Protecting your privacy in the digital age

Privacy Commissioner
Te Mana Mātāpono Matatapu

www.privacy.org.nz

Insights Report June 2023

Introduction

New Zealanders love the internet and each time we buy products, check social media, or complete internet banking transactions our personal information is being recorded online. It's then being used and often sold in various ways you don't know about. If someone's personal information is shared or accessed online without their permission, it's nearly impossible to regain control of what happens to it – what it's used for, how it's processed and by whom.

You have a right to privacy online. The Office of the Privacy Commissioner has a role in helping protect New Zealander's personal information, even when they're online.

In this report we will show you how the digital transformation of society is challenging privacy, and you will learn some tips about ways of keeping your data safe online.

As use of the internet in New Zealand and the world increases (96 percent of the population of NZ has readily available access to the internet[1]), our dependence on the internet increases too.

Our dependence is influenced by the world around us – like shops buying and selling things online or having the convenience of having an automatic robot vacuum cleaner attached to your Wi-Fi, or the fact that government processes are being moved online. As the world around us goes more online, we adapt.

1 Source: Digital NZ 2023, DataReportal

However, one of the downsides of this digital change can be seen by the fact that more than 60% of serious privacy breaches reported to the Office of the Privacy Commissioner (OPC) are happening in the digital world.

This is reflected in the top six concerns for New Zealanders using the internet, as found in InternetNZ's 2022 annual survey. These concerns include 'security of personal data', 'threats to privacy', and 'identity theft'.

Add to that the threat of cybercrime. According to Cert NZ, New Zealand's cyber security agency, the numbers for scams and related financial losses reached an all-time high in 2022.

All of this shows why it pays to be vigilant and there are simple steps you can take to protect yourself.

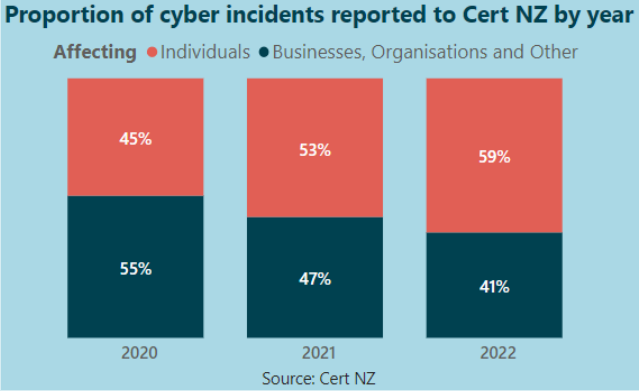
Insight 1

Scams and frauds are increasing, but you can protect yourself

More and more New Zealanders are being scammed and defrauded than ever before. People are losing more money as scammers get bolder and more creative about ways to scam the public.

Last year, the top three types of cybercrimes that affected New Zealanders were:

- Scams and fraud
- Phishing and credential harvesting
- Unauthorised access.



NZ $20 million was lost through cybercrime in New Zealand in 2022; an increase of $3 million on the year before[2].

86% of this loss came from scams and frauds. This includes scams involving unauthorised money transfers which cost NZ $5.9 million, scams involving dating and romance, which cost New Zealanders NZ $3.3 million and scams involving "new business opportunities", which accounted for NZ $3.1 million.

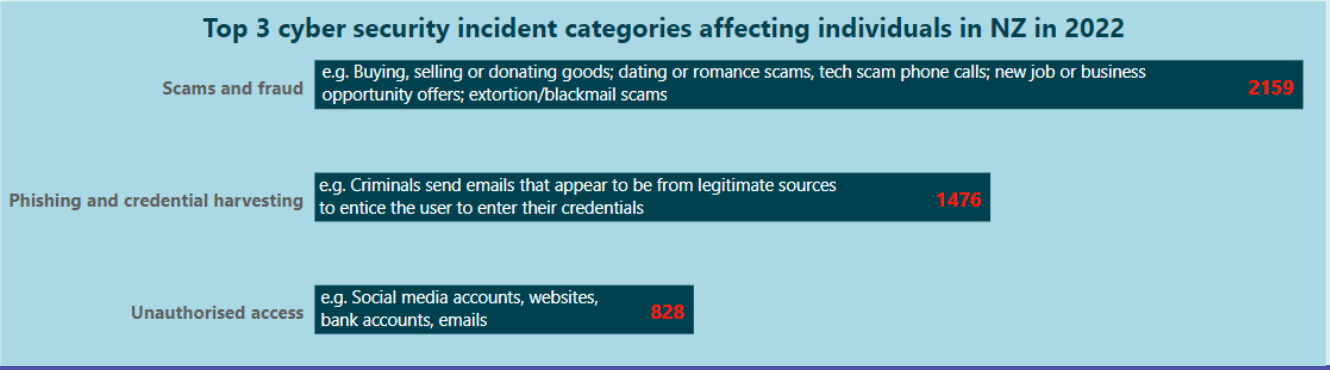
In addition to scams directly affecting members of the New Zealand public, there are large data breaches affecting businesses. When this happens, often people's personal information is taken e.g. in a ransomware attack. This can result in your details being available on the dark web. The dark web contains websites that can't be accessed from your regular web browser. These "dark" pages usually contain illegal or illegally obtained material and are used by cyber criminals for scams and illegal activity.

