The Construction Collaborative
CMSOCIAL.NET

What is…

Two Factor Authentication (2FA)

Two Factor Authentication (2FA), also called Two Step Verification or Multi-factor Authentication, is used to add a layer of security to your on-line accounts. It makes your on-line data and presence more secure by asking you to prove your identity in two ways. 2FA requires you to prove your identity by entering something you know (your password) and by utilizing something that you (and only you) have (a phone or a security key). Think of using your ATM card. You have to present the physical card (something you have) and enter your PIN (something you know). In the digital world, you typically prove your identity by entering your password; however, when 2FA is enabled or required, a second layer of security requires you to prove who you are by using something you have. This can be done using your phone or a physical security key. This is much more secure than using a password alone, but it does add an extra step when you log in.

Authenticating with 2FA by…

SECURITY KEY
A security key is obtained and paired to your account. When the application asks for verification you insert your key in a USB port or connect it via Bluetooth

PHONE
Instead of a physical key, you can use your phone – one method is to set the system to text a code to your phone after you enter your password during log-in. That onetime code must then be entered to complete the log in. You can also install an Authenticator App on your phone that produces a random onetime use code.

Popular authenticator apps include Microsoft Authenticator and Google Authenticator. Google also sells the Titan Security Key with models for USB ports, USB C ports, and Bluetooth.