Browser security

Browsers contain lots of **your** private information

Many browsers collect information about you:

Browsing history - all the websites you visit
Login credentials - usernames and passwords
Cookies and trackers - these are placed on your browser by the sites you visit and can follow you from site to site
Autofill information - names, addresses, phone numbers, etc.

Private or incognito browsing can help with some of these, but **your activities can still be tracked** – Bloomberg

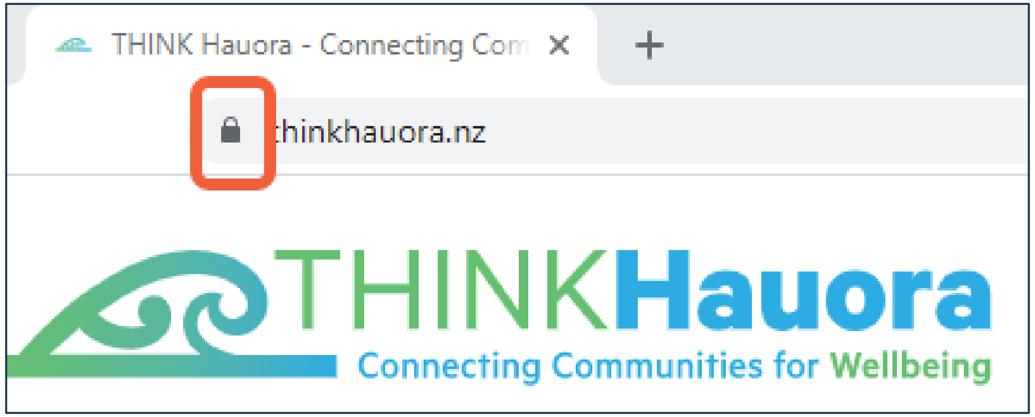
Do this **Practice good cyber hygiene**

+ **Install and apply** updates as soon as convenient
+ **Enable** safe browsing features if available (Google your favourite browser to see how)
+ **Pay attention** to browser warnings about password breaches and unsafe sites
+ **Use** different browsers for personal and business activities (don’t log into your personal GMail in the same browser as you are logged into INDICI or MedTech)

Look for the little 🔒 in the address bar

✓ Do this

Check for the padlock before you give out confidential information like patient data or your credit card!



THINK Hauora - Connecting Com × +

🔒 thinkhauora.nz

THINKHauora

Connecting Communities for Wellbeing

Sites that have an SSL security certificate have an ‘s’ and a padlock

No security certificate means that the connection between you and the website is **not secure** and your information could be stolen.

✓ Do this

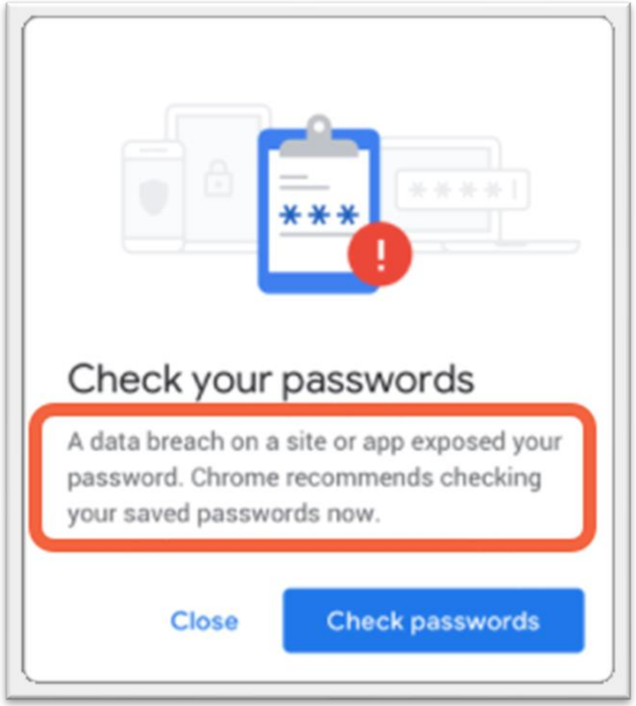
Before you click a link in an email

Look for the ‘s’ in the hyperlink

https:// = connection **secure**

http:// = connection **not secure**

Saving passwords in your browser



Check your passwords

A data breach on a site or app exposed your password. Chrome recommends checking your saved passwords now.