Once your personal information is out there, and depending on how sensitive it is, you could be exposed to scam phone calls, having other accounts attacks or being locked out of them, or identity theft.

This can have some long-lasting effects so data breaches need to be taken seriously when personal information is involved.

In the current economic climate, it pays to be vigilant and proactive about protecting your personal information.

2 Source: Cert NZ



Some tips to help you secure your personal information

Use two-factor authentication to protect your accounts.

This will help to make sure your accounts can only be accessed with your permission. Having two-factor authentication creates a link from your account to your device (usually your personal mobile phone or your email address).

When you try to log into an account that has two-factor authentication, the account will ask for a unique code, which will be sent to your device. Unless this code is entered correctly, you will be unable to log in. This feature is common among social media platforms and online banking and can be accessed via the security settings. If you receive a unique code from an account you are not trying to log into, it will mean someone is trying to access your account, giving you time to login and change your password.

Keep your devices, such as your phones, tablets, and computers, updated.

Phones, computers, and anything else that connects to the internet often have software updates from the manufacturer. Make sure these are installed as they are released. This makes sure any potential oversights found in their security are updated and made unusable to hackers.

Use varied and strong passwords on each of your accounts.

You may want to look at using a password manager to help create a different password for each of your online accounts.

Set your privacy settings in your social media accounts to only friends and family, and only add/ accept people you know.

If a friend posts a link on your page or sends you a direct message with one, check with the person to make sure it's safe. Often when a social media account is hacked, links will be sent to their friends list, usually saying something like "Is this you?" along with a link to a website. Clicking on the link allows the hacker to try to breach the account. Take a moment to double check. Message the person on a different account to check it's really them.

Insight 2

The secret costs of social media

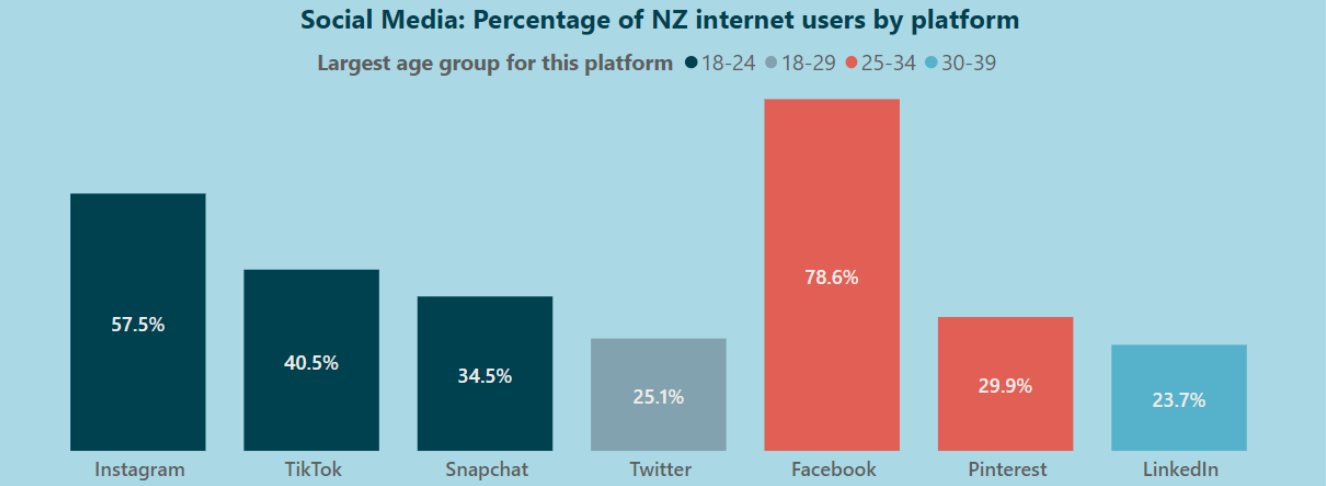
Social media has become an important part of people's lives. We use it to connect with friends and family, share our photos, and plan events, as well as a place to buy and sell things.

