CounterAct
Building People Powered Action

DIGITAL PRIVACY

January 2024

Digital privacy is about making sure that information is accessible to you whenever you need it and not accessible to anyone seeking to exploit it. Strong digital privacy practices help to keep us effective and safe.

Campaign and protest work targets powerful entities, and in turn our work is targeted by governments, corporations, hackers and trolls. The tech boom of the 21st century upended the very concept of privacy, and exposed everyone, especially people in marginalised communities, to risks that did not exist a decade or two before.

Privacy is not a concept that can be universally applied. It is subjective and personal. People have differing needs and vulnerabilities. A piece of information about someone may seem utterly unimportant to you but may feel deeply personal and private to someone else. Seemingly random pieces of information can be combined to create an alarmingly clear profile of behaviour.

It is critical that anyone organising and engaging in working for positive change of any kind be aware of the risks to digital privacy and take appropriate steps to mitigate them.

Learn more about these concepts in Tactical Tech's Holistic Security Manual.

Planning for Privacy

Digital privacy planning usually follows a few simple steps. You don't need to be an expert, there are resources to help, but it is important that these steps are worked through thoroughly for any information that has value for you, your team and your work, before you decide what platform or process is appropriate for your information.

What information do we have that needs to be protected?

Personal information about organisers and supporters, financial data, plans for protests and actions, strategies or tactics. In our organising and campaign work, knowledge is power in a very tangible way. Information needs to be protected against physical vulnerabilities too. If your device is lost, stolen, surrendered or it fails, can you still access the information you need?

Who would want this information?

Hackers who sell name and password data, corporations that profit from what we're trying to prevent, governments and law enforcement agencies who act in the interests of those corporations and practices. These are our 'adversaries.' They want different things, our information is valuable to them in different ways, and they have different resources available to them to try and get it. Assume the worst.

What happens if they get this information?

Not all information is of equal value. Asking this question is a useful way to figure out what is the most important information you have. Information loss could impact your work and the people you're working with in ways you hadn't considered. Again, assume the worst.

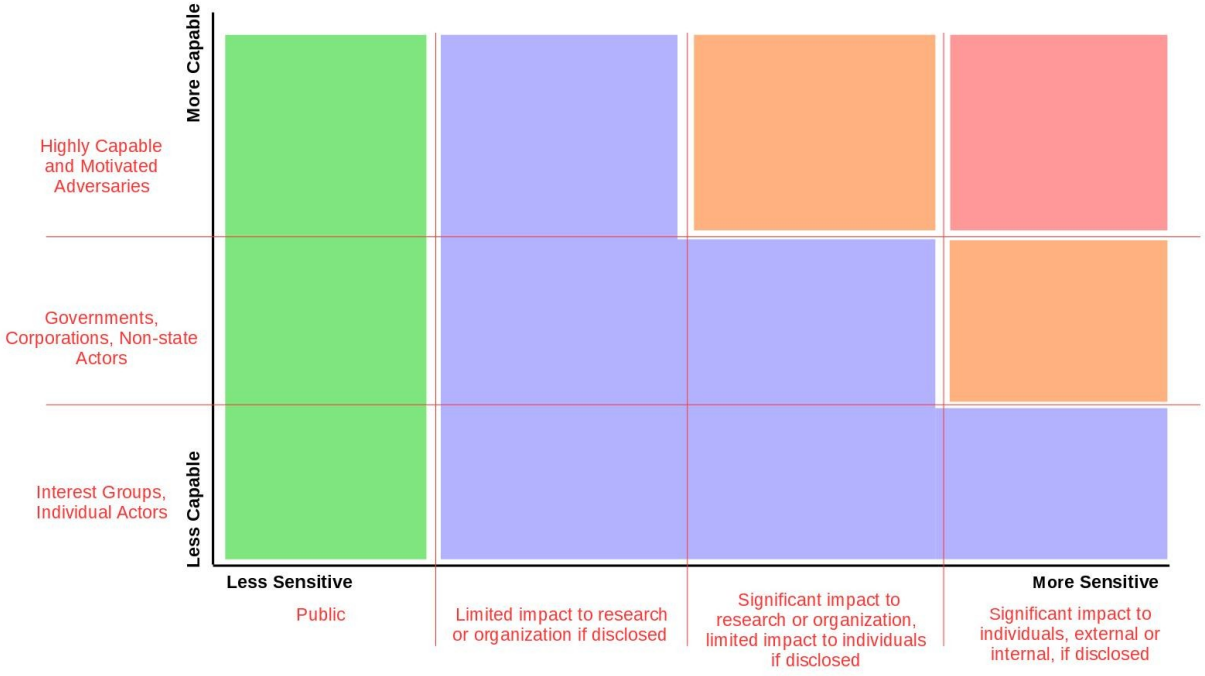
How hard is it for them to get this information? Who else has it?

