

**The webinar will start shortly...**

May 2024

# Own Your Online

## Mastering passwords

# Who are we?



**Sam Leggett**  
Senior Analyst  
Threat and Incident Response



**John Mollo**  
Senior Advisor  
International Engagement and Partnerships

# About CERT NZ

CERT NZ is a government agency which helps people with cyber security issues.

CERT NZ offers a few ways to help.

- Direct, hands-on assistance for individuals and businesses affected by cyber incidents.
- The [Own Your Online](#) website, with guides and resources to build up your online security skills.

# Today's agenda

We're going to cover off:

- why passwords matter,
- password length,
- unique, hard-to-guess passwords,
- when to change passwords, and
- storing passwords securely.

# Importance of passwords

# Why do passwords matter?

Passwords are the keys to your virtual castle.

Cyber attackers are usually going after your personal information or trying to access your online accounts – like your banking.

Weak passwords make the attacker's job much easier.

# How are attackers trying to get passwords?

There's several ways a cyber attacker may try to get your password.

- Brute-force: trying a lot of possible combinations.
- Dictionary attack: trying common password patterns.
- Credential stuffing: trying compromised passwords across other accounts.



# What happens if someone gets your password?

Attackers with your password can commit cybercrimes.

- Impersonating you to defraud others.
- Stealing your identity and opening accounts in your name.
- Accessing your banking and stealing your money.
- Accessing your other accounts like email and social media

# Password length

# How long should your password be?

8 characters?

It could take only 90 seconds to crack.

# How long should your password be?

12 characters?

It could take 18 months to crack.

# How long should your password be?

16 characters?

It could take over a trillion years to crack!



**Unique, hard to guess  
passwords**

# Common passwords can be easily guessed

Some of the most commonly used passwords.

- 12345678
- Password
- Admin
- Qwerty
- User
- Taylor Swift

# Reusing passwords

Reusing passwords means more damage if you are involved in a cyber incident.

- Many online accounts use your email address as your username.
- Many online accounts are accessed through your social media login.

Don't reuse old passwords or use the same passwords across multiple accounts.



# How do you choose your password?

Pet's name?

# How do you choose your password?

## Pet's name?



Liked by **bmorebump** and 5,010 others

**pepper.the.chihuahua\_** Mommy, can we \*please\* go to the park?! (Photo courtesy of @puptrait)  
Follow me for more adorable pictures! 💕 Christmas Cards and shirt available soon!

[View all 47 comments](#)

**How do you choose  
your password?**

Pet's name?

Date of birth?

# How do you choose your password?

Pet's name?

Date of birth?



**How do you choose  
your password?**

Pet's name?

Date of birth?

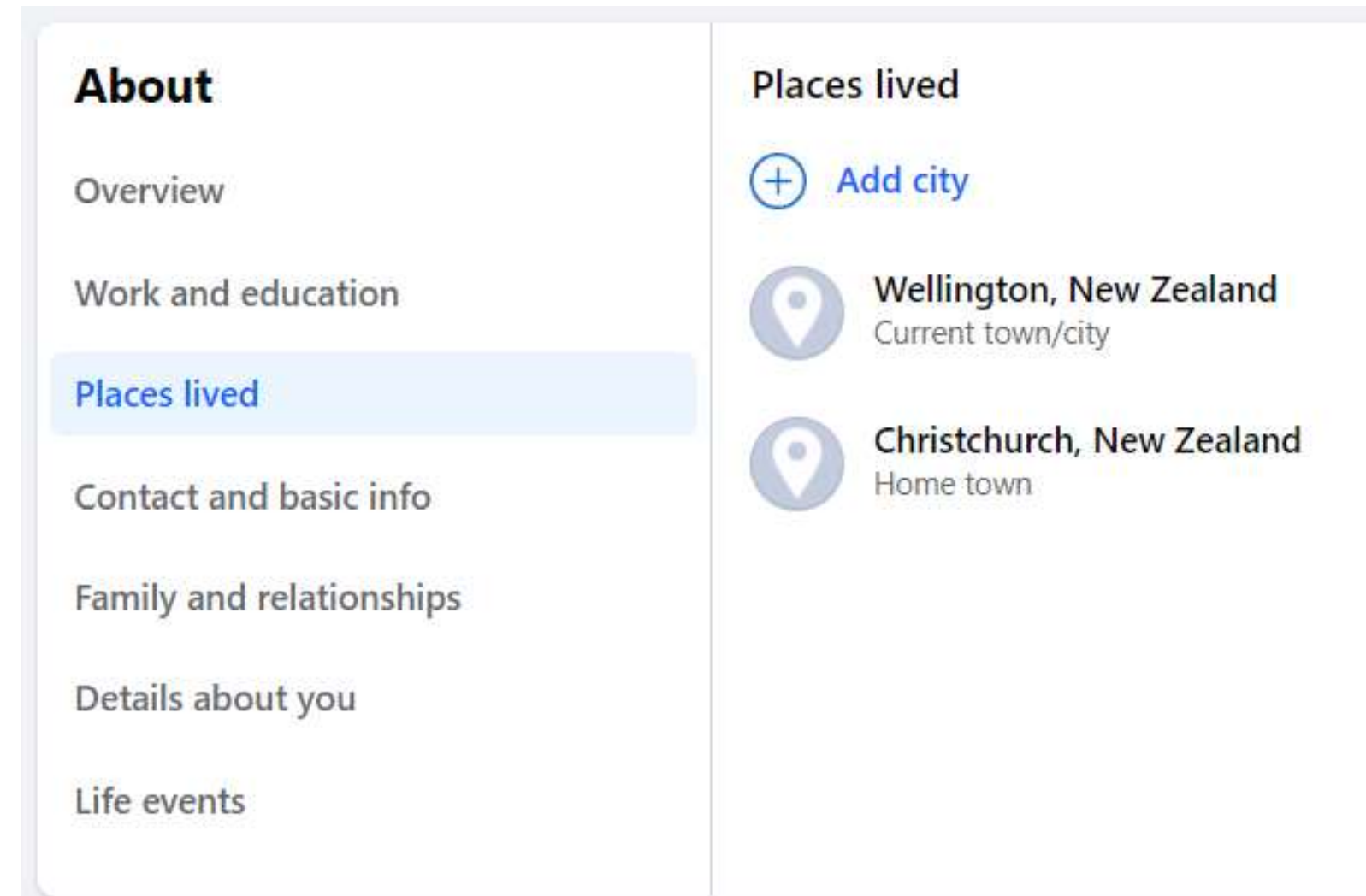
Location?