According to DataReportal, at the beginning of 2023 there were 4.2 million social media accounts in New Zealand. This figure may not represent individual people (some people have multiple accounts across different social media platforms), but it shows how widespread social media use in New Zealand has become.

Social media companies don't charge their users to create accounts, but they get advertising revenue and access to the information that you share on these platforms. These companies, such as Meta (who owns Facebook and Instagram), or Google (which owns YouTube), can record, use, and share the information it collects from us with other companies such as advertising agencies when this is included as part of the "user agreements" we sign when we create our accounts.

These agencies can then use this information to make assumptions about you, to target you with specific advertisements. This is why you may get the feeling you are seeing advertisements about something you just thought about.

If you use these platforms, there is often not much you can do about this sharing unless they offer an opt-out. However, there are some ways you can enhance your privacy settings to make your social media profiles secure and protect you from possible harm.



Sources: socialmedia.org.nz, Sprout Social

Some tips for social media settings

Get to know the privacy settings for each of your social media accounts.

This will allow you to manage who can see your profile and posts, pictures, and information. Depending on the platform, they might be slightly different. It will also help you decide if you want to use that platform or not. Check Netsafe to find out how to use privacy settings on social networks.

Think about who you would like to see your profile and what kind of information you want them to see.

Once you have checked your privacy settings, check who your "friends" are on the platform. There may be people you no longer wish to have access to your photos or posts.

Use varied and strong passwords for your social media accounts.

This will reduce the chance that your personal information can be accessed without permission. Large-scale security breaches of social media platforms can happen. Having varied and strong passwords on different accounts can protect you from having all your accounts breached if one account is hacked.

Check your settings regularly, as they're often updated.

This happens more often than you think. Check that your privacy settings are still in place when you are using social media in case they have defaulted back to the standard open settings.

Use two-factor authentication to protect your social media accounts.

This will help to ensure your accounts can only be accessed with your permission. Having two-factor authentication means there will be a link from your account to your device (usually your personal mobile phone or your email address). When you try to log into an account that has two-factor authentication, the account will ask for a unique code, which will be sent to your device. Unless this code is entered correctly, you will be unable to log in. This feature is common among social media platforms and should be accessed via the security settings. Also, if you receive a unique code from an account you are not trying to log into, it will mean someone is trying to access your account, giving you time to login and change your password.

If you would like to find out more, Netsafe and Cert NZ have a lot of useful information. Here is a selection of further links you might find useful:

Netsafe Guide to social media settings

Staying safe on facebook (Netsafe)

Insight 3

Cookies and trackers, leaving a breadcrumb trail online

Being tracked online is one of the top concerns for New Zealanders according to the latest InternetNZ survey.

To be tracked online doesn't always mean someone's finding out where you physically are. It means you're leaving a trail across the internet, from website to website, like breadcrumbs. One way this trail is created is through your web browser downloading cookies from websites.

There are two main forms of cookies. First party cookies are created by the website you are accessing, and can hold information like whether you are logged into an account on the website. The other type are known as third party cookies. This type is created by people/companies that are not owned by the website creator. Instead, these are often run by advertisers, and help them track you across the web. Just like on social media, it's all in the interest of making money by sending you ads.

Some websites try to be upfront with their use of cookies by having a pop up giving you the opportunity to either "Accept Cookies" or "Accept Third Party Cookies." However, they may not make it obvious that you can opt out of accepting everything.

Accepting everything is generally not the best choice to protect your privacy. This could give the webpage owners information on websites you visit, products you might have in your wish lists, purchases that you've made, your IP addresses, and your location. This info may be sold to advertisers or other businesses.

Opting out and rejecting the cookies as much as possible will reduce the ability of advertising companies to track you through the web and reduce your digital breadcrumb trail.

It is important to note, not all cookies are bad, and some are considered essential for websites to work safely or securely. These types of cookies help to prove you are not a robot, and to remember whether you are logged in, which will help to protect you and your data.

It's always a good choice to investigate the pop up that asks you to accept cookies. You can see what's being accepted and not, and from there make decisions regarding your own data and information.

Some tips on how to avoid tracking cookies on your computer

If there is an obvious choice, REJECT ALL third-party cookies when prompted.