👍 **Convenience** – all your passwords are filled in automatically across all your devices

👍 **Easy unique passwords** – it's easy to use unique passwords when you don't have to remember them all

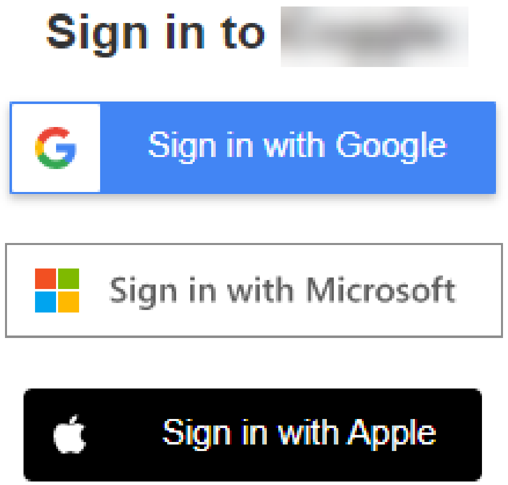
👍 **Monitoring** – Chrome will notify you if your passwords have shown up in a data breach and encourage you to change them

👎 **House of cards** – if your browser or the browser company gets hacked **all of your accounts** are vulnerable

✓ Do this

If you choose to save passwords in your browser, **pay attention to warnings about data breaches** and change any passwords impacted OR consider using a password manager

Sign in with…



Sign in to [redacted]

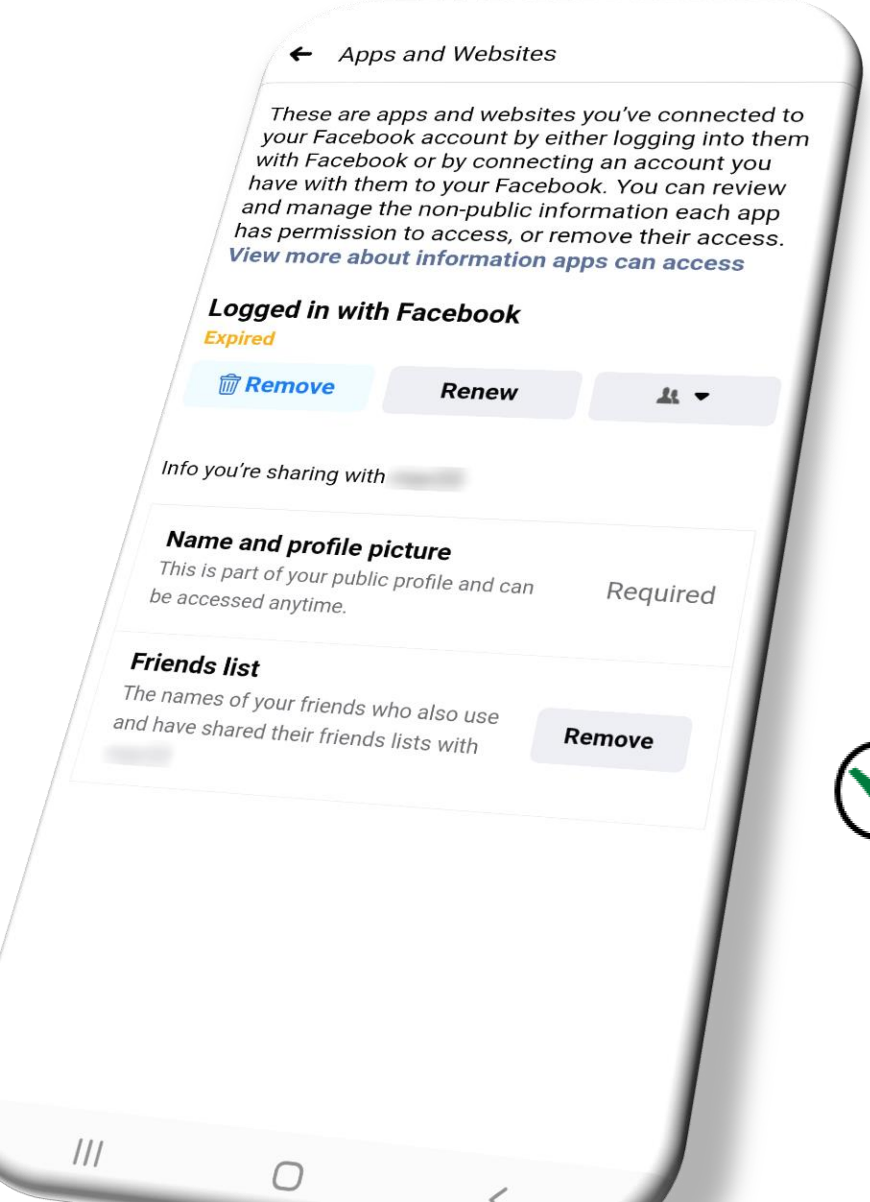
👍 **Convenience** – You only need one password for all your accounts

