TWO FACTOR AUTHENTICATION: YOU WON'T BELIEVE HOW 6 NUMBERS CAN SAVE YOUR DATA

BIG SECURITY FOR SMALL BUSINESSES

YOUR PASSWORDS PROTECT YOUR DATA, BUT WHAT PROTECTS YOUR PASSWORDS?

Strong passwords are a must-have for any business, but you can add another layer of security to your online accounts by enabling two-factor authentication (often shortened to 2FA).

What is 2FA?

Two factor authentication is a system that requires you to input a temporary code when you sign in to confirm that you're the person actually accessing the system. When you turn on 2FA, you will be prompted to confirm your login to your account with a second authentication method. Unlike a password, this code will change regularly (think 30 seconds instead of never)

Step #1: Choose your Tool

The first thing you'll need to do is pick an authentication app for your phone or tablet. Companies like Google and Microsoft have authenticator apps for Android and iOS, or you can pick a tool like Authy.

Microsoft

https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/

Step #2: Turn on 2FA

Most major websites now support two-factor authentication. You'll need to enable this on all of your online accounts, but we promise that it's worth it. Navigate to your account settings for each account and check the Security or Account pages. When you turn on 2FA, you'll usually have to scan a QR (Quick Response - those black and white squares) code with your authenticator app and input the code on your phone to confirm setup. You'll also want to download backup codes for each account.

Step #3: Sign in!

Once 2FA is enabled, you'll be prompted to enter a code from your authenticator app or from your list of backup codes after you sign in with your username and password. This ensures that your account will stay safe even if someone does gain access to your password.

Click to Learn More