ASSESS | UNDERSTAND | PROTECT

seQure

TWO-FACTOR AUTHENTICATION

ENABLE TWO-FACTOR AUTHENTICATION ON YOUR ACCOUNTS

E: info@sequre.co.nz | W: https://www.sequre.co.nz

seQure

Two-Factor Authentication

Passwords alone are no longer enough to keep your accounts secure.

In today's digital world, passwords alone are no longer enough to keep your accounts secure. Cybercriminals are constantly finding new ways to steal login credentials through phishing, brute-force attacks, and data breaches. This is where Two-Factor Authentication (2FA) comes in. A simple, yet highly effective security measure that adds an extra layer of protection to your online accounts.

What is 2FA?

2FA is a security process that requires two separate authentication factors to verify your identity. Instead of just entering a password, you will also need a second factor, such as;

- A code sent to your mobile device
- A fingerprint scan
- A hardware security key.

This additional step significantly reduces the chances of an attacker gaining access to your account.

How does 2FA work?

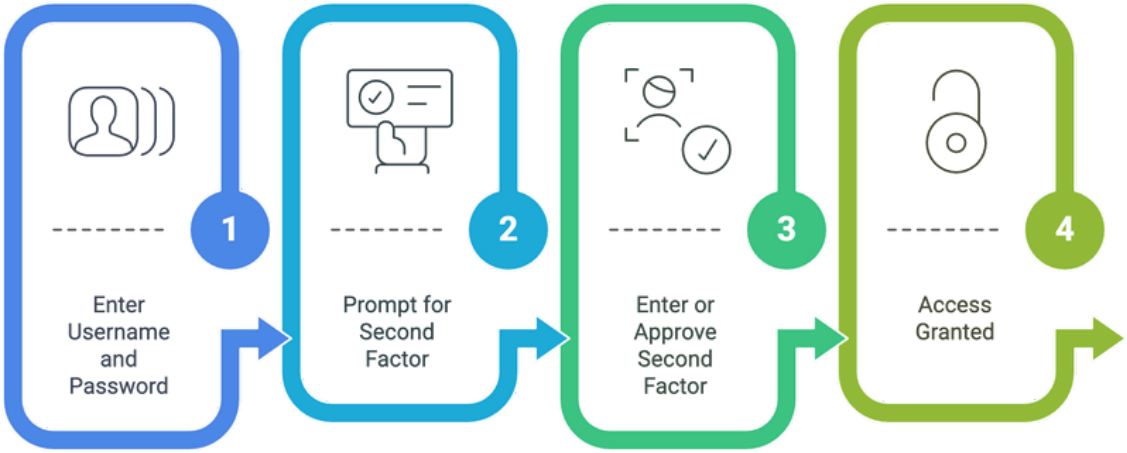
2FA works by adding a second layer of security to your login process. Instead of just entering a password (**something you know**), you must also provide a second form of verification, usually from one of the following categories:

1. **Something you have** – like a smartphone app (e.g., Google Authenticator), a hardware token (e.g., YubiKey), or a code sent via SMS or email.
2. **Something you are** – such as a fingerprint, face scan, or other biometric data.

How It works (example flow)

1. You enter your username and password on a website or app.
2. You are prompted for a second factor – this could be a one-time code from an app, an SMS message, or a prompt from a hardware device.
3. You enter or approve the second factor, verifying that it is really you trying to log in.
4. Access is granted only if both factors are correct.

This method significantly reduces the risk of account compromise, even if someone steals your password.



The Benefits of Enabling 2FA

- Enhanced Security: Even if someone steals your password, they will not be able to access your account without the second authentication factor.
- Protection from Phishing Attacks: Cybercriminals often trick users into revealing their passwords, but 2FA ensures they still cannot log in without the second step.
- Safeguarding Personal & Financial Information: With 2FA, your sensitive data, such as bank accounts, emails, and social media profiles, remain protected.
- Compliance with Security Best Practices: Many businesses and services now require 2FA to enhance cybersecurity and meet compliance regulations.

The Risks of Not Using 2FA

Without 2FA, your accounts are at risk of:

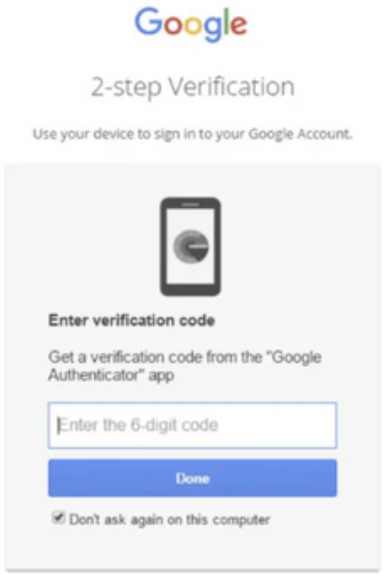
- Password Breaches: Hackers frequently gain access to databases containing user passwords. If you reuse passwords across multiple sites, one breach can compromise multiple accounts.
- Credential Stuffing Attacks: Cybercriminals use stolen login details to access other accounts where the same credentials are used.
- Financial Loss & Identity Theft: Unauthorised access to your email or financial accounts can lead to fraudulent transactions and personal data exposure.

How to Enable 2FA on Your Accounts

Activating 2FA is simple and should be done for all critical accounts, such as emails, banking, social media, and cloud services. Here is how to enable 2FA on some common platforms

Google (Gmail, YouTube, Drive, etc.)

