Protecting You and Your Family

FCCB
FIRST CITIZENS COMMUNITY BANK

A How-to-Guide for Multi-Factor Authentication

Have you noticed how often security breaches, stolen data, and identity theft are consistently front-page news these days? As these incidents become more prevalent, you should consider using multi-factor authentication, also called strong authentication, or two-factor authentication. This technology may already be familiar to you, as many banking and financial institutions require both a password and one of the following to log in: a call, email, or text containing a code. By applying these principles of verification to more of your personal accounts, such as email, social media, and more, you can better secure your information and identity online!

What it is:

Multifactor authentication (MFA) is a security process that requires more than one method of authentication from independent sources to verify the user's identity. In other words, a person wishing to use the system is given access only after providing two or more pieces of information, which uniquely identifies that person.

How it works:

There are three categories of credentials: something you either know, have, or are. In order to gain access, your credentials must come from at least two different categories. One of the most common methods is to login using your user name and password. Then a unique one-time code will be generated and sent to your phone or email, which you would then enter within the allotted amount of time. This unique code is the second factor.

SOMETHING YOU KNOW	SOMETHING YOU HAVE	SOMETHING YOU ARE
✓ Password/Passphrase ✓ PIN Number	✓ Security Token or App ✓ Verification Text, Call, Email ✓ Smart Card	✓ Fingerprint ✓ Facial Recognition ✓ Voice Recognition

When to use it:

MFA should be used to add an additional layer of security around sites containing sensitive information, or whenever enhanced security is desirable. MFA makes it more difficult for unauthorized people to log in as the account holder. If you have the option to enable it, you should take the initiative to do so to protect your data and your identity. Look at your account settings or user profile and check whether MFA is an available option. If you see it there, consider implementing it right away! User names and passwords are no longer sufficient to protect accounts with sensitive information. By using multifactor authentication, you can protect these accounts and reduce the risk of online fraud.