# How do you choose your password?

## Pet's name?

## Date of birth?

## Location?



The screenshot shows a user profile page with a sidebar on the left and a main content area on the right. The sidebar contains a list of menu items: 'About', 'Overview', 'Work and education', 'Places lived' (highlighted in blue), 'Contact and basic info', 'Family and relationships', 'Details about you', and 'Life events'. The main content area is titled 'Places lived' and includes an 'Add city' button with a plus icon. Below this, there are two entries: 'Wellington, New Zealand' (Current town/city) and 'Christchurch, New Zealand' (Home town), each with a location pin icon.

Section	Item
About	Overview
	Work and education
	<b>Places lived</b>
	Contact and basic info
	Family and relationships
	Details about you
	Life events
Places lived	+ Add city
	Wellington, New Zealand Current town/city
	Christchurch, New Zealand Home town

# Choosing unique passwords

More complex doesn't mean more secure.

Use four or more random words  
eg *CorrectHorseBatteryStaple*

# Meeting complexity requirements

Never have I ever....

Added '1' at the end of my password

Added '!' at the end of my password

Substituted '@' for 'a' in my password

Substituted '0' for 'o' in my password



# Meeting complexity requirements

If the platform requires your password to have numbers and symbols:

- use random numbers and symbols, and
- add numbers and symbols in random places in your password.

# Changing passwords

# How frequently should you change passwords?

Many people think you need to change passwords regularly. But that's not actually best.

- Frequently changed passwords are harder to remember.
- Changing passwords every 12 months should be sufficient.
- Make changing your passwords part of your safety routine – like checking your smoke alarms.

# Change your passwords as needed

In addition to changing passwords annually, you should change if you're potentially at risk:

- If you've clicked on a dodgy link.
- If you've been involved in a data breach.

(visit [www.haveibeenpwned.com](http://www.haveibeenpwned.com) to check)

# Storing passwords

# Storing passwords

It's difficult to remember all passwords.

How do you store your passwords?

- Write them in a notebook?
- Use the “Save my password” function in your internet browser?
- Use a password manager?

# Storing passwords in a notebook

Writing down passwords is easy – but in fact can be quite risky.

- If someone gets access to that notebook, they will have all the keys to your online castle.
- Some service provider (like banks) prohibit writing down passwords.
- If you lose or misplace the notebook, you may not be able to access your accounts.
- If you write down your passwords in a notebook, be sure to store the notebook securely. For example, in a safe or locked drawer.

# 'Save my password' function

Internet browsers offer to save credentials, but this doesn't mean they'll be secure.

- If your browser has saved your password, you can go straight to your accounts without logging in.
- Anyone with access to your device can easily access your online accounts. This is a risk if your device is lost or stolen.
- If you use this function, ensure your devices are protected with a password, PIN, pattern, or biometrics.



# Password managers

Password managers are the most secure option for storing passwords.

- These store all your passwords in a virtual vault, and to access them you use one ‘master password’.
- The master password must be long, strong and unique for the password manager option to be secure.
- Password managers are not impenetrable: cyber-attackers have managed to breach them.
- Online searches can recommend the best password managers.

# Recap on today's content

- Choosing good passwords is essential for maintaining security online.
- Passwords should be:
  - At least 15 characters long
  - A combination of four random words
  - Not based on personal information or common patterns.
  - Changed annually, or if you experience a cyber incident.
- Password managers are the most secure password storage option.

# Key takeaways

- Make the passwords on your critical accounts long, strong and unique.
- Review how you store your passwords.



**Any questions?**

# Thanks for your time

---

Sam Leggett & Hadyn Green

0800 CERT NZ

[info@cert.govt.nz](mailto:info@cert.govt.nz)

[www.cert.govt.nz](http://www.cert.govt.nz)

[www.ownyouronline.govt.nz](http://www.ownyouronline.govt.nz)