When a pop up appears prompting you to accept cookies, take a second to see if there is a "Reject Cookies" button. As websites want you to accept as many cookies as possible, the *reject button* will often be hidden in plain sight, either through its colours or its location. Alternatively, there is usually an option to see the *"cookie settings"*. Once in the settings, you have the option to manage what is accepted and what isn't.

Use your web browser itself to help protect against tracker cookies.

Google Chrome, Firefox, and Edge all have ways that can help protect you. Here is a practical guide to turning off third-party cookies in different browsers.

Clear the cookies you collect.

As you go from website to website, cookies inevitably get saved on your browser. Get in the habit of regularly clearing cookies from your browsers (Google Chrome, Firefox, Safari, Microsoft Edge)

Look at adding "extensions" to your browser to help protect yourself.

Almost all of the web browsers being used in New Zealand have the option to add "extensions" onto them that add different functions. Some help to store passwords, some help to reduce cookies, and some help to monitor for potential threats from websites. Search for the extension available on your browser and see what best suits your needs.

Insight 4

How do you keep your child's privacy safe online?

It can be difficult and overwhelming to know where to start when thinking about your children's online privacy.

The right to having your personal information protected; like age, name, address, photos, and videos doesn't have an age limit. All children can expect that their privacy is respected and looked after.

Children are more vulnerable than adults as they are less able to understand what actually happens to their data once its online. The concerns you may have about your own data are heightened when it comes to the data from children. This is often due to a child's inability to understand the consequences of their privacy being breached, or knowing how to deal with it when their personal information is used in ways they did not expect.

While it is important to make sure that the devices children are using are as protected as they can be, either by changing settings or installing privacy protection software, the most important thing you can do is talk to your child or young person.

You can discuss with your child things like, what is personal information and what it can be used for.

You should also talk to them about how their data might be collected and used. Different age groups and different online activities may have different concerns, so it is important to understand what they are doing online and what personal information is being collected

Here are some useful Conversation starters for primary school age children put together by Netsafe to help you start a dialogue with your kids about privacy online and safety.

Their Online Safety Parent Toolkit is also an excellent place for families to start guiding children and young people in their online activities. It is a simple and practical seven step framework. It explains the online challenges young people are likely to encounter, how to best support them and what you can do to help empower young people to have a safer online experience.

Modelling good behaviour is also important to teach children that they are the owners of their personal information. We understand that online platforms like Facebook and Instagram are great for keeping families connected and to share the achievements of children. But this information is your child's personal information so you have a role in protecting this too.

Think about how they may feel in the future as adults if that photo or video was to be found later in their lives.

Talk to them about what they are happy for your family to share online about them (including photos and videos) and ask them for their consent before you post their personal information online. You can do things like tell others something like "don't post pictures of my child" to limit images or footage of your child.

Insight 4 continued

Choose what to post carefully and make sure you check the privacy mode of your posts.

We know that despite best efforts, sometimes personal information will be taken or used in a way that you or your child are not comfortable with.

Have conversations with your children and young people about what you will do together if this happens. Let them know they can come to you and that together you will work out a solution or seek outside help, like contacting the Office of the Privacy Commissioner or Netsafe.

Protecting children's information – what's happening in New Zealand

In 2023, the Office of the Privacy Commissioner is looking at whether the current approach to children's privacy is fit for purpose.

This work includes engaging with children, young people, and their families to understand their experiences around the use of their personal information.

You can send us an email – children@privacy.org.nz to raise any issues, or ask for a meeting to talk more about this work.

We also encourage you to regularly check the Office of the Privacy Commissioner's website for further detail on upcoming events or hui where children and young people's privacy will be discussed.

Some tips on how to protect your children's privacy online

When your child uses a new device or software, check the device settings to make sure the privacy settings are where you want them.

Set up Parental Controls or Family Settings on these devices to manage your child's online interactions.

Use settings to create groups of real friends to play with.

When playing games online, use the settings to only allow real life friends and family into your child's groups. This will cut down the potential for their privacy to be breached.

Keep devices in shared family spaces.

Keep an eye and ear out for your child's online interactions. The easiest way to do that is by keeping devices in family rooms (or somewhere similar) where both you and your child can see what's going on.

Set up accounts for different members of your family, each with their own settings to ensure online safety.

You can often set up "children's accounts" on devices, which by default are limited in their ability to access unwanted information or give away personal information. Set up separate accounts for children of different ages in your home to be able to tailor interactions.

Install the community applications for consoles like PlayStation and Xbox.

