Multi-Factor Authentication

Always enable multi-factor authentication.

It's as easy as learning a new dance move and your online accounts will thank you. Multi-factor authentication, or MFA, is a security measure that requires anyone logging into an account to navigate a two-step process to prove their identity. It makes it twice as hard for criminals to access an online account. When it's available, always turn it on because it's easy to do and greatly increases your security.

How does MFA work?

By adding one more simple step when logging into an account, multi-factor authentication greatly increases the security of your account. Here's how it works. Just like logging into your account, the first step is giving your password or passphrase. The second step is to provide an extra way of proving that you're you, like entering a PIN code or texting/emailing a code to your mobile device, or accessing an authenticator app.

MFA can include:

- A extra PIN (personal identification number)
- The answer to an extra security question like, "What's your favorite pet's name?"
- An additional code either emailed to an account or texted to a mobile number
- A biometric identifier like facial recognition or a fingerprint
- A yes or no button or unique number generated by an authenticator app (like those from Microsoft, Google or Duo)
- A secure token, which is a separate piece of hardware (like a key fob that holds information) that verifies a person's identity with a database or system

What type of accounts offer MFA?

Not every account offers MFA, but it's becoming more popular every day. It's seen on many accounts that usually hold either valuable financial or personal information like banks, financial institutions, online stores, or social media platforms. Any place online that is storing your personal information (especially financial information), or any account that can be compromised and used to trick or defraud someone else should be protected with MFA. Simply put, use MFA everywhere!