**2 Factor Authentication WHY and HOW to use**

**Why 2 Passwords?**

It's easier than you think for someone to steal your password.  
One of the ways in which a malicious individual can get your password is through *keyloggers*.  
  
These types of programs can be installed on your machine a number of ways, including:

**Clicking on a link from a suspicious email sent to you or on a website.**

Not being careful what you plug into your computer - malware can be spread through infected flash drives, external hard drives, and even smart-phones.

Leaving your computer, phone, or tablet for some period of time when not in a private environment - someone can pop in a USB or go to a website and install it on your machine.

**A keylogger** then will "log" and send every "key" that you type back to the person who created it - anywhere in the world - without your knowledge, and as easy as that, someone has your password.  
  
**To combat this, we require a secondary password**, of which we ask only 3 of the 8 characters so that a key logger will not get the entire secondary password. Each time that your secondary password is required, you are asked for a different subset of the password, making it much more difficult to get all the characters.

**Keeping logging in easy**

If you login to a trusted computer, you can choose to not require your secondary password for 30 days. You are still protected, however, because when you or anyone else tries to sign in to your account from *another computer*, your secondary password will be required.  
  
We also have a wide range of other security measures in place which require nothing additional from our users, however, since we have no control over the links that you click on, what you plug into your computer, who else has access to your computer, or whether you have anti-virus and anti-malware programs installed and up-to-date, we decided to put in place this extra layer of security.

**A better solution: 2-Factor Authentication**

Better still is if you have a smart phone and use 2-Factor-Authentication, where a code from your phone is required in place of your secondary password. Your phone will generate a different code every 30 seconds - a code that is different on each phone - so even if a malicious person has both your passwords, they will not be able to login without your phone in their hand.

In a similar way to requiring the second password only once every 30 days, if you login to a trusted computer, you can choose to not require the code from your phone for 30 days, yet still be secured.

**FIRSTLY** – go to your **App Store** or **PLAYSTORE** if Android phones. **Download GOOGLE AUTHENTICATOR.** You will need this later and it supports up to 20 different codes so do NOT WORRY

To set up 2 Factor Authentication, go to the '*Account*'" menu and click on '*Enable 2-Factor Authentication*'.

**2-Factor Authentication**

**Please note — 2-Factor Authentication is now mandatory.**

**What is it**

2-Factor Authentication (also known as 2-Step Verification), is an extra layer of security that requires not only a password to login, but also something that you, and only you, have with you — an app on your smart phone that generates a unique code different to the code generated by the app on any other phone (and the code changes every 30 seconds).

**Why you should use it**

It's easier than you think for someone to steal your password.  
2-Factor Authentication can help keep bad guys out, even if they have your password.

**How it works**

When signing in to your account - instead of entering 2 passwords, you will be required to enter your first password and a code from a mobile app.

But when you sign in this way, you can choose not to reqruie your 2-Step Verification code again on *that particular computer*. From then on, logging in to that computer will require only your first password and nothing more.

You'll still be secured, because when you or anyone else tries to sign in to your account from *another computer*, a 2-Step Verification code from the app on your phone will be required.

With 2-Step Verification, if a bad guy hacks your password, he'll still need your phone to login to your account.  
We strongly encourage using 2-Step Verification for the safety of your patients private data.

**2-Factor Authentication**

For security reasons, please enter your password before continuing:  




**2-Factor Authentication**

|  |  |  |
| --- | --- | --- |
| Let's set up your phone | | |
|  |  |  |
| 1. |  | Install [Google Authenticator](https://support.google.com/accounts/answer/1066447?hl=en) on your device. |
|  |  |  |
| 2. |  | Open the Google Authenticator app and scan the QR Code.  **Please note** - if this is your first time installing Google Authenticator, it will guide you through to also install a barcode scanner app to work with it. Once downloaded, **do not open the barcode scanner app**. Open the Google Authenticator app and scan the QR Code. |
|  |  |  |
|  |  | QR CODE WILL APPEAR HERE Scan you Smartphone camera here – Take a picture with your smartphone. Then Tap the picture that appears on your smartphone camera and it will auto start IF NOT enter the code underneath – THE CODE WILL CHANGE FOR EACH USER EACH TIME |
|  | | |
| If your Google Authenticator cannot read barcodes, you can enter this key manually: | | |
|  | | |
|  | | |

Enter the GOOGLE Authenticator code and then

**2-Factor Authentication**

|  |
| --- |
| You have successfully enabled 2-Step Verification! |
|  |
| **Please note:** You will be required get a new code from this app next time you login to this compuater and the first time that you login to any new device. If you ever need to disable 2-Step Verification, the link to disable it is in the User Extras menu.  [Continue to Mediclinic](https://portal.mediclinic.com.au/) |