Multi Factor Authentication: What is it and why you should use it

Author : Cat

Date : June 7, 2016

It may sound complicated but Multi Factor Authentication (MFA) is not only simple, it is becoming necessary in an increasingly digital world.

What is it?

To log in to to any digital platform, you are required to provide something to identify yourself as the owner of the account. Usually this consists of a unique identifier such as a username (or email address), and a password. In the case of hardware, like a phone or laptop, the device itself is unique, so you only need to provide the password. The password is one factor. The problem is that passwords can be guessed or stolen.

Whenever I think of the idea of MFA I always imagine those crazy scenes from Mission Impossible movies where the guy needs an iris scan to get through one door, and then a voice match for the next, and then an ID card, and then a passcode (which the hero spies manage to replicate, of course). Though the real examples don't involve such sophistication, the idea is the same.

As I would explain to a 6 yr old:

Knock knock

Who's there?

Me

Me who?

Look out your window and verify who I am.

Two factors. One in me saying who it is, second in visible verification. That simple.

The different ways you can authenticate are divided in to three categories:

- ***Knowledge***: something you know. Like a password.
- ***Possession***: something you have. Like a phone.
- ***Inheritance***: something you are. Like a fingerprint.

Depending on the software or device that you use, you'll have one item in the *Knowledge* category, and one from another category. The additional authentication can be a text sent to your phone, a passcode sent to a landline, or any one of several biometrics (physical identification like fingerprints, iris scans or voice activations). There are usually two factors so sometimes you will hear the term *Two Factor Authentication*, or *2FA.*

To be clear, most MFAs occur only when a user tries to access the account from a new computer or device. So you won't need a special code every time you open your email on your phone BUT if you try to set your account up on a new device, then the extra verification will be needed. This makes sense from the perspective of someone stealing your password and attempting to login in. Most hardware manufacturers are also working on MFAs so a lost phone or tablet also requires

multiple verifications to get in to it.

Should you use it?

In simplest terms, yes. You set it up once and will only need to verify when you set the account up fresh on a new device or access it from a foreign computer. A small amount of effort to pay for a large amount of insurance.

Almost all of the major networks, including email, have the ability to use MFA. Some software may have different names with 'Authentication', 'Verification' or 'Approval'. Facebook, for instance, calls theirs *Login Approvals.* You can find MFA in your settings under 'Security'. If you don't have a cell phone for texting (SMS) you can always use your landline to have codes sent.

At the very minimum, be sure to set it up for your email account. This is the one account someone can use to reset all of your existing passwords. If this account is compromised so are all of your others.

Google even provides suggested second steps for when you cannot access your phone codes.

Whatever method you chose to use, prioritize your most important accounts and start there. As with all security measures, hopefully you will never need the back-up of MFA, but if someone does get your password, you'll be glad you have it.