacy experts, designed to protect its users' privacy and anonymity. By default, TAILS saves no information from your session. Meaning, when you turn off the computer all traces of what you did while using it are wiped clean. By default, TAILS also sends internet traffic through Tor.

You can install TAILS on a computer so that the computer always uses TAILS. However, you can also install TAILS on a USB stick. Using TAILS from a USB stick hides even the fact that you have access to TAILS. The only way someone can find any trace of your ever having used TAILS is if they find the physical USB stick with TAILS on it.

- To use TAILS from a USB stick, first install TAILS on a USB.
- Then plug the TAILS USB into a computer. Turn on the computer (or restart the computer, if it was already on).
- Before the normal operating system installed on the computer actually starts, you will be given the option to open something called the "boot menu". The boot menu is where you can tell the computer to run TAILS instead of your standard operating system.

- Unfortunately, this part is a bit tricky, since the exact key to press will depend on what operating system and model of computer you are using. Your computer will show you what key to press – the so-called “boot menu key”, but it might flash by pretty quickly.
  - Common boot menu keys on a PC are: Esc, F7, F8, F9, F10, F11, and F12 (and can also be the Novo key on a Lenovo)

    You can find a more detailed list (and start-up guide) on the TAILS website: https://tails.boum.org/install/win/usb/index.en.html#start-tails
  - On a Mac, press-and-hold the Option key (Alt key). See the TAILS website for more: https://tails.boum.org/install/mac/usb/index.en.html#start-tails
- From the boot menu you can then choose to start TAILS from the USB stick.

With TAILS running on your computer, it will use your computer’s hardware to run without leaving a trace of your activities on your “normal” computer’s hard drive.

You can read more about TAILS, and download it, on its website: https://tails.boum.org/

How to delete files securely

When you delete a file on your phone or computer, the file is not actually destroyed. What happens is that you give the computer permission to use that space on its memory for other things, if and when your computer needs more space. The file that you deleted will no longer show up if you do a search for it, but it is still there. And there are programs someone can use to find such “deleted” files.

If you want to completely remove all evidence of a file ever having existed, then the only way to safely do that is to write over the file. Meaning, to fill the space on the computer’s hard drive that the file was on with something else. And, to be safe, you will need to write over that space on your computer’s memory several times.

If you know what file you want to delete, there are programs that can write over them, multiple times, for you. (TAILS also has such a program.) If, however, you have previously deleted a file, and don’t know where it is on your computer’s hard drive, and want to write over it, you may need to fill all of the available memory on your computer multiple times. *Fill it with what?*, you might ask. Sushi recipes, Unicorn pictures, Rick Ashley videos – anything that doesn't matter if it is found. Filling an entire hard drive multiple times is a time-consuming process. Thankfully, there are programs that can help do this for you. Note, however, that if the person you are concerned about is tech-savvy enough to recover deleted files, they are likely to notice that you have securely deleted (or overwritten) something – they just won't know what.

If you do not need to delete a file, only make sure that others cannot access it, you can encrypt the file. This is not at all as difficult as it might sound – there are programs that will do this for you. You will need to enter a key – a password – that you can use to unlock (or decrypt) the file. However, the existence of the file will not be hidden – it will just not be possible for someone who doesn't know the key to access the file. (If you want to be extra cautious you can encrypt a file and then delete it.)

Securing your devices and online accounts when living with someone you don't trust

There are two different approaches here, depending on what you believe the person's reaction might be to your increasing your security. The short version is:

- If there is no reason to fear a bad reaction, you can use all the tips in this guide and secure the heck out of your devices.
- If, on the other hand, their reaction to your securing your devices and accounts might be bad, don't do anything that would raise suspicion or anger them, and instead create new, secret communication channels.

Let's take a closer look at each scenario, and what you can do, in turn.

If there is no reason to fear a reaction to your securing your accounts or devices

Don't use facial recognition or your fingerprint as your only screen lock on your phone. These can be accessed in your sleep by holding your phone in front of your face or placing your finger on the phone. Instead, use a PIN or password, preferably six digits or longer. As with online account passwords, don't make your password or PIN easy to guess. So, for instance, don't use the date of your birthday (or a child's birthday) to lock your phone.

