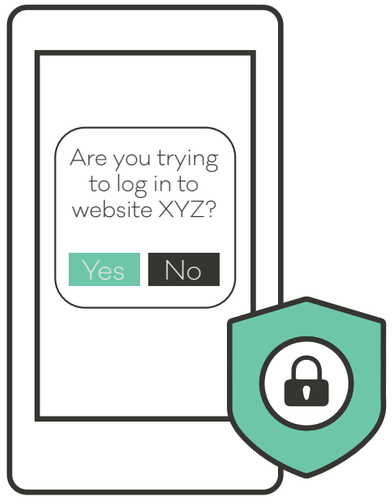
Protect your accounts with two-factor authentication

certnz

When you log in to your accounts online, you mostly use a simple 'username and password' combination. CERT NZ recommends adding another layer of security to your accounts called two-factor authentication (2FA).

Why do you need two-factor authentication?

Your password could be stolen in a phishing scam, or from a business that had a data breach. Adding 2FA to your accounts makes it harder for an attacker to access them – just knowing the password isn't enough.

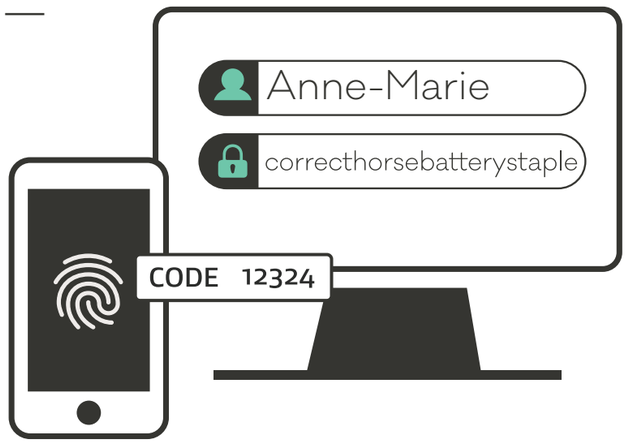


What is 2FA

To log in with 2FA you need your username and two other things — your password and something else — before you can access an account.

These two things can be:

- **something you know** (like a password)
- **something you have** (like a token or an app on your phone), or
- **something you are** (like a fingerprint).



How it works

When you log into a social media account, you use both your password and a temporary access code from an app on your phone. Even if someone finds out what your password is, they can't get into your account with that alone. They also need to have physical access to your phone so they can get the code, which isn't very likely.

How to turn it on

You can enable 2FA on most of your online accounts, like your email or social media accounts. You'll often find the option to enable 2FA in the privacy settings. Alternatively, check their website for how to turn it on.

For more information on 2FA see **www.cert.govt.nz/simple-steps**