These apps will notify you of direct messages to your child's account and make sure you are aware of any strange behaviour. However, your child is entitled to a degree of privacy when they communicate with their own friends.

For more specific guidance, use the following links:

Conversation starters for intermediate school age children

Conversation starters for teens

A Parents' Guide to Instagram (e.g. Managing privacy, managing interactions incl. blocking unwanted interactions)

Tiktok Family Safety Toolkit

Snapchat Guide

Privacy on Snapchat

Insight 5

The evolving technologies that can impact your privacy

The use of biometric technologies and generative artificial intelligence (AI) is becoming more common in Aotearoa New Zealand.

Why does biometrics and AI matter in New Zealand?

In New Zealand, your data is collected and analysed more often than most people realise and biometrics -collecting technologies and generative AI are new ways to do that.

Biometrics refers to technologies that are used to recognise something about people based on their biological and behavioural data. This data can include people's faces, eyes, fingerprints, voices, signatures, keystroke patterns, or even odours or the way they walk.

Because the use of biometrics touches on so many aspects of our lives, and because this information cannot be taken back once it is out there, OPC is working on ensuring our privacy rights stay safe. In 2022, OPC announced a consultation on whether or not a code is required, to govern biometrics in New Zealand. This consultation is happening in the second half of 2023.

AI refers to 'artificial intelligence', which is a term for technology that can automatically take steps to find, store, and manipulate personal information as needed, sometimes to the detriment of the person involved.

Generative AI refers to tools like ChatGPT which can create text or images in response to prompts and guessing what would "fill in the blank". This is a fast-evolving technology and more work needs to be done to understand how to monitor and regulate it, so that the personal information it might use doesn't lead to harm to individual privacy.

For now, OPC has released guidance to set expectations on how New Zealand agencies and businesses use AI. We will continue to monitor developments and update this guidance as use of this technology develops.

Be aware of your own personal information

The best thing to do regarding all your personal information is to practice good "privacy hygiene." This means only making public the specific information you don't mind being public. This means not posting every picture of yourself on social media, being aware of your personal information that is online, and taking actions to protect yourself and your information.

Some tips on how to handle biometrics and AI

Be mindful of places where biometric technology is being used, and where you are asked to hand over your biometric information.

When facial recognition is in place at a place you work or visit, or if a trial of this technology is happening, there should be signs posted letting you know. If an organisation wants to check your identity using biometric technology, they should explain what they're doing and you should usually be given an alternative way of proving who you are. Ask questions if you want to know more about how the organisation will use and protect your biometric information.

When online, think about how you are using tools and applications, or what/how much personal information you share online.

All of this information could potentially be used and recorded by AI. It's almost impossible to remove pictures, posts, and words online as they are often recorded in multiple places. AI can potentially track this information down and use it for purposes you didn't intend.

If you have concerns about how your information is used with biometric technology or AI, remember that you have the right to complain to the organisation using it.

Most businesses and organisations will want to help you resolve your issue quickly, before it comes to our office. The easiest way to do this is by sending an email to the company. Most companies have their contact email on their websites and will have a Privacy Officer. You need to make reasonable efforts to resolve your issue before making a complaint to our office.

If you still have concerns after complaining to the organisation, you can bring your concerns or lodge a complaint with us.

If an agency does not respond to your request within 20 working days or you are not happy with their response, you may be able to raise your concerns or make a privacy complaint to our office. Lodging a complaint with OPC can be done online via privacy.org.nz.

About the data and sources

In this report OPC is using data, statistics and advice from a variety of sources. These include:

Kantar Public for InternetNZ, *New Zealand's Internet Insights, 2022*

Cert NZ, *Quarter Four Cyber Security Insights 2022*

Cert NZ, *2022 Report Summary*

Netsafe

Data Reportal, *Digital 2023: New Zealand*

SOCIAL.MEDIA.ORG.NZ, *NZ Social Media Statistics 2023*

Sprout Social, *Social Media Demographics to inform your brand's strategy in 2023*

US Norton, *How to clear cookies + cache in every browser*

Digitaltrends.com, *How to avoid party cookies in every browser*

Cyberpurify.com, *5 reasons why parents should stop "sharenting" – Think before you post*

Internetmatters.org, *Video games, consoles & platforms*

Privacy Commissioner
Te Mana Mātāpono Matatapu

Office of the Privacy Commissioner I Te Mana Mātāpono Matatapu
PO Box 10094, The Terrace, Wellington 6143
T +64 4 474 7590 Fax +64 4 474 7595
E enquiries@privacy.org.nz
www.privacy.org.nz