

# HELP PROTECT DATA FROM COMPROMISE AND FRAUD



## User names and passwords are not enough

Web and mobile apps have become critical to how we live and work. But along with a new sense of freedom and convenience, today's online environment also brings new risks.

Fraudsters are defeating password-based security, driving the need for two-factor authentication (2FA) to be adopted by consumer-facing Web services.

Telstra's deep capabilities in mobile identity can help you protect online accounts from compromise and fraudulent activity with 2FA based on each user's mobile identity – phone number, device and behaviour.

2FA delivers one-time pass codes via SMS and voice calls to protect online accounts, logins and transactions.

## Manage risk with robust online account security

Account registration	Account access and usage	Account recovery
Validate and authenticate users during account registration using SMS or voice messages to help ensure the account is attached to a legitimate user and phone number.	Verify high value transactions accessing personal information, transferring funds or making payments using SMS, voice, push notifications or code challenges.	Help reduce costs associated with password resets by sending a one-time passcode via SMS message, voice call or push notification to authenticate and verify end users.

# ROBUST AUTHENTICATION METHODS IMPROVE CUSTOMER SATISFACTION

## Fraud damages brands

Account signups are easy to automate, so fraudsters can quickly create thousands of accounts for use in malicious activities. Loyalty programs are at risk too where points are stolen and credit cards are used to buy additional reward points and sell them online at a discounted price.

Such abuse can damage brand reputation and fuel abandonment.

## Two factor authentication (2FA) and account security is no longer optional – it's necessary

Our mobile identity solutions combine phone number, device and mobile activity or behaviour. This helps you to prevent registration fraud, stop account takeovers and securely authenticate end users via SMS, voice and mobile application.

SMS & Voice Verification	PhoneID Fraud Prevention	Mobile App-Based Authentication
Offers phone-based verification and 2FA using a time-based one-time passcode sent over SMS or via voice call.	Delivers real-time security intelligence and data on phone number's attributes, usage and history, with the ability to provide underlying data to further assist in decision-making and security.	Enables you to easily build 2FA and transaction verification into existing native mobile applications. It is delivered as a software development kit (SDK) for iOS and Android.

*All three authentication methods can be easily integrated into existing web or mobile applications and workflows.*

## How we're helping customers save time, money and deliver peace of mind

- **Password resets** – decrease time and cost spent on resetting passwords
- **Online Sign-ups/Transactions** – help detect and combat registration fraud and defend against account compromise
- **SecureID tokens** – help save costs by replacing the need to re-issue, maintain and manage separate tokens
- **Loyalty programs** – help protect hard-earned points from being stolen and credit cards fraudulently charged.



## Manage mobility security with Telstra

We can help you preserve your customer ecosystem by detecting a suspicious user before account creation and protect your existing user base from account compromise.

Plus we can bring all your mobile services together on one bill, which includes your hardware, plan and professional services costs. That means one provider and one point of contact.

📞 call 1300 Telstra

🌐 [telstra.com/mobileidentity](https://telstra.com/mobileidentity)

🏠 contact your Telstra account executive