There is no perfect security plan, no way to make information impossible to obtain. Almost all information is shared with someone, whether it is the online service you use for your documents, your internet service provider, the company who made your device, the person you share your office with… In the course of your work, your information is available to more people than you might think.

What can we do to make this information too hard for our adversaries to access?

There are tools and systems we can use to make it extraordinarily difficult for even agencies with seemingly limitless resources to access our information. Small changes in our practices and behaviour can make things exponentially more difficult for our adversaries. Remember that whatever you do has to work for every person and every use of your information. A less powerful tool everyone can use provides far more security than an overly complex one people work around.

Tim Sammut's Secure Communications Framework is a graphical tool that can help you understand your digital privacy needs.



People

In the search for appropriate tools for your information it is easy to overlook that the single greatest vulnerability we have is people. Either by accident or on purpose, people's behaviour can lead to important information being obtained by those who shouldn't have it.

Personal information has different value to different people. We always have to keep in mind that some information in some situations makes some people far more vulnerable than others. Securing that information is the minimum standard you must aim for. Remember that information about you and your work may be used to target and exploit other people, not just you.

In day to day life outside of campaign work we're all targeted by scams and spam, schemes to steal our money, our passwords, and any other information of value.

We've seen these efforts evolve and become more sophisticated, largely due to a kind of digital herd immunity—pretty much everyone knows by now that the Nigerian Prince does not actually have millions of dollars that he needs to put into your account—and that immunity continues to grow.

People are making their passwords harder to guess, using more secure login methods for their banking, keeping a backup copy of their photos, and doing a range of other things that are now second nature, to preserve their digital privacy. Collectively we're all making it harder for people with bad intentions.

A chain is only as strong as its weakest link; if a tool or system is too burdensome to use, it won't be used at all. That digital herd immunity has only grown because tools and systems made it easier for people to change their behaviour. Many older programs and platforms required a lot of time to use and manage, but modern security tools have evolved to become much more user friendly, and in some cases even more convenient than not using them.

If we all build better habits to protect our own information, we can then build on those habits for our most critical information within the campaign. There are a few simple things you should be doing for your digital privacy no matter what work you're doing.

Is my device listening to me?

Yeah? Kinda? But probably not in the way you think.

At the end of 2023 a marketing company claimed they could do what many suspect had already been happening for years; they offered precise ad targeting using conversations recorded by your devices. However this was quickly debunked and the company hastily released a clarification.

We are surrounded by microphones and cameras. It isn't just phones and laptops. Doorbells with internet connected cameras are massively popular. 'Voice assistants' are found in cars, TVs, other 'smart' home appliances and dedicated devices like the Amazon Echo or Google Assistant. These devices have an always-on microphone that listens for an activation keyword. Most of the time it is more of a nuisance as the device activates when it isn't wanted, or fails to understand the keyword when it is wanted, but not always.

There have been cases of conversations inside peoples' homes being recorded, Amazon being the worst culprit. Employees were caught watching video from customers' Ring doorbell cameras, and Alexa has recorded private conversations and sent them to another person without being directed to on multiple occasions.

Aside from the activation keyword (OK Google, hey Siri, Alexa, etc), every time a command is given to one of these devices it sends the audio up to a server and receives back the instructions that were interpreted. Google, Apple, Amazon, Samsung and other vendors claim that they do not retain audio that is identifiable, but the privacy protections and the recourse available to users is murky at best.

Advertisers don't need to go to the trouble or expense of constantly listening to you to target you with creepy precision. They don't need to record the conversation you had with your new partner about what they might like for their birthday to show you an ad for the perfect gift. They already know the birthday is coming up. They already know you went to the same restaurant or shop at the same time. They already know what you've been searching for online and what your partner has been searching for. They already know what you've bought recently, and what your partner has bought recently.

