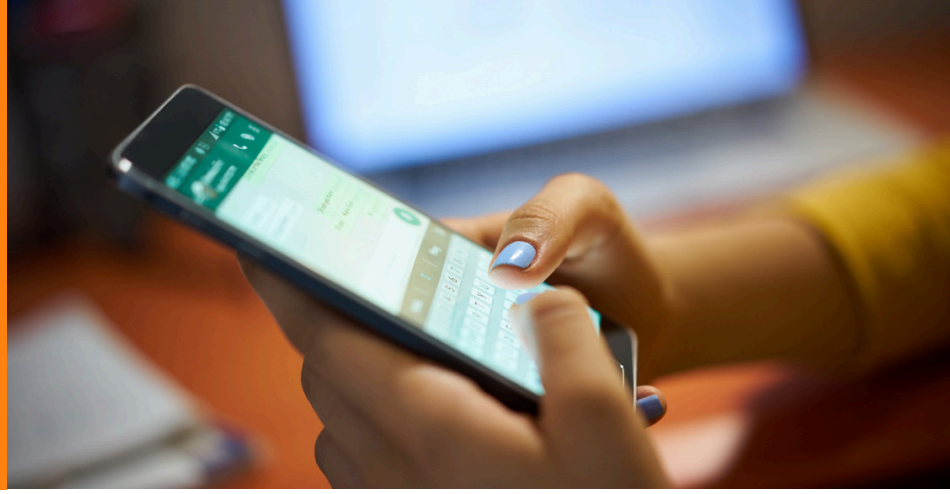
MFA

Keep your account secure



Protect What Matters Most: Enable MFA Today

In a world where cyber threats never sleep, Multi-Factor Authentication (MFA) is your simple, powerful first line of defense.

What is MFA?

MFA is an extra layer of security that requires two or more steps to verify it's really you logging in —not just your password. Think of it as a smart bouncer for your financial accounts: one credential isn't enough.
Bottom line: It makes it dramatically harder for hackers, scammers, and identity thieves to get in —even if they steal your password.

Why does this matter for you?

Passwords alone are no longer safe. Data breaches happen daily. With MFA turned on, even if criminals get your username and password, they're still locked out without that second step. It's one of the easiest ways to safeguard your money, data, and peace of mind.

How does MFA work?

1. Enter your username and password as usual.
2. Complete one quick additional step to prove it's you.

That's it. Takes seconds, adds serious protection.

Common, easy MFA methods:

- A one-time code sent by text or email
- Push notification on your phone (just tap "Approve")
- Authenticator app (Google, Microsoft, or similar) that generates a fresh code
- Biometrics like fingerprint or face ID
- Security key (a small physical device for maximum security

Your next step is simple

When you see the option to turn on MFA for your accounts here or anywhere else—enable it. It's free, fast, and one of the smartest financial decisions you can make.

To comply with regulatory guidelines for digital banking, you will be required to set up MFA for your home banking or mobile app.