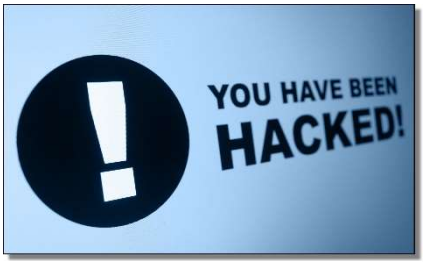
Dual Factor Authentication Nirvana

It is called Dual Factor Authentication (DFA) or Multi-Factor Authentication (MFA). Whatever you call it, it adds another step to log into ANYTHING that has confidential information. Yes, you will be using DFA or MFA to get into just about any program or site that has sensitive information. AND in most cases, you are not the one to decide if it is needed and whether you are going to use it.

MFA (that is what I am calling it from here on) is expensive for vendors to implement and support. They want to provide good security so that your data and their systems are not compromised. MFA is generally accepted as the best way to accomplish that goal right now. It, like all technology, will evolve. Right now, something must be done to stem the breaches and losses. The cost of having your systems, information or identity compromised is WAY more than the comparatively negligible cost of MFA and Password Management. Yes, I just injected a new phrase, Password Management, more on that later. The biggest investment, time on your part, Is to set up the ability to manage MFA and then a few seconds each time you use it.

If you are like most people, you are being forced to use more than one password across your logon sources whether you like it or not. There are many methods being used to keep people from using one password for everything. It is social engineering "for the common good". If you are like most people, you change a letter, add a number or character to your favorite password.



How do passwords get hacked? Mainly by what is called brute force. In brute force hacks, the longer the password, the less likely it is to get hacked. It does not matter if the password is a phrase, a name, a number letter combination or unintelligible combination of letters, numbers, and characters. The longer the password, the longer it takes to hack using brute force. Therefore, it is now generally accepted that a phrase of 12 characters or more is the best password. How long does it take to crack a password using brute force?

- "abcdefg", 7 characters: .29 miliseconds
- "abcdefgh", 8 characters: 5 hours
- "abcdefghi", 9 characters: 5 days
- "abcdefghij", 10 characters: 4 months
- "abcdefghijk", 11 characters: 1 decade
- "abcdefghijkl", 12 characters: 2 centuries

This is using standard computing technologies, not super computers.

As you can imagine, a phrase like "The Quick Brown Fox Jumped Over the Lazy Dogs Back" would be impossible to break unless the hacker was specifically testing for phrases, and in that case adding a number somewhere in the phrase would make it impossible to crack.

Knowing what is available, what best fits your lifestyle and how to use it is important. Sometimes you do not have a choice, sometimes you still do, you just need to analyze the options. That is what we are presenting here.

No one wants to use complicated passwords or MFA, but it is now a fact of life. Everyone needs to come up with a strategy based on the best information available, when it comes to passwords and MFA. You and your business need to come up with a plan to use passwords and MFA, if you don't your life associated with the technology will be complicated, confusing, and fraught with hours trying to fix access to accounts you really want to use.

The most useful MFA tool is your smart phone, and it can be your best password management tool also. There are drawbacks associated with using a smart phone with MFA and we will go over those. If you do not have a smart phone, your life will be a bit more complicated. The statement is: Your smart phone is the device you should use for MFA when you have a choice. Yes, some vendors decide for you and force you to do MFA their way. Just realize it and do what it takes to meet their demands. Swinging at windmills is a waste of time and boycotting a vendor because you dislike one thing when everything else about the vendor is awesome is counterproductive.

What is MFA?
It is another way to authenticate to the security system that you are who you say you are. It is NOT a password replacement.
What are the methods used for MFA?

- There are "Authenticator APPs" that you can download on your smart phone.
  - Some give you a code to enter
  - Some just require you to allow access with a pop-up
- You can get a text message with a code you have to enter or respond to the text.
- You can get a phone call with a code you have to enter or hit a button.
- You can receive an email with a code you have to enter
- Some ask you questions to verify who you are.

You may think that we left off Captcha, but that doesn't apply here. Captcha is verifying that you are human, not a form of MFA. Captcha is "easy" for humans but nearly impossible for machines.

To the advice. Finally.

For MFA, we recommend you download these free Apps from your phone's APP Store and group them in a folder on the main page of your phone:

- Microsoft Authenticator
  - For everything Microsoft
  - It's free
  - Don't use it for anything other than Microsoft, it can be a pain.
- Authy
  - For everything else.
  - Authy is free
  - Authy is similar to Google Authenticator, uses the same instructions and is better.

In addition, if you have over a dozen different sites or programs that need passwords, you might consider a password manager like LastPass, 1Password, BitWarden or Keeper. All of these are going to make you learn their system, but once you learn it and install the programs on all your devices, your life will be easier and more secure.

- LastPass has a free version that they try to “Hook” you with, then get you to pay around $30 a year.
- 1Password is probably the best subscription product out there and costs around $30/yr.
- BitWarden is $10 a year but is nowhere near the quality of LastPass or 1Password.
- Keeper is the up-and-comer that is making inroads against the LastPass and 1Password for $30 a year.
- DashLane is EXPENSIVE and no better than 1Password.

As you can imagine, there are drawbacks to MFA and Password Managers. If your phone gets damaged or lost, you lose access to your programs UNLESS you have set up alternative methods. When you set these Microsoft Authenticator, Authy and whichever Password manager you choose, plan to spend some time doing it right, answering all the questions and documenting everything. It WILL save you frustration and hours of your life somewhere down the road.

Now the kind of bad news.

Microsoft is requiring MFA with all its products, including Office 365/Microsoft 365.
Yes, you read that correctly. Microsoft has made the decision to force all users to use MFA and they have invested a LOT to support it. Business customers are first and we will be notifying you in the not-too-distant future when it will happen and prepare you for it.

My first reaction to this was, "I'm switching to Google Apps". I investigated it and not only are Google Apps not as "evolved" as Office 365, but they are rolling out MFP also. You can't get away from it.

Microsoft uses the Microsoft Authenticator APP for MFA, but has other options:

- **Call My Mobile Phone:** When the users receive the confirmation call, they press # in the phone's dial pad to log in.
- **Call My Office Phone:** This works like Call My Mobile Phone, but sends the confirmation call to a separate line, such as a desk phone.
- **Text Code to My Mobile Phone:** The user receives a code sent via SMS text message to their phone, then enter it in the Office 365 login form.
- **Notify Me through App:** The user can use a Microsoft smartphone app to receive and confirm the notification; the app is available for Windows Phone, iPhone, and Android.
- **Show One-Time Code in App:** This uses the same app as for the Notify Me through App option, but sends a one-time six-digit code that must be entered in the Office 365 login screen.

We recommend the Authenticator APP.

Want to learn more about MFA?
https://en.wikipedia.org/wiki/Multi-factor_authentication