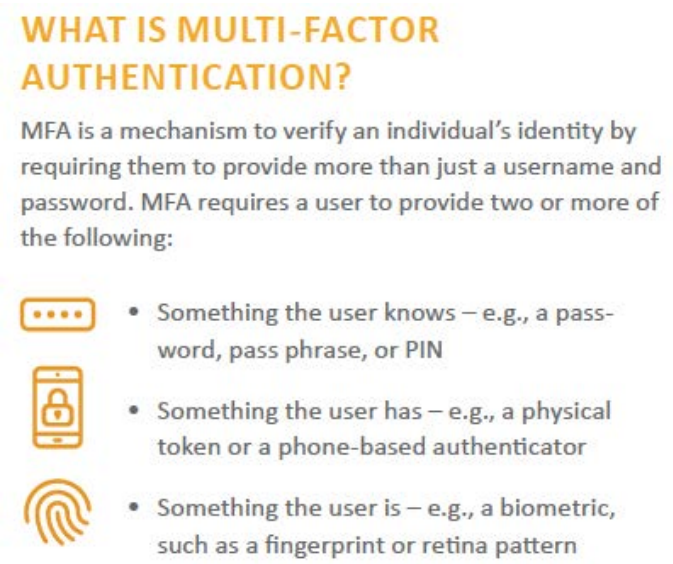
Multi-Factor Authentication

You've recently set up a travel management portal for your small business that requires everyone to log in using a username and password. The portal also requires a user to have an authentication app on their phone for verification of their identity. That way, a one-time code will be accessed in the authentication app and entered into the portal to confirm their identity. This scenario depicts the use and benefits of multi-factor authentication, an increasingly common method to add multiple layers of security to internet-enabled services.

You can find the NIST Multi-Factor Authentication video and other SBCC videos at:
https://www.nist.gov/itl/smallbusinesscyber/videos

What is Multi-Factor Authentication?

When it comes to securing online accounts, most of us are familiar with the standard combination of using a username and a unique password. For many years, this was considered a reasonably secure way to limit access to just the authorized users of the account. However, due to normal human behavior, people tend to choose easy to remember passwords or reuse the same passwords at multiple online accounts.



A simple password is likely one that a hacker can discover using a variety of hacking tools; and a reused password may have been previously revealed in a data breach. Once a username/password combination has been listed among the data of known breached accounts, it is no longer secure, no matter how long or complex that password was. In fact, databases of known breached account information reveal the actual passwords in use around the world, and we can see that people typically fail to choose sufficiently long, complex, and unique passcodes. A study of the most common passwords used globally has "123456", "qwerty" (six consecutive keys on a keyboard) and "password" among the top 5.

Therefore, it is necessary to add more layers of authentication beyond a password to ensure that accounts remain secured. These additional layers lead to the term of 'multi-factor authentication' or MFA and can include three elements:

- things you know – such as a password or other personally-known information such as the answers to security questions

- things you have – such as an id badge with an embedded chip, or a digital code generator
- things you are – such as physical traits like your fingerprints or voice

MFA utilizes factors from multiple of these elements to prove users' identities. For example, in addition to entering a password, a user may be required to provide a code that was sent to their phone or email account.

Setting up MFA is usually an easy one-time process for each online account. Of course, it's also a best practice to use a passcode on your phone and on your computer – otherwise someone with physical access to these devices could potentially gain access to your accounts. Adopting MFA isn't going to close the door on every threat to your accounts – but research shows making it much harder for hackers to get in means they'll train their sights on less protected accounts first.