MANAAKI

GUIDE TO DIGITAL SAFETY

The digital world provides great opportunities, but also comes with great risks. This guide has been put together to provide tips for whānau to keep themselves safe online. While some tips are good for all online users, a number of these tips are specifically for instances where people are being directly targeted for online harassment.

The Manaaki Collective

Contents

Protecting your Computers and Phones

Update your phone and computer software

This seems simple but it is really important. On a regular basis technology organisations are improving their software and finding vulnerabilities. These vulnerabilities can allow for people to hack or find your details without you being aware. When you don't update your phone or computer it allows for these vulnerabilities to not be fixed leaving you open to being attacked or your information being taken through these vulnerabilities.

Utilise secure messaging

Moving your messaging to other, secure messaging platforms like Signal is a good idea.

Group messages - For both signal and facebook messages/groups - Be aware that group messaging exposes the phone numbers of everyone in the group, and that if a group is not tightly managed then people may slip in (especially once it reaches much past 40-50 people).

Phones safer than computers for opening files

If you absolutely have to open a file and you're unsure about it, try opening it on a phone. This is because most unsafe files in emails are usually intended to corrupt or destroy laptops and computers. It is still a risk but if you will not delete the file this is the next best thing to do.

If you can - use a Virtual Private Network (VPN)

Just by using your device, engaging with websites, social media and other tools your information and location can be tracked. This is because your device and IP address can be shared. A Virtual Private Network (VPN) hides your IP address by letting the network redirect it through a specially configured VPN host. It will then show your location as the VPN host (rather than your own address).

A good VPN will do the following features:

- Hide your IP address
- Allow two factor authentication to log into the VPN
- A killswitch - this ensures that if your VPN connection is suddenly interrupted, your secure connection will terminate it. This will aim to reduce the likelihood of anyone compromising your data through the VPN

Here is a guide on how to set up a VPN.

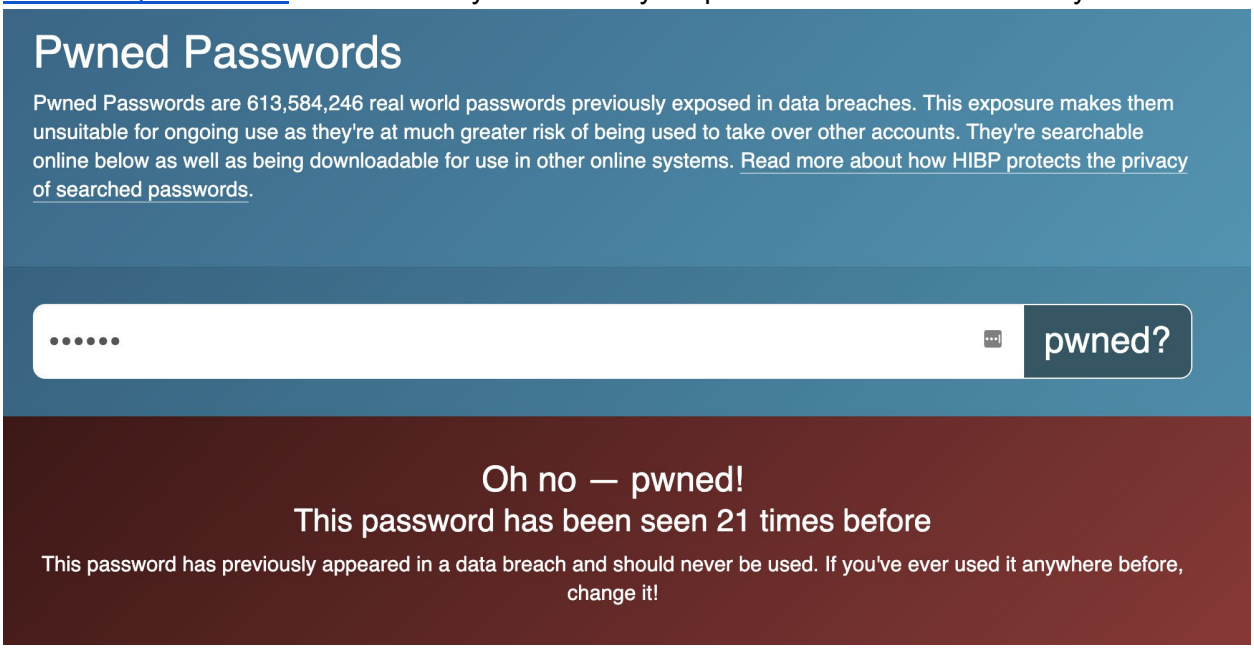
Protecting your Online Accounts

Passwords

A really key part of protecting yourself online is to have strong passwords. This means that you don't repeat the same password over and over again. Surveillance Self Defence website has a great guide on Strong passwords here.

This also suggests using a password manager as a way to remember but we also suggest strong passwords. Tools such as 1Password and LastPass are suggested options. A password manager will store the passwords you have for all applications. Some are even very handy and will populate login fields for you with plugins making it very easy to use.

