4.

REDUCE YOUR TRACES

The browser on your phone stores a lot of information about you – your location, what you search for, which websites you use – and may give that information away. You can regain some control of that info by making a few changes.

Phones, tablets and computers tend to come pre-installed with browsers that don't prioritise your privacy. Instead, you can download and use a browser that already keeps your web activity more private by default, shielding you from trackers.

And for some added privacy boosters, you can install extras known as "add-ons and extensions" (these are easy-to-install mini-programs for your browser that can make your online activity more private).

5.

UNTAG YOURSELF AND OTHERS

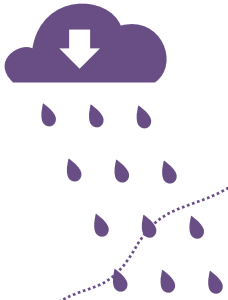
Have you contributed to your friends' data build-up by tagging them in photos and posts in the past?

Lighten their data load (and your conscience in the process) by untagging them in as many photos and posts as you can.

Pass it on! Encourage your friends, family and co-workers to join you in controlling fly-away data. If we all work together to control our data traces, we can better help each other detox.

To block spying ads and invisible trackers, install uBlock Origin (for Chrome, Safari and Firefox) or Privacy Badger (for Chrome, Firefox and Opera).

To make sure your connections to websites are secure where possible, install HTTPS Everywhere: a browser extension that ensures that your communication with many major websites is encrypted and protected in transit. If you're a Safari user who'd like this feature, set your default search engine to a non-Google product like DuckDuckGo, which redirects you to encrypted connections automatically.



DATA DETOX KIT

CONTROL YOUR SMARTPHONE DATA

to increase your online privacy

If you think about what your data tells others about you, it may not seem like that big of a deal: who cares if you're a fan of country music, like to buy more shoes than you need or start planning your next vacation a year in advance?

The problem lies in what's happening with your data. Taken together over time, intimate digital patterns emerge: your habits, movements, relationships, preferences, beliefs and secrets are revealed to those who analyse and profit from them, like businesses and data brokers.

As you follow this Data Detox, you'll get a glimpse into how and why this is all happening and take practical steps to control your data traces across the internet.

Let's get started!

A product of TACTICAL TECH

Supported by Firefox

datadetoxkit.org
#datadetox

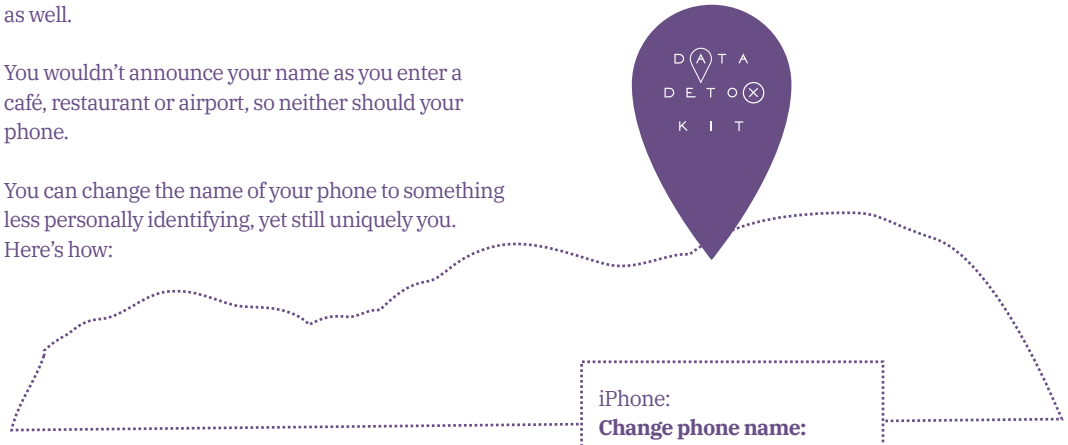
1.

CHANGE YOUR DEVICE NAME

At some point, you may have "named" your phone for Wi-Fi, Bluetooth or both – or maybe the name was automatically generated during setup. This means that "Alex Chung's Phone" is what's visible to the Wi-Fi network owner and, if your Bluetooth is turned on, to everyone in the area who has their Bluetooth on as well.