It only takes a few separate pieces of information to form a detailed picture, particularly when it is cross referenced with another person. American retail giant Target was able to ascertain a teenage customer was pregnant before she'd had the chance to tell her parents. The parents found out when vouchers for nappies arrived in their mailbox addressed to their daughter. This was back in 2010. Advertisers have vastly more information available to them to understand your purchasing habits and intentions nowadays.

The tech giants and the companies who buy advertising space on them don't need to listen to our every word, they're doing just fine with the vast amount of information they can already gather or buy. But more than 10 years after Edward Snowden blew the whistle on the extent and power of government surveillance, we know that any device with a camera or microphone could be activated and exploited by an organisation with the motivation and resources.

What is Encryption?

Encryption is how we secure information that is stored or communicated electronically. Using complex maths, the 1s and 0s that make up a digital file are scrambled in such a way that it cannot be read until it is decoded. This decoding is done with a key, which 'unmixes' the file so it can be read again.

As with many other security measures, perfect encryption does not exist. It is theoretically possible to decrypt a file without its key, but the better the encryption, the more computing power is needed to do it. Modern encryption techniques are so mathematically complicated that the computation needed to decrypt them without the key simply can not be done with existing technology.

In modern secure software applications, all of this complexity is performed behind the scenes. All you need is your user ID, like a phone number or email address, and your password, just like any other app.

You can learn a whole lot more about encryption here.

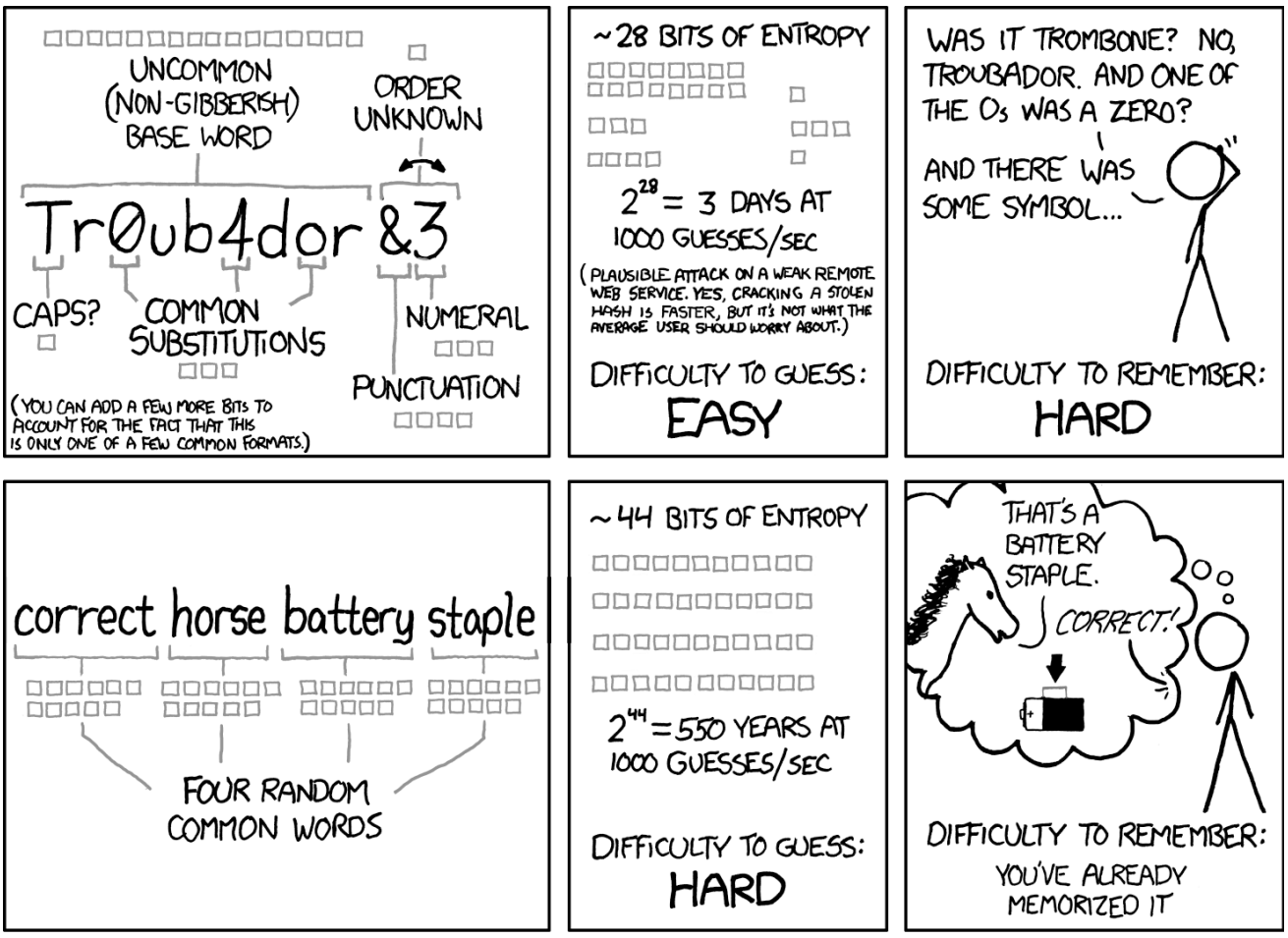
Password? Passphrase? Passcode? Passkey?

