4.

PROTECT YOUR VIRTUAL VALUABLES

Just as you take care of the valuable items in your home, you should do the same for the information you're storing virtually — whether it's your financial records, scans of your passport, or even your address or phone number, it's worth thinking about where you're storing **your most valuable personal data**, and how you can protect it.

A **spot clean** is great if you want to make a few quick improvements over coffee. Search for specific information that's sitting in your email or other accounts and delete it: scans of your ID, bank details, or your health insurance info, to name a few. If it's something you'll need later on, you can always download it or print it out before erasing it from your email account.

A **deep clean** is more thorough, and is good to do once a year. Archive everything in your email or social media account, download it to your computer, and delete the account contents to start fresh.

Tip: Don't just delete — also empty your trash bin and temporary files!

It's up to you whether you'd like to back up your archives and documents to a cloud or save it to an external hard drive or USB stick. No matter how you save, make sure that you won't lose it, it has a strong password and makes sense for you.

5.

PASS IT ON

While it might be easy to forget, the web is called a "web" for a reason. We're all connected online through different networks, not only as "friends" on social media, but also through the contacts in our email accounts and the photos we share online. When you secure your accounts, strengthen your passwords and clean out your data, it's not only you who benefits — everyone you're connected to is made a little bit safer by your effort.

When you're cleaning out your email and social media accounts, consider what else you can download and delete that might help your friends or co-workers: your sister's bank details, the key code to your office or that scan of your son's passport are just a few of the records that could cause a headache if they were to get into the wrong hands.

Pass it on! Increasing your digital security can be as simple as following a few basic steps. Share this Data Detox with your friends, family or co-workers, to help them change their habits in ways that make sense for them.

DATA DETOX KIT

SHIFT YOUR SETTINGS

to secure your data

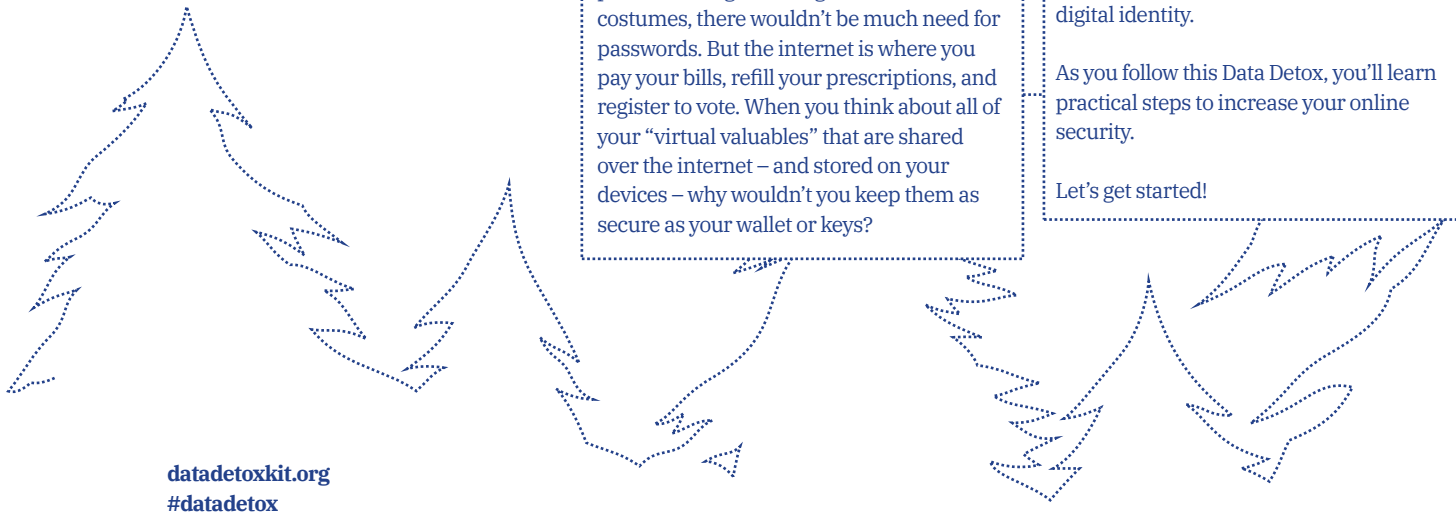
If the internet were just a place for sharing pictures of dogs wearing dinosaur costumes, there wouldn't be much need for passwords. But the internet is where you pay your bills, refill your prescriptions, and register to vote. When you think about all of your "virtual valuables" that are shared over the internet – and stored on your devices – why wouldn't you keep them as secure as your wallet or keys?

There's one simple way to make it harder for others to access your virtual valuables: don't make it easy for them to guess your passwords. Most people don't need specialised technical skills to get into your accounts – they can do it just by making a few guesses at your passwords or running an automated program.

And once they're able to get into one account, they can try that compromised password on other accounts, gather information about you and your habits, take over accounts you own or even use your digital identity.

As you follow this Data Detox, you'll learn practical steps to increase your online security.

Let's get started!



A product of
TACTICAL TECH

Supported by
Firefox

datadetoxkit.org
#datadetox

1.

LOCK YOUR DIGITAL DOOR

Screen locks: the password, pattern, fingerprint or face ID you use to access your device are some of your best defences against someone who might want to get into your device. But there are lots of different kinds out there and it might be hard to know which one is right for you.

Having any lock on your phone, tablet, or computer gives you more protection than no lock at all. And just like the different types of locks you might put on your doors, some screen locks are stronger than others.

Of all the locks out there, long, unique passwords are the strongest. That means if you unlock your device with a password, it should include **letters, numbers and special characters.**

Let's say you're using a basic swipe to open your phone. You can slowly bump up your security by setting up a long password. Or do you use a pattern lock now? How about making your pattern longer? Use 1234 as your PIN? How about rolling some dice seven times and memorising that PIN instead? **A little change can go a long way towards keeping control of your devices.**

2.

LET THE RIGHT ONE IN

Creating top-notch passwords is easy. All you have to do is follow a few basic principles. Your passwords should be:

Long: **passwords should be a minimum of eight characters. Even better? 16-20 characters.**

Unique: **each password you use – for every site – should be different.**

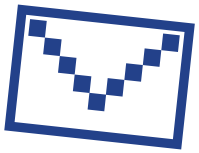
Random: **your password shouldn't follow a logical pattern or be easy to guess. This is where password managers become very helpful.**

The strongest of passwords use a combination of letters, numbers and special symbols. This time-honoured advice still makes for a stronger, harder-to-guess password. Some password systems unfortunately don't let you use special symbols (like @#$%-=+), but along-enough combination of letters and numbers is still better than a short one.

Ideally, you should use a **dedicated password manager** to generate and store all your passwords. A password manager — like 1Password and KeePassXC, the ones often recommended by security experts — is basically an app whose sole purpose is to protect your login credentials and other sensitive data.

3.

ADD A SECOND KEY



Setting up two-factor authentication (2FA) or multi-factor authentication (MFA) means that even if someone finds your password, they probably won't have the additional factor they need to get in.

Take a look through the security settings of your most-used sites and apps to see if you can **set up this extra key**. Start with the most important ones — any finance apps, or services like email, which you use to recover your other accounts.

Google:
Sign in to: myaccount.google.com →
Security →
2-Step Verification →
Get Started

Facebook:
Menu →
Settings →
Security and Login →
Use Two-factor Authentication

Tip: When setting up a next layer of verification, you'll need to select a second way of confirming it's you. Try to avoid using SMS (text messages sent to your phone number) as your second factor, just in case you lose your phone. Email is usually a more reliable option.