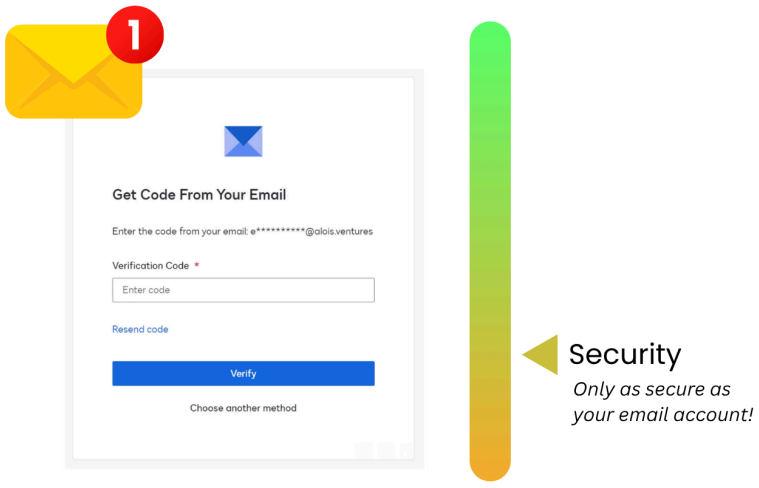
What is Multi-Factor Authentication?

MFA is a way to improve security by requiring more than just a username and password to log into an account. You may also see the term “Two-Factor Authentication” or 2FA.

MFA requires proof from at least two different categories. A password or a pin can be categorized as something you know. Biometrics, like your face, fingerprint, or iris pattern, can be categorized as something you are. Your phone, your laptop, or a security key can be categorized as something you have.

Types of MFA

Some second factor authentication methods are better than others! Here are some of the most common ones used.

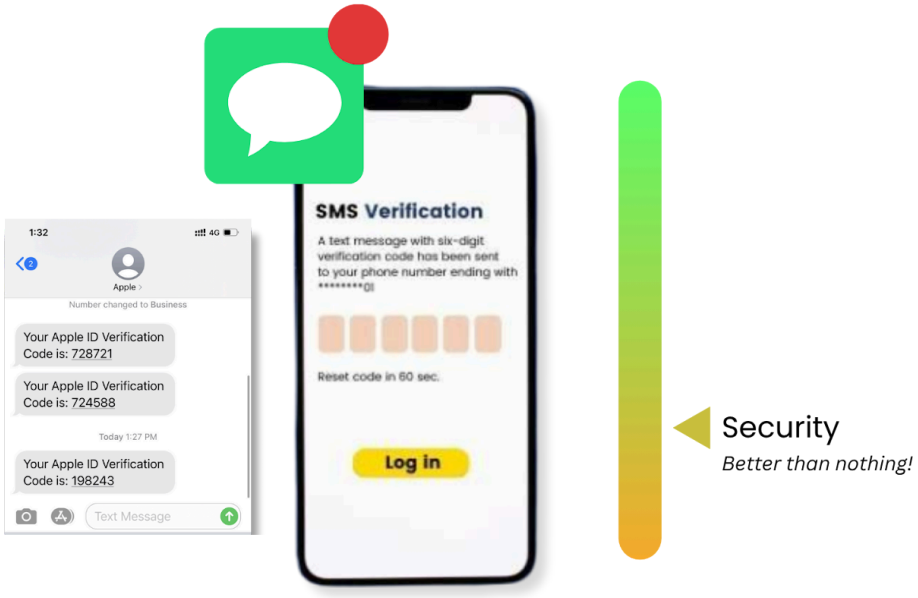


Emailed Verification Codes

Emailed verification codes are only as secure as your email account! Email accounts are frequently compromised through phishing, password reuse, or account takeover attacks. If an

attacker gains access to your email, they can intercept these codes and bypass your 2FA protection entirely. Fake login pages can capture both your password and forward the emailed code to an attacker.