These terms are often used interchangeably, but they have different meanings.

The most commonly used, and the least secure, is the password. A password is a string of characters, almost always fewer than ten letters, traditionally spelling out something memorable and important to you, to verify you when you log in somewhere. Passwords are vulnerable both because they can often be guessed by someone who knows you or knows about you, and because modern computers can guess them in a short amount of time. More recently services have required more complex passwords to counter this, by forcing users to include upper and lower case characters, symbols and numbers into their passwords. Password managers are excellent for generating and storing these more complex passwords.

A passphrase is a more secure variety of password. Stringing together multiple words to create something much longer makes a passphrase harder to guess and much tougher to crack. You can make a good passphrase only you can guess using dice.

Nerdy web comic XKCD published this very nerdy explanation of passphrases.



The term passcode is used to describe a numerical key like your bank card PIN, or the lock on your phone, or a 6 digit 'one-time' code. The latter is the most common way Two-Factor Authentication (2FA) is implemented, which you can read more about below.

Passkeys are significant step forward for security. They are structured similarly to other forms of encryption, and work to verify your account with the device you are using to access a particular service. Using a passkey means that the user, the account and the device being used to access the account all have to match with what was registered with the service. A password matches only the account and the user. An increasing number of services are enabling passkey logins, and they should be used wherever they're available.

You can do these things today

Lock your device properly

Every device you use should have a secure PIN or passcode, and be set to lock in a short amount of time. Biometric tools like fingerprint or facial recognition are convenient, but can be easily used by someone who can compel you to unlock your device if you've been detained and your device is seized. If you insist on using those logins, make sure you know how to quickly lock your device to leave it requiring a password. Always disable biometric logins before you attend a protest or action.

Set your device to automatically update

More than 90% of all software updates are security updates.

Whether it is from from either the hardware company that made your device or the software companies that made the programs you use on your device, these 'patches' (because they cover holes) are almost always about addressing a security vulnerability, so should always be installed as soon as you're able. Look up how to set your device to automatically update online.

Turn on encryption

Many devices now come with their stored data encrypted by default, and will only decrypt when your passcode is entered. Other devices can switch encryption on in the device settings. Search for information about encryption on your device online.

Really delete data from your device

Data recovery programs are very capable, and can read information that has been 'deleted' by your device operating system. Sensitive digital information, just like paper records, should be destroyed in such a way that it can not be read again.

Because different devices store and encrypt data in different ways, the programs to securely delete that data differ. Search for the information about securely deleting data from your device online.

Limit the data your device sends out

We have a GPS device with us almost all of the time. If you look at your WiFi networks you'll often see other people's phones with their hotspot turned on, or an option to AirDrop a photo to a stranger.

Check your device settings like location, camera roll and WiFi to make sure you're only sharing the information you need to with the apps as you use them.

The apps we use constantly send data to their host servers or third parties. Privacy policies are written to be deliberately confusing, obscuring just how much about you the apps record. The business model of the modern internet is dependent on the extraction and monetisation of information about you. This information can then be easily obtained by organisations that are opposed to the work we do.