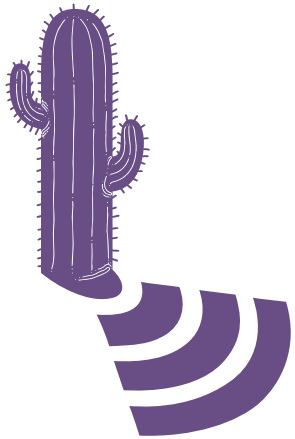
You wouldn't announce your name as you enter a café, restaurant or airport, so neither should your phone.

You can change the name of your phone to something less personally identifying, yet still uniquely you. Here's how:



iPhone:
Change phone name:
Settings → General →
About → Change the name

Android:
Change Wi-Fi name:
Settings →
Wi-Fi → Menu →
Advanced / More features →
Wi-Fi Direct →
Rename Device
Change Bluetooth name:
Settings → Bluetooth →
Turn Bluetooth on
if it's off → Menu →
Rename Device →
Turn Bluetooth off



2.

CLEAR YOUR LOCATION FOOTPRINTS

While it may seem like your location data are just random bits of information, when they're seen all together, they could reveal important details about you and your habits, like where you live, where you work and where you like to hang out with your friends. That's what makes it highly sought-after by many companies and data brokers.

You can go through each app's permissions and turn off the location services. Look for the apps that don't actually need it for the service (does that game really need to know where you are?) and for the ones who you don't want to have it:

Android:
Settings →Apps → Manage location access on a per-app basis

iPhone:
Settings →Privacy →Location services →Manage location access on a per-app basis

3.

TIDY UP YOUR APPS

Your social media apps, games and weather apps are interested in your data ... and they may be collecting quite a lot of it.

Getting rid of those random apps on your phone that you never use can be a powerful way to detox your digital self.

Plus, tidying up can also free up space on your phone, decrease data use and increase battery life.

Android:
Settings → Apps →
Select the app you want to uninstall → Uninstall

iPhone:
Press down on one app until they all start wiggling and small crosses appear in the top left corner of each app.

To delete an app, tap the small cross of that app.

To return to normal, press the home button.

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

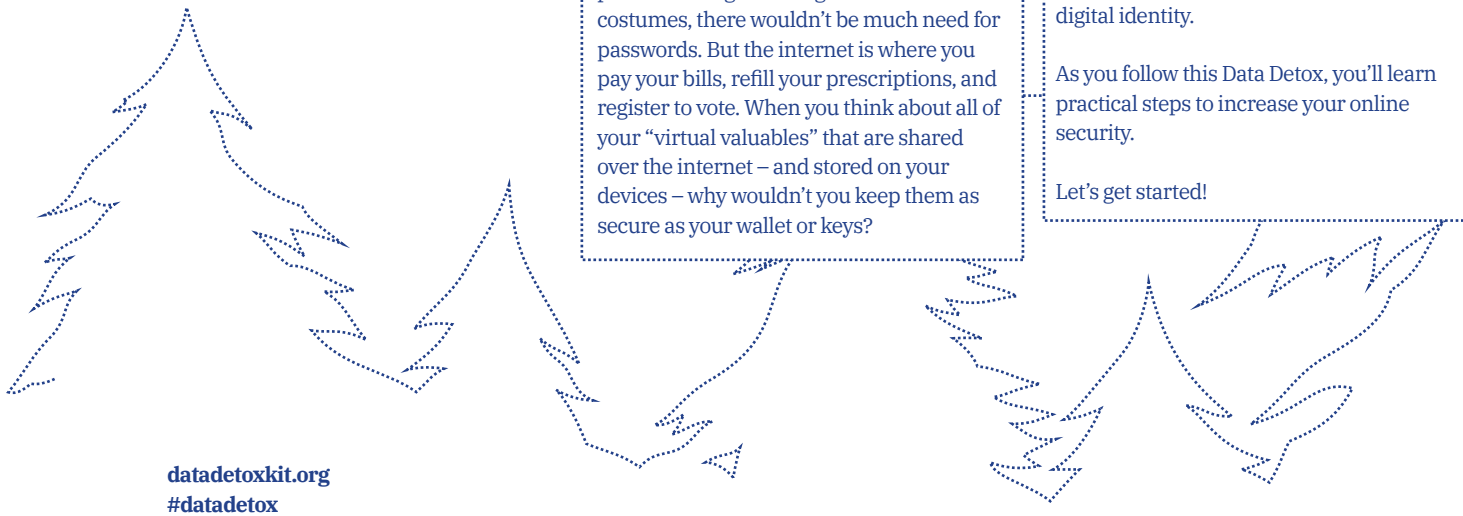
If the internet were just a place for sharing pictures of dogs wearing dinosaur costumes, there wouldn't be much need for passwords. But the internet is where you pay your bills, refill your prescriptions, and register to vote. When you think about all of your "virtual valuables" that are shared over 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.**

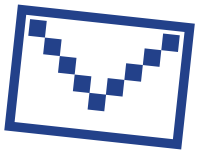
Random: **your password shouldn't follow a logical pattern or be easy to guess. This is where password managers become very helpful.**

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.