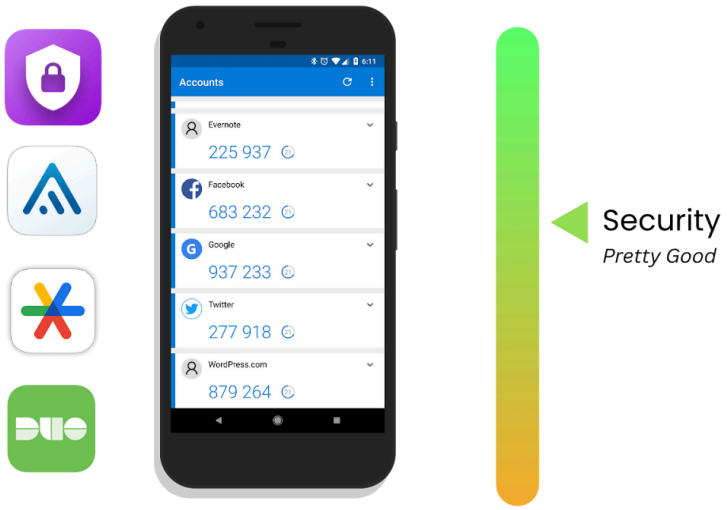
That means that emailed verification codes are generally considered to be among the weakest forms of 2FA out there. Use strong, unique passwords and set up MFA on your email account to improve security, but aim for a better method when possible.



SMS Verification Codes

SMS Verification as 2FA is better than nothing! But it is vulnerable to things like SMS interception, device compromise, SIM Swapping, and other kinds of attacks, which can lock you out of your accounts for good.

(Use strong passwords and add SIM protection with your cell service provider to guard against SIM swapping!)



Authenticator Apps

Using an Authenticator App is a great way to level up your 2FA security. Instead of waiting for a text message to arrive, you just open the app, which generates 6 digit codes that change every 30-60 seconds. These codes are called Time-based One-Time Passwords, or TOTP.

Setting up your accounts within your authenticator app is quick and easy: You just scan a QR code.

Some free authenticator apps I recommend are Ente Auth, and Aegis Authenticator. Duo Mobile offers enterprise accounts with a level of admin management for organizations. Google, Apple, and Microsoft also offer authenticator app options.

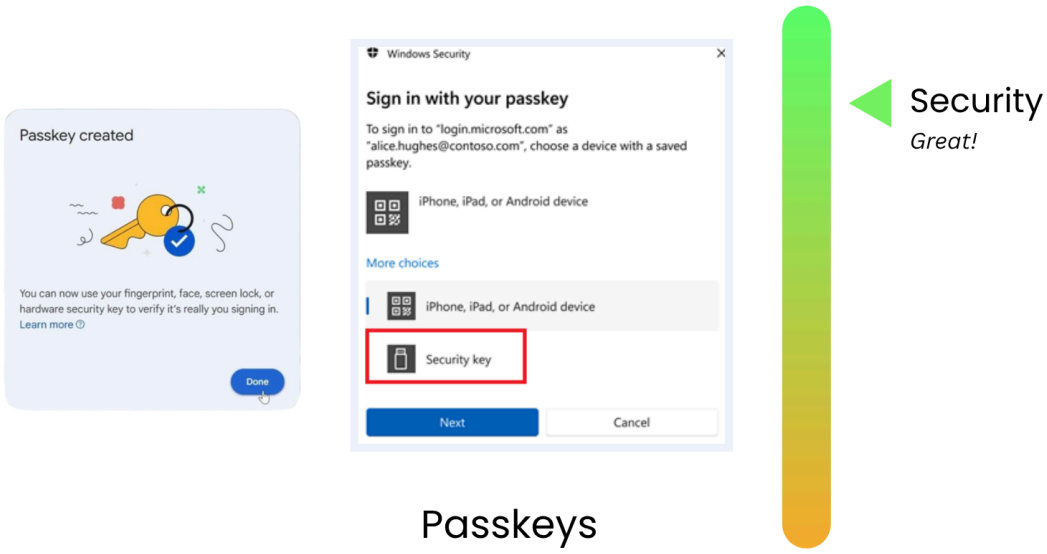
While some password managers offer built-in TOTP (Time-based One-Time Password) features, we recommend using a separate app - that way an attacker needs to compromise two different systems to gain full access to your accounts. They might get your passwords but not your TOTP codes, or vice versa.