There are a range of alternatives you can use to keep the information you share to a minimum, which you can learn about below.

Browsing the web

The most common web browsers gather a lot of information about you and bombard you with advertisements. On your phone or computer, Google Chrome and Microsoft Edge are the biggest culprits, but they're very easy to replace.

The Brave web browser uses the same technology as the others to read and display web content, without all of the advertising surveillance, and is available for any device or operating system.

The Firefox browser is the most recommended alternative, it is produced by the Mozilla Foundation, who work to maintain a secure and open internet for everyone who needs it while protecting people's right to privacy.

If you require a greater level of privacy, consider using Tor. Tor is a web browser that obscures what you are looking at online by using a series of 'nodes' in between you and the information you're looking at. Normally you connect to your ISP and your ISP connects to the information you want. All of this is visible to your ISP; they know what you're looking at, when you looked, how long you looked, what you used to look, and so on. When you use Tor, your ISP only knows that you connected to the first node, the second node can only see that a node connected to it and wants to connect to another node and look at some information, the third node can only see that the second node wants to look at some information, which it passes back along the chain. You can learn more about Tor here; it may sound complex under the surface but using it is very similar to a normal web browser, and it is available on most devices.

Searching online

Every time you use an advertising platform to search online, that platform learns more about you, which in turn can then be exploited by them or anyone they share that information with. As those search engines become more polluted by advertising, they become less useful as a source of information and only work as an advertising funnel.

Duck Duck Go is a privacy focused search provider and meta-search tool, a search tool that uses other search tools without giving away any additional information about you. You can use it for Google, Bing, Wikipedia, Netflix and thousands of others. Set your device to use Duck Duck Go as the default search in just a couple of steps.

Use a Password Manager

Password managers save your time and protect your information. There are good options to choose from, and they're very easy to set up and use. They can enter your name and passwords for you when you browse, tell you if your existing password is not secure enough or has been compromised, and help you generate new and unique passwords that it then remembers and enters for you. Modern password managers can also do this for your passkeys too. Choosing a password manager is easy, learn more here.

Set up Two-Factor Authentication (2FA) on every account

Two-Factor Authentication is how a system makes doubly sure you are who you say you are. The use of two different methods of authentication—a password, a fingerprint, an app or physical token assigned to you with a code number that changes every half a minute —for access vastly reduces the likelihood that anyone else could be accessing your account.

2FA serves as insurance against someone knowing your password. There are a range of apps and devices you can use for this, learn more here.

Use a VPN (Virtual Private Network)

One of the most used surveillance techniques used by corporations and governments is to monitor what information goes in and out of home and office networks. In Australia it is a legal requirement that your internet service provider (ISP) keeps this information about you. Additionally your ISP may block access to some sites.

A VPN gets around this by doing your web browsing for you. Instead of connecting to a website, you connect to a VPN and it connects to the site for you. The impact on your connection speed is negligible. All your ISP can see and record is that you connected to your VPN. Some VPNs keep records like ISPs do, so for more privacy choose one that doesn't. Learn about finding the right VPN for you here.

Use the 3-2-1 data backup plan

The 3-2-1 rule is a simple way to protect your data from physical damage or loss.

(3) make, keep and look after at least 3 copies of your information. You have your original, plus two extra copies of everything of value.

(2) store your information on at least 2 different types of media, like an external USB hard drive and your computer, so you have ready access to it if something breaks.

(1) store at least 1 copy of your information somewhere else, not in the same location as the other two. Several cloud data services offer the option to do this and look after the encryption for you. Most of the others can store data you encrypt before uploading.

Learn More

Several of the links above are to resources from the Electronic Frontier Foundation's Surveillance Self Defence project. To learn more about each of these steps and other things you can do, have look here; https://ssd.eff.org/

There is a thorough piece about preparing to attend a protest that should be essential reading for everyone, particularly in the midst of the current attacks on protests governments around Australia are engaged in.

A word about Windows

The professional and business versions of Windows include Microsoft's Bitlocker to encrypt your data, but the cheaper home version does not. There is software available to encrypt data on your Windows home system. A tool like VeraCrypt can do this, alternatively services like Sync and NordLocker can both encrypt data on your device and back it up to cloud storage.