👍 **Trust** – you aren't giving away your data to strangers as all your data and access is managed by one provider

👎 **House of cards** – if the one account you are using to log into all the other accounts or that company gets hacked **all of your accounts** are vulnerable

✓ Do this **Regularly audit** what information your delegated logins are sharing with other websites

Audit your delegated logins



Apps and Websites

These are apps and websites you've connected to your Facebook account by either logging into them with Facebook or by connecting an account you have with them to your Facebook. You can review and manage the non-public information each app has permission to access, or remove their access. View more about information apps can access

Logged in with Facebook

Expired

Info you're sharing with [redacted]

Name and profile picture
This is part of your public profile and can be accessed anytime. — Required

Friends list
The names of your friends who also use and have shared their friends lists with [redacted]

When you use Facebook or Google to log into a 3rd party app – information from your profile may also be shared.

facebook Google

Google other services such as Microsoft or Apple ID for instructions

✓ Do this

Delete access to any apps you no longer use

Restrict access to required information only

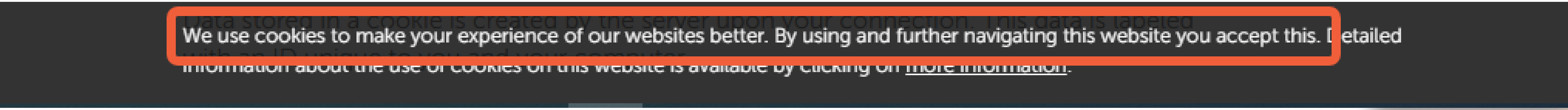
Think carefully about where you have saved your credit card details

Cookies can’t be bad for me, can they?

Cookies personalise your online experience and hold information like whether you are logged in or what items you have in your shopping cart

Cookies themselves aren’t bad, but they can be a risk because they hold information about you

Data stored in a cookie is created by the server upon your connection. This data is labeled with an ID unique to you and your computer.



We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

Cookies may be saved on your computer **without you ever clicking on anything**

You probably have hundreds of cookies (the computer kind) stored on your computer