4.

MAKE YOURSELF HEARD

If you aren't happy with the addictive or persuasive designs or misinformation on websites you frequent or apps you use, you can send emails, write tweets and let companies know that you don't agree with their practices. When companies are pressured to take action by their most valuable assets –their users – there's a chance they might change.

If you don't feel like your feedback is being heard, there's something really powerful you can do: use a different website or app. If you've communicated that you're unhappy with something a website or app is doing and then actually stop using it or uninstall it – and enough people do it – **they'll notice.**

5.

SPREAD THE WORD

Pass it on! This is an easy tip to forget, but it can have a big effect. Tell your friends, family and co-workers about the things you're noticing, and even ask them to join you in this detox! Everyone struggles with managing their phone habits. What's important is that you find a way that feels right for you and suits your lifestyle. Experiment until you find the right fit, then update your habits as your needs change over time. There's no one-size-fits-all solution.

And finally, communicate your tech choices with those around you. Let's say you'll be unreachable on your messenger app everyday after 8pm because that's when you'll start your screen-free routine: tell your family and friends so they can call you instead. Keep the dialogue open, ask questions and you can live a balanced online life that suits you.

DATA DETOX KIT

ESCAPE THE DEFAULTS

to enhance your digital wellbeing

When was the last time you "unplugged" and didn't touch technology for a day, or even just an hour? If you're constantly online, you're not alone. How can you make sure that time on your device is quality time?

It starts with knowing that the irresistible pull toward your tech isn't your fault! Believe it or not, your favourite apps and websites are designed so that every feature, colour and sound has been 'optimised' to keep you hooked, sold and coming back for more.

Want to find a healthier balance between your online life and your offline one? That's what this part of the Data Detox is all about.

Let's get started!

A product of TACTICAL TECH

Supported by Firefox

datadetoxkit.org
#datadetox

1.

BE PRESENT IN THE MOMENT

This tip is tougher than it sounds. Staying in the moment requires daily practice. It's like a muscle in your brain you need to train regularly in order to build up its strength. You can start by noticing your relationship with the technology you use.

How much time do you spend on your phone?

If you're unhappy with the answer, there are settings and strategies you can follow to gain control of your tech use.

If your goal is to spend less time on Facebook, Instagram or Snapchat, change the settings and permissions of those apps to make them work better for you.

Some apps like Instagram even have an option where the app gently reminds you when you've reached your daily time limit.

Instagram:
Profile → Menu → Settings → Account → Your Activity → Set Daily Reminder

If you find that your phone disrupts your real-life conversations with rings, buzzes or flashes, you can silence it temporarily, put it face down or even tuck it away in your pocket or bag so it's out of your eye line.

2.

SPOT THE DESIGN TRICKS

Persuasive design, also known as "dark patterns," are designs based on human psychology that are used to provoke you into signing up for something, buying something or giving away more personal information than you thought or intended.

Common design nudges may include the use of particular colours, placement of buttons, unclear texts or incomplete information. Sometimes these tricks are obvious, but other times they're harder to spot. You might have already noticed some of these when signing up for a subscription or shopping online. The reason you see these design tricks everywhere is because they work – they get us to click, subscribe, buy more often and keep coming back. The more you're aware of the subtle prompts and manipulations embedded in the websites you use, the more savvy and informed you'll become.

There are a number of things you can do to outsmart your apps.

Recognise when you're being nudged: The first thing you can do is simply be aware of the use of these techniques.

Screenshot and share: Take screenshots anytime you encounter persuasive designs online and share them with your friends (omitting any personally identifiable details – privacy first!). You can also ask companies to change their practices.

Stay calm: If there's a countdown clock on a purchase page, ask yourself, "Is this really urgent?" If you find yourself clicking a button when you didn't really want to, think about the wording on the buttons or the colours used by the service. If you feel confused, don't immediately assume you're at fault — consider the words used by the website or app, as they might be unclear.

3.