Recent versions of Windows send considerable amounts of data back to Microsoft. The bulk of this is to enable advanced features on your computer, but if you want to prevent this from happening there are programs you can use to reduce what is sent and lower the demands on your machine.

Encrypted alternatives to 'free' programs

The steps above can be applied regardless of hardware or software. It is crucial to remember that security vulnerabilities and solutions constantly evolve. That is why it is essential that devices and programs are kept updated, and why any solutions you implement should be re-evaluated regularly.

Everyday services like documents, messaging, and email have long been provided by tech giants. These apps are provided with little or no fee and a user friendly interface, all while recording and monetising your information.

By the end of 2023, secure encrypted alternatives largely caught up. No-cost plans for applications with familiar, user-friendly interfaces and the functionality you need, and that keep your information secure, were readily available.

The best of these services are open source and available to be audited so that external experts can evaluate the software and confirm the security capabilities are as advertised. Look for 'end-to-end' encryption, that is the content of your communication is encrypted before it leaves your device, and only decrypted by the intended recipient once it is on their device.

As with any communication, the 'signal chain' is only as secure as its weakest link; if the recipient's device is not up to date and easily hacked, or they leave their device unlocked and able to be read, encrypted applications are useless. Ensure user behaviour and habits are secure before you implement any new platforms.

Every software platform is subject to the laws of the country it operates from. If your security needs extend to needing to know this level of detail—if in your security needs assessment it emerges that may you need to secure against government information demands or surveillance agencies—seek independent expert advice!

Voice calls, Video and Instant Messaging

Regular SMS or MMS messages can be read by anyone along the signal chain, that is every system or service the message passes through, from your device through your ISP or telco to the recipients ISP or telco to their device.

Some companies claim some of their applications are end-to-end encrypted, but do not make them available for audit, or the applications are offered by companies that are built on information extraction such as Facebook or Google. You don't need to risk it when there are better alternatives.

The most commonly recommended instant messaging platform, for all the reasons outlined above, is Signal. It works for individual and group chats, photo sharing and video calls. Wire is another excellent and arguably more private option because it does not require a phone number to register. Wire also offers additional functionality on a paid plan.

These apps can be set up to automatically delete messages, which is an essential feature to implement if you communicate about actions that could lead to your device being seized.

Email, Contacts and Calendars

One of the oldest mechanisms of online communication used to be one of the most arduous to secure. The older methods used to encrypt email traffic are still applicable, though they're now more user friendly than they once were. You can read about how to use PGP encryption with the Thunderbird email program here.

Much more user friendly options are available, but are only effective if both the sender and receiver are using the same platform. Tuta is a good choice, it includes contacts and calendar functions, and they also have committed to using green energy. Paid plans allow for a secure form to be placed on your website so supporters or whistleblowers can share their stories securely and anonymously.

ProtonMail and Skiff both offer this type of secure email, contacts and calendar, along with some other functions.

Documents

Tools like Google Docs and Office 365 are enormously popular for remote work and collaboration, and it has taken a long time for secure alternatives that are easy to use to become available.

Proton , Sync, Nord and others offer encrypted cloud storage—some along with excellent VPN options—while Skiff was the first web app to take the next step and offer secure document collaboration. These platforms can all be installed on mobile devices as well as computers, and are adding new features rapidly, so have a look and see if they meet your needs.

Self-hosting

Depending on your security requirements—and the capacity of your campaign—another option is hosting your own platform for all of these functions. A platform like NextCloud can be hosted on any web server, and provide chat, communication, contact management, collaboration and more. Files on the platform can be encrypted and secured behind 2FA logins.

Choosing the right tools

There will always be a trade-off. Cutting-edge features will always come to the platforms that profit from them first. The explosion in AI will dramatically change the way digital tools are used, while the demand for platforms that offer a range of features AND privacy is still very low. Advocacy and change-making necessitates using the social platforms our audiences use; we can only reach people where they are. But our internal planning and organising should be kept secure, we need only look at the nationwide crackdown on protest to see how important this is.

Making ethical technology choices is a complicated challenge. The best we can do is inform ourselves, and protect ourselves, our work and our supporters.

Anytime we have the choice, we should use platforms and services that share or support our values.