HIGHTOWER

# Passwords, Passkeys, and Face ID

*Simple Ways to Strengthen Online Accounts*

Protecting your online accounts is one of the simplest and most effective ways to reduce cybersecurity risk. Email, banking, investment, and cloud storage accounts often contain sensitive personal and financial information, making them attractive targets for cybercriminals. Fortunately, a few straightforward habits, such as using strong passwords, enabling multi-factor authentication (MFA), and taking advantage of passkeys and biometric logins can significantly improve your online security.

## Why Strong Passwords Matter

One of the easiest ways cybercriminals gain access to online accounts is through weak or reused passwords. If the same password is used across multiple websites, a single data breach can expose several accounts at once. Using strong, distinct passwords for each account helps limit the impact if one account is compromised.

A smart practice is to create a different password for every important account, especially those associated with your email, banking, investments, shopping, and cloud storage. Distinct passwords create separation between your accounts, making it more difficult for an attacker to move from one compromised account to another.

## How to Manage Your Passwords

Remembering dozens of complex passwords isn't realistic for most people. Password managers securely generate and store strong, complex passwords so you don't have to memorize them. Common options include 1Password, Dashlane, Bitwarden, Apple Passwords (formerly iCloud Keychain), and Google Password Manager.

Like any security tool, password managers should be protected with a strong master password, updated recovery settings, and multi-factor authentication whenever available. Though strong passwords are an important first step, they work best when combined with additional security measures that help protect your accounts even if a password is compromised.

## Additional Layers of Security

### Multi-Factor Authentication (MFA)

Multi-factor authentication adds another layer of security by requiring a second form of verification when signing in. This may include a code sent by text message, an authenticator app, a push notification, or a physical security key.

Authenticator apps generally provide stronger protection than text message codes because they are less vulnerable to certain types of attacks. However, if SMS verification is the only option available, it still offers significantly more protection than relying on a password alone.

### Face ID and Fingerprint Login

Biometric authentication, such as Face ID or fingerprint recognition, offers both convenience and security. Because these methods are tied to your physical characteristics, they are much harder to guess or reuse than traditional passwords. They also make it easier to consistently use stronger authentication methods.

### Passkeys

Passkeys are an emerging authentication technology designed to reduce reliance on passwords altogether. They use cryptographic credentials stored on your trusted device, making them more resistant to phishing attacks and credential theft. When offered by a trusted financial institution or website, passkeys are generally a strong option for securing your account.

## *key takeaways*

No single security feature can eliminate every cyber threat, but combining strong, complex passwords with multi-factor authentication, password managers, biometric authentication, and passkeys creates multiple layers of protection. Together, these tools make it more difficult for attackers to gain access while making everyday logins more secure and convenient.

HIGHTOWER

200 W MADISON, 25TH FLOOR
CHICAGO, IL 60606

(312) 962-3800
HIGHTOWERADVISORS.COM