Do this **Clean out your cookies** often to reduce the risk

Go to the settings menu in your browser and look for cookies

Cleaning out cookies in Chrome & Edge

In Google Chrome

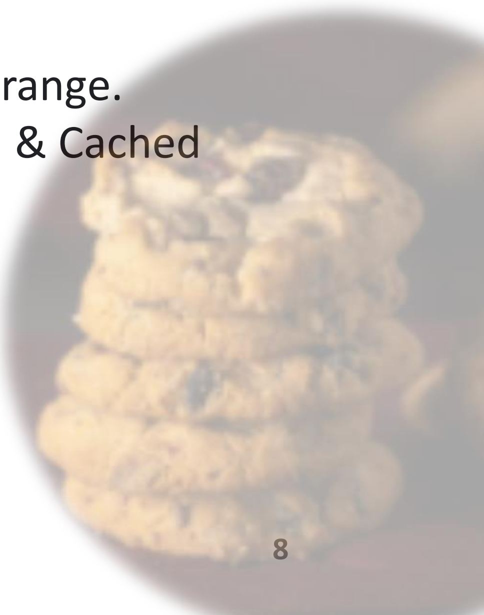
1. **Open** Chrome
2. At the top right, **click** ⋮
3. **Click** More tools → Clear browsing data…
4. **Choose** a time range. To delete everything, **select** All time
5. **Check** the boxes next to Cookies and other site data & Cached images and files
6. **Click** Clear data

(process on August 2021)

In Microsoft Edge

1. **Open** Microsoft Edge
2. At the top right, **click** ···
3. **Click** Settings
4. **Click** Privacy, search, and services
5. Under Clear browsing data, **select** Choose what to clear.
6. Under Time range, **choose** a time range.
7. **Select** Cookies and other site data & Cached images and files
8. **Click** Clear now

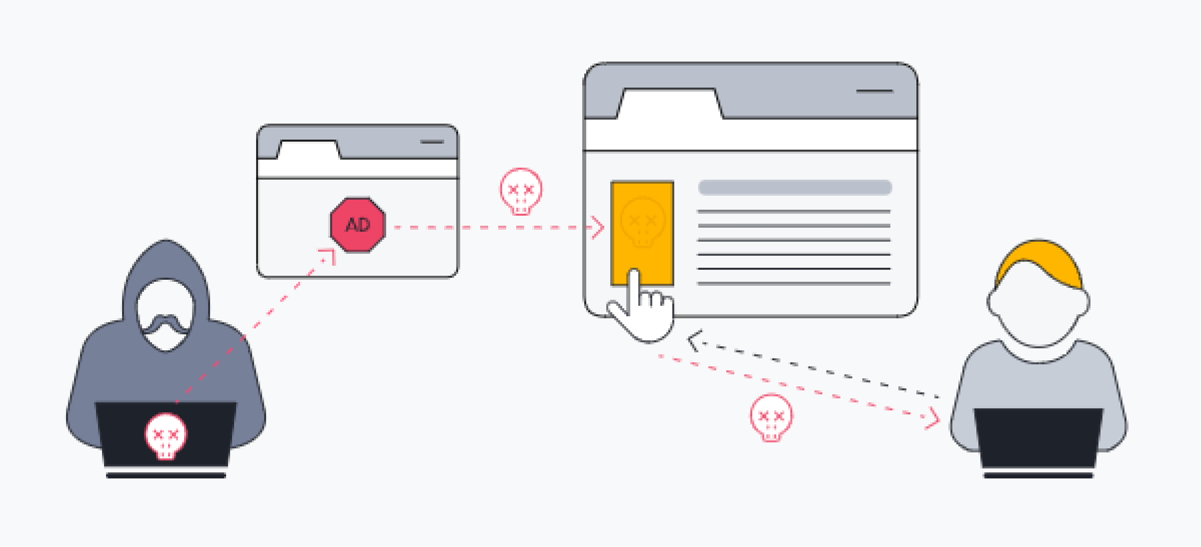
(process on August 2021)