Change the PIN on your SIM card so it is not the default password it had when you bought the SIM card (default PINs for SIM cards can commonly be found online if you know what telephone provider someone has).

Lock your computer with a password. Again, a password that your partner won't be likely to guess. Shut down your computer, or set it to sleep or hibernate, when you leave it, even just to go to the bathroom. And set the computer to require a password when you wake it up from sleep or hibernation.

Set the computer to go to sleep when not in active use, in case you forget to put it to sleep yourself when leaving the computer unguarded.

In addition to locking your computer, you can add en extra layer of security by encrypting your computer's hard drive. This process of encrypting the hard drive can be set to be done automatically. When you fire up your computer, you will be asked first for a decryption password, and then for the password to unlock your computer. (Don't use the same password for both.) For most scenarios this is likely to be more security than you need. However, if the person you are living with is computer-savvy, then they could for instance access your files by connecting your hard drive to a different computer (running a different operating system) and thus be able to bypass your computer's password check. However, if your hard drive is encrypted, they would still not be able to access your files.

Regarding both phones and computers, be mindful of "shoulder surfing". In other words, your partner looking over your shoulder to see your password or PIN as you are unlocking the device.

As a final (somewhat self-evident) note: In addition to these tips, everything we have discussed earlier in this guide about securing online accounts, computers, etc. is of course also relevant and important.

If you fear a negative reaction to your securing your accounts or devices

If there is any reason whatsoever to believe the person you are living with might become violent or otherwise react poorly, then you need to be careful about their realizing you are looking for signs of stalking, are interested in improving your security, or are trying to do things without them noticing.

You can keep your accounts as they are and instead create new, secret accounts for communication. Maintain the appearance of normalcy on your computer and phone – do the things you would normally do. And use your new account(s) for secret communications.

If the person you are living with has access to your phone, you should consider the possibility of stalkerware (or some other form of tracking) having been installed on your phone. The same goes for your computer. If your device is infected with such a program, then they can know what you have done on that computer. Use a computer they cannot monitor – for instance a friend's computer or a computer at a public library – to create a new email account, social media account, or whatever account you want to use to use for secret communication. (If there is a spy program on your phone or computer, then the person you are living with might be able to see both that you have created a new account, as well as even get a log of the password for it.)

If you have a place to hide a "burner phone" – an extra phone that you don't tell this person about, then that is another option worth considering. (If you hide it in your house, remember to set it to silent and turn off all notifications, so it doesn't give away that it exists.) You also need to be mindful of the paper trail such a phone might leave: you don't want to get the phone bill sent to your home or to an email account this person might be able to access. Also, if they can access your bank information, or read your bank statements, then you don't want payments for your phone to be visible on your bank account or bank statements. To avoid these kinds of issues, you can buy a burner phone and SIM card using cash. Only getting a separate SIM card that you swap in and out of your existing phone for secret conversations can be dangerous, as your phone can save information from your secret communications (like text messages or contact information).

Another option is TAILS, which we discussed earlier. With TAILS you can use any computer, even the one in your home, without leaving a trace on the computer itself. The only sign of your use of TAILS will be the USB drive that has TAILS on it.

Note: You need to be mindful so that you don't accidentally continue discussions from your new email, social media account or other communication channel on your old communication channels – the ones that the person you are living with might be watching. (For instance, accidentally using your watched email to reply to a message a friend sent to your secret email.)

Acknowledgements

First and foremost, we offer a heartfelt thanks to all the people who have shared their stories with us. Your questions and concerns helped shape this guide. It was a pleasure talking with every single one of you (which is quite amazing given the unpleasant topics of our conversations).

We owe a further debt of gratitude to the many social workers and volunteers who have taken the time to speak with us. In particular, Jonna Brandt of Tukikeskus Varjo (Viola ry) who has been both a fountain of information as well as a tireless supporter of this guide through its many incarnations – starting from when we were gong to write “a few key tips we could print on something the size of a business card.” Thanks also to the rest of the workers and clients at Tukikeskus Varjo and Viola ry, as well as at Naisten Linja, and Avopalvelu Pesä.

Thanks to Antti Kurittu for taking the time to read an early draft and correct some mistakes. And thanks to our editor, Chris McPhee, for doing the spectacular job he always does.

We sincerely hope this guide will help the people who need it.

Linus Nyman & Laura Kankaala