**2FA: When passwords aren’t enough**

Levi King

[kingle@metrostate.edu](mailto:kingle@metrostate.edu)

There are many ways to steal a password. Some are simple, like “shoulder surfing” while you type; others are complex, like attacking a database. Passwords, these short strings of letters, numbers and symbols aren’t so safe in and of themselves, which is why we shouldn’t depend on them alone. For better security, we need more than one factor on our side.

What’s a factor? In computer security, it’s anything that can be used to verify your identity. Passwords are just one factor we use to prove we are who we claim to be. But they shouldn’t be the only one.

**The Second Line of Defense**

Two-Factor Authentication (Often abbreviated as 2FA), is an old idea, patented in 1984, that’s finally becoming a common standard. To secure your accounts, you pick two factors to prove who you are, making it twice as difficult for attackers to steal from you. These factors can consist of something you know, something you have or something you are.

The first factor is, of course, something you know: a password. They can be stolen, yes. But if we ditched passwords entirely, we would be throwing a factor away, which is silly. Passwords are still a perfectly good first line of defense, as long as you follow a few simple rules: don’t make them easy to guess, don’t share them, and don’t reuse them for multiple accounts. If you find these things difficult, I suggest using a password manager to create and remember completely random passwords for you — though that’s a topic for another column.

The second factor usually depends on something you have, like your phone. After you enter your password, the website you are logging into will use your phone to send a code that only works once, whether by text message or an app. This is a one-time password, or OTP, and they change constantly. That means they're impossible for a hacker to steal from a database. They would need to steal your phone in order to get access.

The second factor doesn't have to be an OTP. It might be a different form of physical ID, like a card with a chip.

The third factor is based on something you are. If you have a new smartphone, it might have a fingerprint reader. Scanners that can read your fingerprint, retina or other unique details of your body are called biometrics, but they’re not widely used because the hardware is still rare.

**How Do I Get 2FA?**

First, find out which accounts support it. Big companies like Amazon and Google already do. Here’s a good, simple website to help you get started: www.TurnOn2FA.com

Once you’ve found a site with 2FA support, there’s usually a choice. On Amazon, you can have OTPs texted to you when you log in. If you’re worried about not having phone signal, you can use an authenticator app instead, which generates codes even when your phone has no internet.

Sensitive financial accounts might have another option: PayPal lets you use a physical security key generator instead of your phone. These small devices do nothing but make random numbers all day long, and when you need to log in, you just check what the current random number is. However, these may be less convenient than an app on your phone, and it’s up to you to purchase and keep track of these tokens.

In the end, using 2FA is very simple, but it’s not universal. Your StarID doesn’t have any 2FA options yet, though it might in the future. The peace of mind that comes along with 2FA is invaluable. I feel better knowing attackers can’t steal my identity through some random website database breach, and so will you. Don’t wait until it’s too late to set it up.