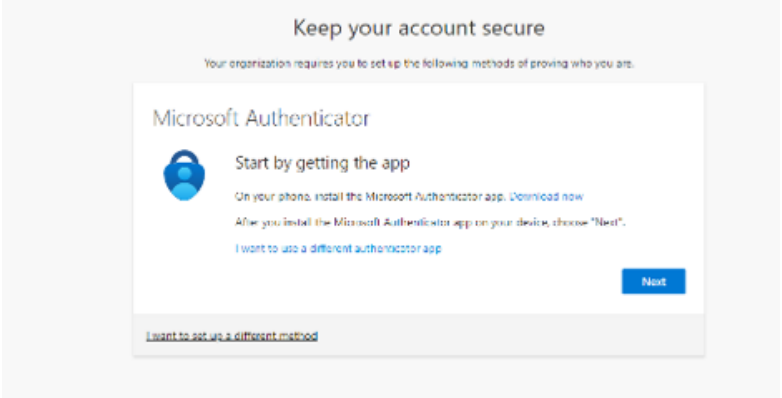
1. Open your web browser and go to **Google's 2-Step Verification** page.
2. Sign in to your Google account if prompted.
3. Under '**How you sign in to Google**', select Turn on 2-Step Verification
4. Follow the on-screen instructions to set up 2FA by either using
   a. SMS codes
   b. Google Authenticator (or alternative applications)
   c. A security key.



Google 2-Step Verification official page

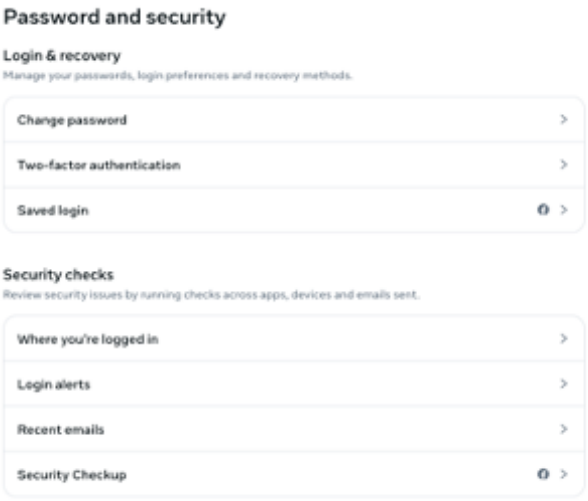
Microsoft (Outlook, OneDrive, Office 365)

1. Navigate to Microsoft's Security page in your browser.
2. Sign in to your Microsoft account.
3. Under 'Advanced Security Options, find the 'Two-Step Verification' section.
4. Click on 'Turn on' to begin the setup.
5. Follow the prompts to enable 2FA using an authentication app, phone number, or another verification method.



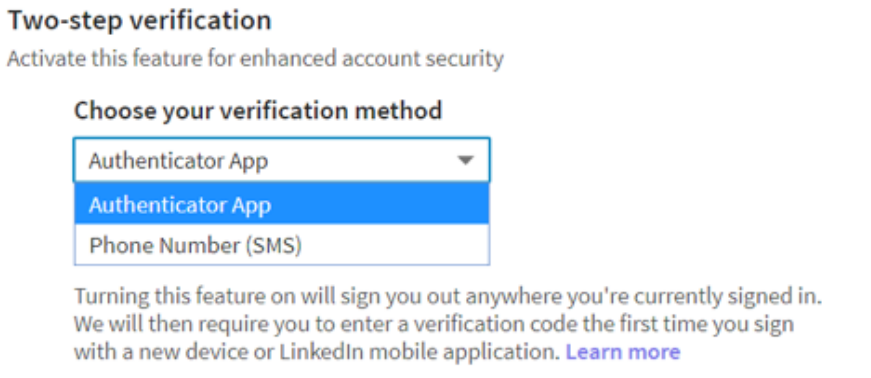
Facebook

1. Navigate to **Meta's account center for password and security** in your browser.
2. Or alternatively, Open Facebook and go to '**Settings & Privacy'**.
3. Click on '**Settings'**, then '**Password and security**' and '**Password and security**' again.
4. Click on '**Use Two-Factor Authentication**'
5. Choose your preferred authentication method (*text message or authentication app)* and follow the setup instructions.



LinkedIn

1. Go to '**Settings & Privacy**' under your profile picture.
2. Select '**Sign-in & security**' and find '**Two-step verification'**.
3. Choose your verification method and activate 2FA.



LinkedIn 2-step verification official page

Banking & Financial Services

Most banks and financial institutions offer 2FA as part of their security features. Check your bank's website or mobile app settings to enable it – a similar process would apply.

How seQure Enhances Your Security

At seQure, we understand that cyber threats are evolving, and your security posture must evolve too. Our cybersecurity services provide tailored security insights, helping individuals and businesses strengthen their digital defenses. We ensure that your accounts, devices, and sensitive information are protected with best-in-class security solutions, including continuous monitoring and proactive threat detection.

By implementing 2FA and leveraging seQure's expertise, you can stay ahead of cybercriminals and protect what matters most.

Final Thoughts

Enabling 2FA is one of the easiest and most effective ways to protect your online accounts from unauthorised access. Don't wait until a security breach happens—take action now. Secure your digital identity with 2FA, and let seQure help you build a stronger, safer cyber presence with their managed protection, 24/7.

You can find out more on - https://www.sequre.co.nz/managed-protection

About seQure

seQure is a cybersecurity service designed to protect individuals from online threats through tailored proactive security. We specialise in managed protection, offering continuous monitoring, threat detection, and expert support to protect your digital life — from devices and accounts, to personal data. Whether you have been victim of a scam, feel exposed online, or simply want peace of mind, seQure gives you the tools, guidance, and coverage to stay secure in an increasingly connected world. We deliver discreet, effective protection you can rely on — no jargon, just security that works around the clock, 24/7.

seQure - Personal, Proactive, and Simple.
Learn more: https://www.sequre.co.nz →

Contact us today: sales@sequre.co.nz