Use Multifactor Authentication Wherever Possible

Many doors have many locks. Think of the door with many different types of locks. If one is good, more is better. The same should be said of the keys that we apply to the digital things we want to protect. The first level of authentication, providing that you have the right to access a file such as a tax return, picture, or document, is your password. A password is something you know, which grants you access to whatever you protect with your password. But sometimes passwords can be taken or guessed. If you want to increase the level of protection on sensitive items such as email, online banking, password managers, and any other application, there is a second layer of protection you can add. This is referred to as multifactor authentication.

Multifactor authentication allows many layers of security to protect sensitive information. Think of a safe in your house. You have to be able to unlock the door, know the location of the safe, then have the key or combination to access the safe. This puts many obstacles in the way of someone who does not have permission to access your safe. And it combines different things that are needed to access the safe. Multifactor authentication works in the same fashion by combining the many different types of information that are needed to access a resource. The following are examples of types of authentication methods you can apply:

- **Something you know:** A picture you remember, a password, a PIN
- **Something you have:** An app on your smartphone, a device that you plug in, a token, etc.
- **Something you are:** Fingerprints, speech, retina, etc.

The *factor* portion of multifactor authentication is an important piece of this equation. You create unauthorized access to what you want to protect when you take two elements (such as something you know and something you have) and require them both to access the information. This is referred to as two-factor authentication. The more you combine elements, the less likely it is that someone will be able to access information without your permission.

What can you do?

Check for websites that allow multifactor authentication, and enable this feature. A good amount of popular websites such as LinkedIn, Facebook, Google, Dropbox, and many more support at least two-factor authentication. Please visit https://twofactorauth.org/ for more information and a detailed list of websites that support this feature.

More current devices are allowing users to register fingerprints as a “something you are” method of authentication. In most cases this also requires a password that is needed if the device is restarted. Keep in mind that a fingerprint can be combined with a PIN or password for increased security.

In our current living environment, smartphones are at our side all day. Many applications can produce a one-time password or PIN to access websites and unlock applications (such as password managers). One of the most popular applications is Authy, which is available from the Apple and Android stores; others exist. Google and Microsoft both have their own apps available. Check with the sites and apps you are enabling two-factor authentication on to see what they support or recommend.

PRO-TIP: Enable 2FA on EVERYTHING! Especially your email and social media accounts. Check https://twofactorauth.org/ to see which services support it.

WIPFLi CPAs and Consultants