2FA OR NOT 2FA?

That is the question.

April 5, 2022
CCCGC General Meeting

What is 2FA?

Two Factor Authentication as defined by Wikipedia

Multi-factor authentication (**MFA**; encompassing **authentication**, or **2FA**, along with similar terms) is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA protects user data—which may include personal identification or financial assets—from being accessed by an unauthorized third party that may have been able to discover, for example, a single password.

Two factor authentication

What are some of the 2 factor derivations?

2FA - Two Factor Authentication

MFA - Multi Factor Authentication

2SV - Two Step Verification

What's a factor? A factor is a something unique that a person uses to access one of their accounts. This includes things like passwords or smartphones. If you have to use a password and a phone that is Two Factor. Two unique and different factors. If you have to use two passwords then you are using Two Step Verification. The Factors are the same, ie they are knowledge based but there are still two steps in the process.

Want to get confused very quickly? Here's a link to an article that explains the difference between the three derivations.

https://rublon.com/blog/2fa-2sv-difference/

Where would you use 2FA?

2FA is used as a security measure to protect your important online accounts from being hacked.

Once set up, the account requires a second factor to be used to allow access to that account.

If your user name and password are stolen, the hacker would still need access to your phone

to be able to access the account. Some common uses.

Bank Accounts, brokerage accounts, email accounts, government accounts such as Social Security, Medicare and the IRS.

I use 2FA with my Microsoft account.

I use 2SV with my AT&T phone account. I set up a pin with ATT so that anyone trying to

access the account needs the user ID, password, and the pin.

How do you set up 2FA.

In general you go to your account setting and then security.

If the account offers 2FA, that should be a choice you can select.

Once selected you may have to confirm your phone number that

they will use to send you the text with the code you need to log in.

What else can you do?

You can use an Authenticator

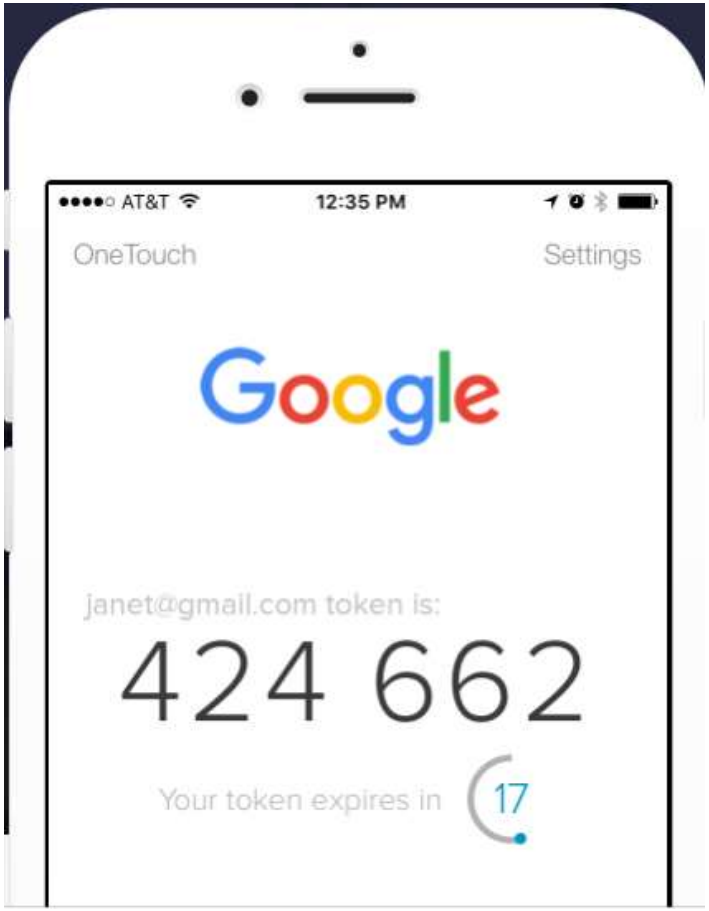
An Authenticator is an app that generates codes for accounts that you have set up. The codes changes every 30 seconds or so. When you log into an account that has an Authenticator set up, you would enter a password and then another box would appear in which you would enter the code from the Authenticator App.