STAY MEDIA SAVVY

Just as you can learn to outsmart the features and designs that are meant to keep you scrolling and clicking, you can also get smart about spotting news items or posts that are meant to mislead you.

By now you've probably heard about the problems of 'misinformation' and 'fake news'. You can get wise to misinformation if you make it a habit to ask critical questions of any news you consume, especially if it seems surprising, outrageous or too good to be true.

In the end, you'll want to verify which news is real or fake – especially if you plan to share it with family or friends.

What website is this from?
Who wrote it (and when)?
What does the whole article say, beyond the headline?
Which sources are they referring to?

If you think it's misinformation and want to stop it from spreading, most platforms have a place where you can report the posting. You may also want to decide whether or not to continue following the account that published it.

5.

SEEK THE TRUTH ON THE INTERNET

The term “fake news” is used to refer to a wide range of inaccurate or misleading information, including satire, poorly researched or unverified content, hoaxes and scams. Fake news isn’t always spread maliciously, but regardless of the reason behind why it’s shared, the result is generally the same: people on the receiving end believe that something wrong is actually right, or that something happened that never did.

At best, it may be a humorous meme. At worst, it might be inaccurate health information or false political information.

Even with your best efforts to investigate and ask critical questions of the articles you read, it may still leave you feeling confused. But know this: you’re not alone!

All Hands on Deck
Just because a website doesn’t acknowledge their mistakes, it doesn’t mean they don’t make them. In fact, the most reliable publications are those that are extra careful with the truth, and employ people or entire departments whose sole job it is to fact-check.

Look for sources that issue corrections when they’re wrong. Even better is when the update is summarised right at the top of the article and shared on social media, so you don’t need to search too hard for it.

6.

BURST YOUR FILTER BUBBLE

After websites and apps build a profile of what your interests are, you might find yourself in a filter bubble. This is when services feed you more stories like the ones you’re already clicking on. How does that limit or change what you hear about?

Being in a filter bubble can cause people to see completely different stories, news headlines, articles and advertisements, as demonstrated in the interactive article Blue Feed, Red Feed (graphics.wsj.com/blue-feed-red-feed).

If you know you’re viewing algorithmically curated content designed specifically for you across your apps and websites, the question is: how can you step outside of your filter bubble?

Change the Winds and Mix Up Your News
A good way to burst your filter bubble is to subscribe to services that aggregate news and information from a variety of sources and with a diverse pool of perspectives. RSS feeds, forums and mailing lists that exercise a broad range of opinions and themes may help you see outside of your bubble. Global Voices (globalvoices.org) and The Syllabus (the-syllabus.com) are great options to start with.

DATA DETOX KIT

6 TIPS TO STEER CLEAR OF MISINFORMATION ONLINE

Apps, websites, and online media can be essential for accessing news, life hacks and entertainment. But amidst all that content, it can be tough to navigate the distractions to find what you’re really looking for.

What’s more, it can be hard to tell the difference between fact and fiction when you encounter a video, picture or article online.

From personality quizzes that try to profile you to shocking headlines and altered photos or videos that can convince you of a completely different reality, what you see online is not always what it seems.

In this Data Detox, you’ll explore misinformation-related topics and buzzwords, starting with a close-up look at your responsibility and then exploring the bigger picture, while getting advice on how to find your way through what’s out there.

Let’s go!

datadetoxkit.org **#datadetox**

A product of TACTICAL TECH

Project partners
Save the Children 100 ANNI
IFLA

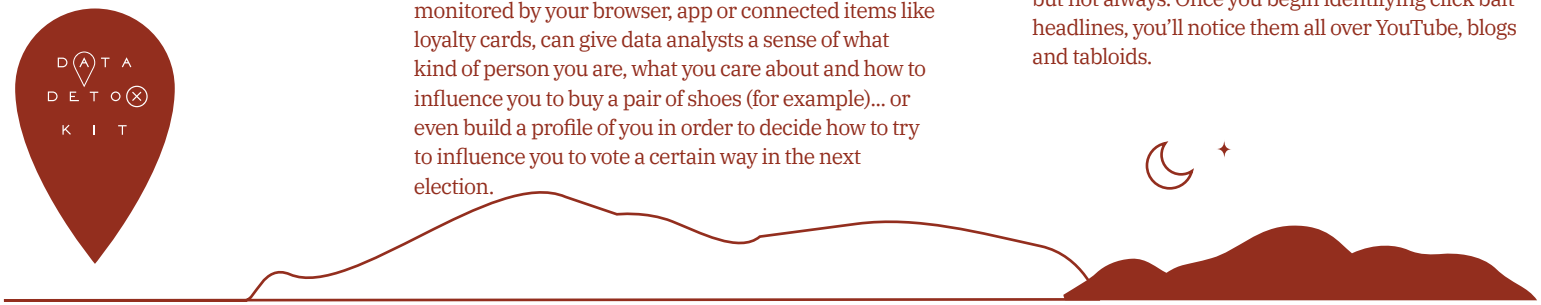
Funded by the European Union

1.

