



## Credentials are targets

36% of data breaches involve phishing. One credential is harvested they often go up for sale on the Dark Web. Unwanted account access is now a risk.



## Humans make mistakes

90% of data breaches involve human error. Cyber criminals also continuously try to breach popular services to gain access to their credential vault.



## MFA is vital

It is vital to protect your business users against unauthorised access. Using either a smartphone app, txt message with the access code, or a voice call to authorise system access is paramount.

## MFA addresses modern threats.

Using MFA as a 2nd requirement to access an application is like having a deadlock on your front door.

Authentication using only a username and password is single-factor authentication.

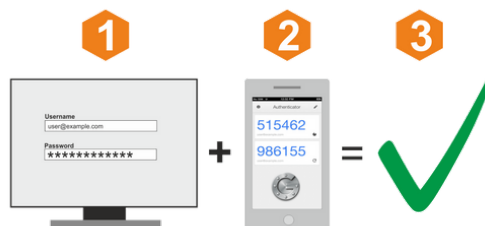
MFA raises the bar for security by requiring a user to offer 2 out of 3 factors to verify their identity:

- Something you know (e.g. username and password)
- Something you have (e.g. A smartphone app software token)
- Something you are e.g. biometric - fingerprint, facial recognition

The bar is simply too low with passwords only. Even legacy MFA methods, such as SMS or mobile authentication, have all been proven to be highly vulnerable to phishing. MFA with OTP is the modern and effective approach to keeping your hard work, brand image, and business protected.

## Benefits-at-a-glance

- Reduces fraud and identify theft
- No client software needed
- Minimises password recall
- Included with all MS365 Subscriptions
- Simple "Approve / Deny" process
- Reduces support costs
- Achieves compliance



## Have a question? Let's chat...

Whether you're interested to learn more about key features, pricing or anything else, we're here to help.

Reach out to us today

Call: +64 0800 485 644

Email: [security@rocketit.co.nz](mailto:security@rocketit.co.nz)

Website: [rocketit.co.nz](http://rocketit.co.nz)