Consider getting an ad blocker

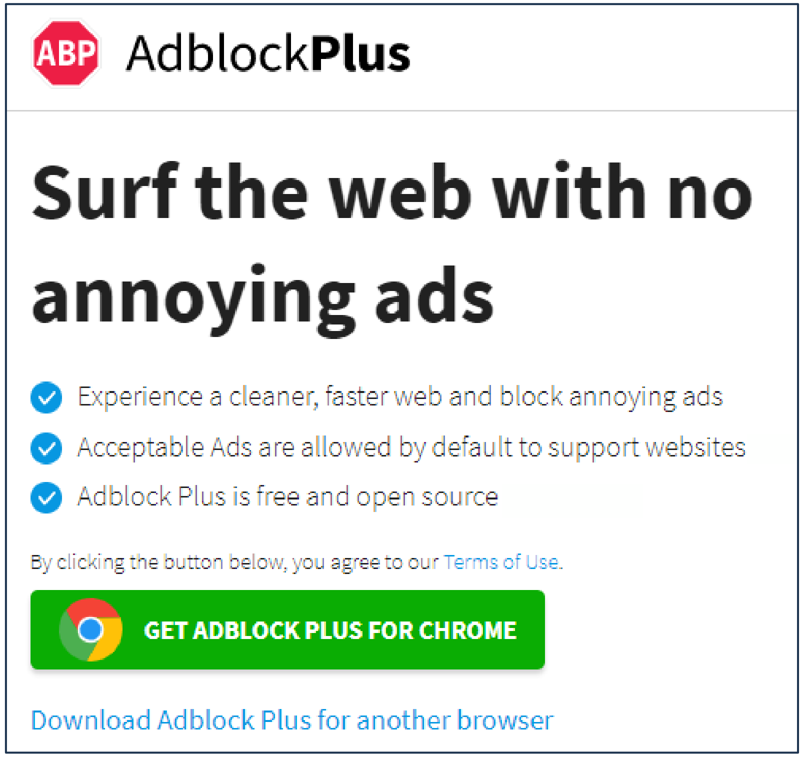
Trusted websites may contain malicious ads that can harm your computer and your data without you ever clicking on the ad – CSO

Stop the adverts before they get to your browser by using an ad blocker



Malvertising attacks use legitimate online advertising networks to spread malware. - AVG

AdblockPlus is free and does the job



AdblockPlus

Surf the web with no annoying ads

- ✓ Experience a cleaner, faster web and block annoying ads
- ✓ Acceptable Ads are allowed by default to support websites
- ✓ Adblock Plus is free and open source

By clicking the button below, you agree to our Terms of Use.

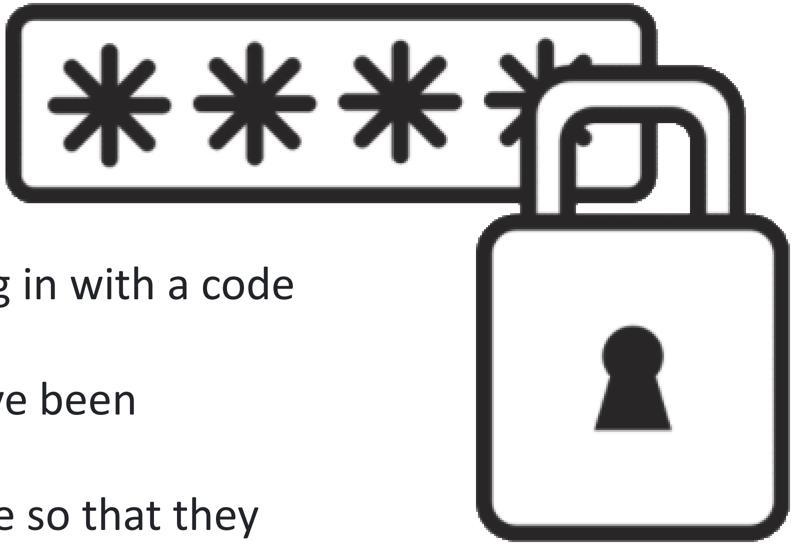
GET ADBLOCK PLUS FOR CHROME
Download Adblock Plus for another browser

Turn off on sites like your PMS to allow pop up windows to function correctly

Consider getting a password manager

It is difficult to use unique passwords for every online account but "using one password everywhere means that if just one site you use gets hacked, an attacker potentially has the password that unlocks your entire online life."

- The Verge



Make sure that your password manager has:

✓ **2-Factor Authentication** - requires you to authenticate any log in with a code sent to your phone

✓ **Password Flagging** – informs you if any of your passwords have been compromised in a data breach

✓ **Encryption** – the passwords are kept in an encrypted database so that they are secure if the company gets hacked

✓ **Backup and recovery** – you won't lose access to your data if there's a problem

THINKHauora

Connecting Communities for Wellbeing