REALISE YOUR POWER TO MAKE WAVES

Liking, sharing, retweeting, reposting – these actions all describe how you interact with what you see online – and your interactions make a big difference. When enough people engage with a picture, video or post, it spreads rapidly, by definition becoming 'viral'.

Take a moment to ask yourself: "What's my influence online?" When was the last time you saw a shocking or funny article, headline, video or image, and within seconds you had already forwarded it to your friends? Researchers have found that the stories and images most likely to go viral are those that make you feel fearful, disgusted, in awe, angry or anxious. If this is something you did just this morning, don't feel bad!



Sharing Is Caring
Sharing is a form of participation. When you share something (anything), you're playing a part in the chance that it might go viral. If it turns out to be a fake, for example, do you really want your name and reputation attached to it? Before you share a link, consider whether you might be spreading something untrue, destructive or toxic.

2.

THINK TWICE BEFORE TAKING THAT PERSONALITY TEST

When was the last time you saw a quiz (either in text or photo filters) called something like:

- Which decade are you?
- What is your spirit animal?
- What is your perfect vacation?
- ... the list goes on!

While there's a chance this was a fun quiz designed to get you to engage, it's also possible that the questions were carefully crafted to collect data in order to categorise your personality, based on so-called psychometric patterns.

Your answers to a quiz like "Which Simpsons character are you?," along with your other habits that might be monitored by your browser, app or connected items like loyalty cards, can give data analysts a sense of what kind of person you are, what you care about and how to influence you to buy a pair of shoes (for example)... or even build a profile of you in order to decide how to try to influence you to vote a certain way in the next election.

Keep More Secrets
When you think of private information, your passwords, identification number and bank account number might be the first things to jump to your mind. But details about you such as what scares you, what annoys you and your ambitions are just as personal. These details can be considered valuable by data analysts, shedding light on what makes you tick as a person. Think twice before giving away that kind of information in a survey or a quiz.

3.

DON'T TAKE THE BAIT

Click bait is a term used to describe sensationalist, dishonest or made-up headlines used with the intent to provoke people to click on the headline or link. The more attention an article, video or image receives, the more money it's likely to earn. That means there's a motivation for creators to say anything it takes to get you to click on or share their content.

Based on the personality profile built about you by the platforms you use (like Facebook and Instagram), you may get customised headlines that have been created to trigger your emotions in a way that's most likely to get you to click.

Click bait may be found alongside misinformation, but not always. Once you begin identifying click bait headlines, you'll notice them all over YouTube, blogs and tabloids.

Get to the Source
When faced with click bait, don't stop at the headline. If it looks like a secure link, click into the article and find out who the author is, when it was published and which sources it's referring to. It could be that inside the article, there's a note that it's paid content or an advertisement, or maybe it's categorised as an opinion piece. These details can help you decide whether it's worth your energy.

4.

WATCH OUT FOR FAKES

Deep fakes are videos, audio clips or pictures that have been digitally altered, typically to replace someone's face or movements or to alter their words. While "deep fakes" is a recent term, they have actually been around in one form or another for ages. It's even easier to create so-called **cheap fakes** – misleading content that doesn't require sophisticated technology, but instead can be created by simply putting the wrong headline on a photo or video, or using outdated content to illustrate a current event.

It might seem impossible to truly combat fakes, but there is something key you can do ... stay anchored.

Stay Anchored and Explore
Just like when you're dealing with click bait, don't accept something at face value. If a video or photo you've seen seems surprising or outrageous, recognise that feeling and consider there might be more than meets the eye. Otherwise, if you notice the same image is filling up your feed or has been shared with you multiple times, recognise that as a possible reason to get to the real source.

That's when you'll want to ask more questions: who published it (which website, who was the author)? When was it published? If it's an image, do a reverse image search on TinEye (tineye.com) and see where else you find it.

Cross-check other credible news sources before you consider it to be true and before you share it with your friends and family.