Multi-Factor Authentication

What is it?

Rather than just relying on a password (a single factor), multi-factor authentication (MFA) requires two forms of identity confirmation: generally a password/passphrase AND a one-time token delivered to a device owned by you.

The token is generally a four or six digit number that is valid for a limited time. It can be received on a mobile device in the form of an SMS or delivered via a dedicated app (preferred) such as Google’s Authenticator. Here’s an example. The small pie icon in the lower right indicates how much time is left before the token expires.

Google

537 907

ambar@gmail.com

Why should I bother?

Passwords by themselves are no longer considered a secure and private form of authentication. In the past few years, literally hundreds of millions of commonly used passwords have been exposed and published on the Internet.

This enormous repository of passwords is mined by cyber gangs who meticulously test the credentials against the major on-line service providers (Gmail, Hotmail, Facebook, Twitter, Instagram, banks, etc.) to find valid matches that give them access to active accounts.

Since many people reuse the same password, or slight variations, for multiple service providers, the chances of finding a valid match are relatively high. (This is why you should use a password manager.)

---

1 https://haveibeenpwned.com/Passwords
If you enable MFA with those providers who offer it (and there are many), a password alone, even if it’s the correct one, will not be enough to gain access to the account. The intruder will need the second factor to complete the authentication process.

Additionally, if you fall victim to a phishing attack (a fraudulent request for your password), having MFA enabled will prevent your compromised credentials from being used to access your account. Again, the perpetrator will need that second factor to get in.

**Protect the 2nd Factor!**

Of course, MFA is only secure if you protect the device that is used to obtain the second factor. If you’re using a mobile device for this purpose, make sure you safeguard it by requiring a passcode or biometric authentication (finger print, face recognition) to access the device. Otherwise, whoever has your phone is you! And always opt for the app rather than receiving your second factor by SMS (text message). This article explains some of the concerns associated with mobile phones as the source of your second factor:

http://www.circleid.com/posts/20170827_not_quite_two_factor_or_is_your_phone_number_something_you_have/

**How to enable MFA**

Here are resources for activating MFA with some of the major on-line service providers. Others may be found by searching on the provider’s name and MFA or 2FA.

Instagram  
https://www.wired.com/2017/03/instagram-two-factor-authentication-now-turn/

Twitter  
https://www.cnet.com/how-to/how-to-enable-twi...ts-two-factor-authentication/

Facebook  
https://www.eff.org/deeplinks/2016/12/how-enable-two-factor-authentication-facebook

Snapchat  
https://www.turnon2fa.com/tutorials/how-to-turn-on-2fa-for-snapchat/

Google  
https://www.google.com/landing/2step/