If you use a regular password and are not willing to change it we recommend going to websites such as haveibeenpwned.com and it will tell you whether your password has featured in any known data breaches.



Creation of new accounts for password recovery

It's really great to set up new emails for your password recovery. This means that if your main public email is compromised at any stage not all of your accounts can be taken. As an example some people use a different email for their password manager and another different email for their password recoveries. They will NEVER share these emails publicly and instead will only share their main public email.

Multifactor

Turning on multifactor authentication for all your accounts is really important - especially your emails. Multifactor authentication means that you need two forms of devices to authenticate. So if you log in via the internet you could use a text message or an email to confirm you are who you say you are.

The three key theme for organisations to prove your identity is:

- Testing you for something that you know.
- Testing you for something that you have.
- Testing you for something that you are.

Code Generator Apps

It is recommended to use code generation apps like Authy and Google Authenticator instead of texting codes to your phone. These are easy to manipulate and telecommunication companies can intercept your text messages (if social engineering is occurring). These require you to have your app registered and when someone tries to log in it requires the code you generate.

YubiKey

Even better is if you can afford and get a Yubikey. The YubiKey - like other, similar devices is a small metal and plastic key about the size of a USB stick. They plug into your computer (some also connect to your phone). You can use them either in place of, or alongside your password, to authenticate web logins. Think of it as a physical key that, instead of unlocking a door, unlocks your online life.

Social Media Behaviour

Avoid Amplifying hate accidentally

Screenshot don't quote/link to the content in most cases. in addition to amplifying it in timelines it will link it back to you. If you want to talk about people without them coming back at you do it in coded ways or ways that are not easily searchable. e.g. John Johnson -> JJ or JJ'son. This is especially important if they have an unusual name. If you do share it, do so either in private posts or with the links "defanged" e.g.: www[.]google[.]com (this makes it so the algorithms don't make it a link)

Social Engineering

Basically social engineering is the art of manipulating people so they give up confidential information. Many people try to do this through helpdesks to get your password reset so they have access to your accounts.

It is something you need to be aware of as it could impact you and the compromising of your data.

Facebook Memes

Caution when sharing Facebook Meme's. Some of them are asking for your details for password recovery (i.e. your mothers maiden name, your first car). These memes are actually data mining your details to compromise your accounts.

Locking Down Social Media

If you are experiencing extreme levels of hate, consider "locking down" social media by switching over to locked accounts, or even closing some accounts down temporarily until it is safer to engage online.

Public address registers

Electoral Roll (NZ) - request to remove your address

If you're enrolled to vote then your address will be publicly available for people to look up. There is a simple way to register yourself to be on the unpublished roll. At the bottom of this page is a form called "Concerned about your personal safety", you need to fill this in and get it sent back to the team to process: https://vote.nz/enrolling/get-ready-to-enrol/can-you-go-on-the-unpublished-roll/

Unfortunately you do need some evidence to provide to be on the unpublished roll. These are:

- A letter explaining why your work or personal circumstances place you at risk. This letter could be from your employer, lawyer, social worker, advocate, or someone of standing in the community.
- A copy of a protection order that is in force under the Domestic Violence Act 1995.
- A copy of a restraining order that is in force under the Harassment Act 1997.
- Information from a police officer or corrections officer explaining why publishing your name and address could prejudice you or your family's safety.

Software Recommendations

TOR Browser

Tor is free and open-source software for enabling what it calls "anonymous communication". Basically the tool hides your location and prevents someone from monitoring your browser.

You can download TOR on Windows and MacOS.

Additional resources

One issue with a lot of online resources is they may not be centered (or even useful) in an Aotearoa New Zealand context. Here are some outside of Aotearoa guides that may be useful in addition to this.

Eff Guides:

The Manaaki Collective Guide to Digital Safety

- Doxxing: Tips To Protect Yourself Online & How to Minimize Harm - https://www.eff.org/deeplinks/2020/12/doxxing-tips-protect-yourself-online-how-minimize-harm
- SURVEILLANCE SELF-DEFENSE TIPS, TOOLS AND HOW-TOS FOR SAFER ONLINE COMMUNICATIONS - https://ssd.eff.org/en
    - Your Security Plan - https://ssd.eff.org/en/module/your-security-plan
    - Attending a Protest - https://ssd.eff.org/en/module/attending-protest
    - How to: Use Signal for Android - https://ssd.eff.org/en/module/how-use-signal-android
    - How to: Use Signal on iOS https://ssd.eff.org/en/module/how-use-signal-ios
    - Creating Strong Passwords - https://ssd.eff.org/en/module/creating-strong-passwords
    -

(US CENTRIC but useful)

- ACLU Staying Safe Guide (good boilerplate) - https://www.aclu.org/blog/privacy-technology/internet-privacy/staying-safe-when-you-say-metoo
- Crash Override resources http://www.crashoverridenetwork.com/resources.html
- Crash override coach - Crash override Coach - http://www.crashoverridenetwork.com/coach.html
- Iheartmob safety guide - https://iheartmob.org/resources