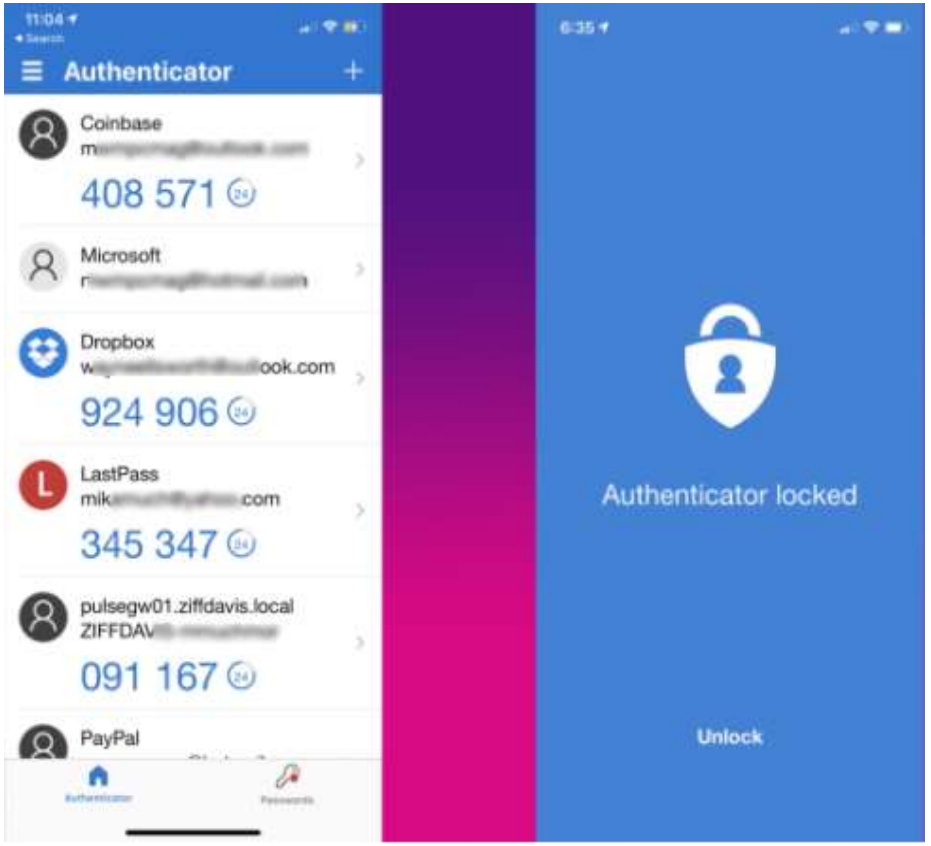
Here's a good discussion about Authentication Apps

https://www.pcmag.com/picks/the-best-authenticator-apps

Here's a good YouTube video on setting up 2FA and using an Authenticator App

https://www.youtube.com/watch?v=hlpoc3C1kWM


AT&T
12:35 PM
OneTouch
Settings
Google
janet@gmail.com token is:
424 662
Your token expires in
17


Authenticator
Coinbase
408 571
Microsoft
Dropbox
924 906
LastPass
345 347
pulsegw01.ziffdavis.local
091 167
PayPal
Authenticator locked
Unlock

Here's a good comparison of the Microsoft and Google Authenticator Apps

https://www.zubairalexander.com/blog/comparison-of-google-and-microsoft-authenticator-apps/

Not all web sites will allow the use of an authenticator so you continue to use 2FA.

It's better and safer than just using a password.

One final note. Everyone should set up a pin with their cell phone company. That then becomes two step verification, a password and a pin.

Why? Because if someone gets your login id and password, they may be able to hijack your phone. They are then potentially in a position to get you 2FA text messages from you financial institutions possibly getting them access to those accounts.

https://www.howtogeek.com/358352/criminals-can-steal-your-phone-number.-heres-how-to-stop-them/

Things To Do

1. Protect your phone with 2FA, a secondary pin or password to make that account more secure.
2. Use 2FA with as many of your accounts as you can.
3. Note that Gmail is now implementing mandatory 2FA.
4. Use an authenticator app to make some of this easier.
5. Don’t click on suspicious links.

“To be, or not to be? That is the question—

Whether 'tis nobler in the mind to suffer The slings and arrows of outrageous fortune, Or to take arms against a sea of troubles,
and, by opposing, end them?”

William Shakespeare - Hamlet