GCOMM

# DOUBLE UP
# ON SECURITY

☎ 1300 221 115

gcomm.com.au

# DOUBLE UP ON SECURITY

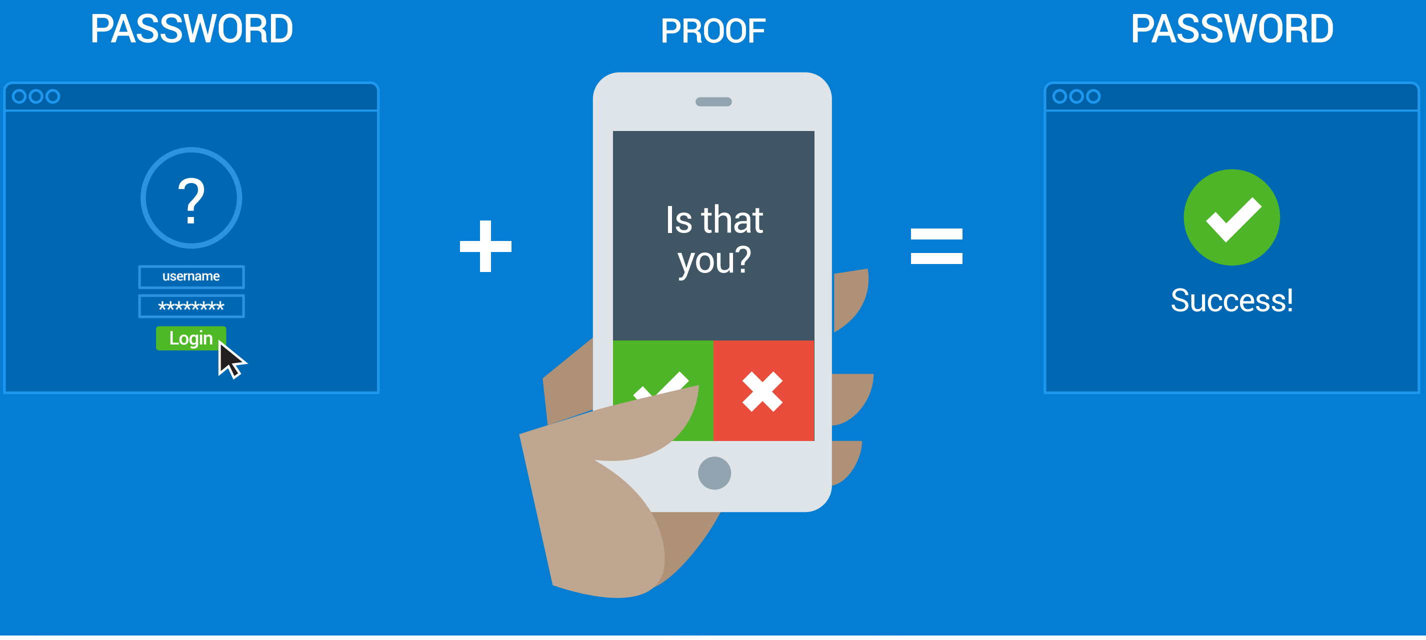
Add an additional layer of verification to make sure users are really who they say they are.

Multi-factor authentication (MFA) strengthens access security by requiring users to use two methods to verify their identity. This can include a password and username, plus a smartphone app to approve authentication requests.

Combining multiple authentication factors protects against remote attacks such as phishing, social engineering and secures your logins from attackers going after weak or stolen user credentials.

## PROTECTION AGAINST COMPROMISED CREDENTIALS

By integrating multi-factor authentication with your applications, you prevent attackers from gaining access to your corporate networks, cloud storage, financial information and accounts as they do not have the physical device that's needed to complete the two-step authentication.



# TWO-FACTOR AUTHENTICATION METHODS

Each two-factor authentication method has its own advantages and disadvantages for different types of users.

## PUSH NOTIFICATIONS

Verify your identity by approving a push notification from an authentication mobile app on your smartphone or wearable.

## SMS PASSCODES

A unique passcode is sent to your phone via SMS that you must type into your two-factor prompt.

## SECURITY TOKENS

Using a hardware token, you can press a button to verify. This device is programmed to generate a passcode that you must type into your two-factor prompt.

## TOTP

Similar to SMS, a two-factor authentication app can generate new, unique passcodes for you to type into the two-factor prompt. These are known as time-based one-time passcodes (TOTP).

## PHONE CALLBACKS

This method calls your phone and waits for you to pick up and press any key to authenticate before granting you access to your account.

## U2F DEVICE

Universal 2nd Factor (U2F) is an authentication standard that uses an authenticator (a USB hardware device) and a server. A user authenticates by tapping the device inserted into their computer's USB drive.

CISCO DUO

GCOMM partners with Cisco to deliver Duo MFA, one of the leading security solutions on the market for all business types and sizes.

**CONTACT US TO LEARN HOW DUO MULTI-FACTOR AUTHENTICATION CAN PROTECT YOUR BUSINESS FROM ATTACKERS.**

GCOMM ☎ 1300 221 115 gcomm.com.au

GCOMM

Connectivity | Cloud | Managed IT Services

23+

years in network support and engineering

8

points of presence across Australia

8000

business connected services

500

managed customer networks

700

TB of protected customer data through our backup platform

500

business customers across the country

## ABOUT GCOMM

We are Australia's connectivity, cloud and managed IT services provider for mid-large businesses. We combine our strong network foundation, engineering capabilities and partnerships with recognised technology vendors to enable our clients to transform their business. Established in 1996 in Queensland, GCOMM has grown to offer a range of technology solutions through a direct and wholesale channel. The company has won several awards and our engineers hold leading industry certifications.

**Need help?**

Call us on **1300 221 115** or contact your **GCOMM Account Manager.**

☎ **1300 221 115** ✉ salesteam@gcomm.com.au 🌐 gcomm.com.au