Authenticator Apps have a significant security advantage over SMS Verification, but they can't defend against Phishing and Social Engineering, some forms of malware on compromised devices, and other technical vulnerabilities.

Security Keys and Passkeys

Passkey and Security Key are at their heart sort of like a lock and a key made out of fancy math: there are two parts that fit together that are needed to unlock your account. The entire unit is generated by your device: one part is stored on your device (or in your password manager,) and the other part is stored by the company running the account (like Google, Microsoft, etc.)

Passkeys and Security Keys are safer than passwords: If the company holding the account experiences a data breach, only half of what's needed to access your account can possibly be revealed. There's also a check built into the fancy math of every passkey or security key that makes sure you're not visiting a fake website pretending to be the real one, so both are incredibly phishing resistant.

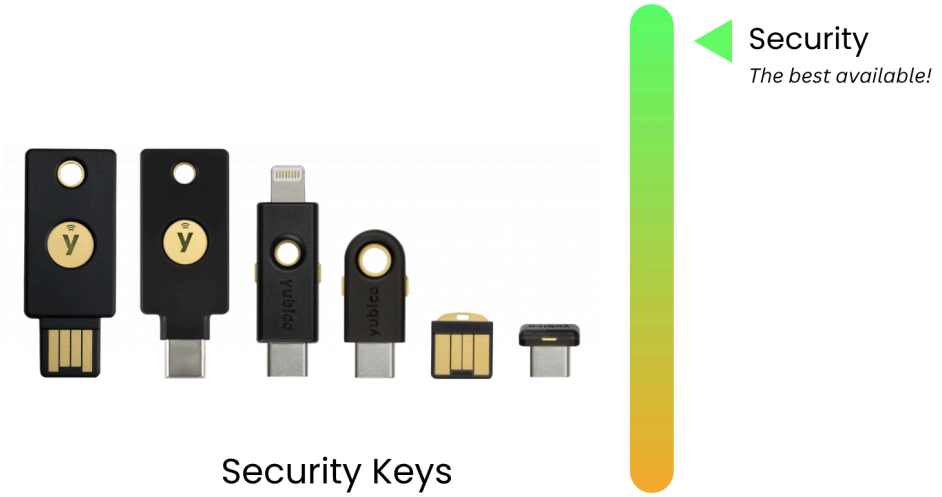


Passkeys and Security Keys are very similar! The difference is that Security Keys are a unique device for this sole purpose, (pictured below,) while passkeys can be generated and stored on devices like your phone or laptop.

The user experience is also very similar. When you use a security key, just plug it in to your USB port, or tap the NFC chip against your phone, and follow the prompts on screen to enter your lockcreen passcode or device PIN, and touch the key, and you're logged in!

When using a passkey, you'll also follow the prompts on screen and enter your lockcreen passcode or device PIN. If you store your half of the passkey inside your password manager for additional security, you'll also have to unlock that.

Both passkeys and security keys are good options to improve your security, offering protections from attacks like phishing, SIM swapping, SIM interception, Man-in-the-Middle Network Attacks, and malware. Even if someone knows your password, they can't access your accounts



Security keys do have a key advantage over passkeys for high risk users in that they're a dedicated device that stays with you physically and is completely offline. Hackers can't steal what's on your security key remotely. They'd need to physically take it from you. With passkeys, if your Apple/Google/Microsoft or password manager account is compromised, an attacker might access synced passkeys… though they would still need to crack your device's PIN.

YubiKey and Nitrokey are two good options for Security Keys. They start at about $50 each, and it's a good idea to purchase two per user to have a backup in case one is lost.

While they require some upfront cost, security keys provide the strongest protection available for most people's online accounts.

Some MFA Vulnerable Methods

- Security Questions - Your mother's maiden name, the street you grew up on, your elementary school, etc. Personal information that is easily discoverable with an internet

search, or a quick look at a databroker database is one of the least secure MFA methods out there.

If you have to use a security question, you can improve your security by using a fake answer.

- Voice Call MFA is similarly prone to SIM swapping and social engineering attacks as SMS MFA
- Email-based MFA is only as secure as your email account itself. Only use this if your email account has strong protection: a long unique password, and its own strong MFA set up.
- Voice Pattern - While once in vogue, voice patterns are now easily replicable by AI.