2FA vs Password Manager

Using a combination of techniques to protect your password is imperative. In this article, learn why using a blend of password management and 2FA keeps your IT security locked tight.

In a recent post, we discussed some of the best ways to keep passwords protected. We mentioned the use of password managers to keep everything organized and using **2FA (Two-factor authentication)** to add extra security. But do you really need two additional tools to worry about when securing an IT network?

The Benefits of a Password Manager

One of the oldest pieces of password management wisdom is to use unique passwords and make different passwords for every site. This is a practice that everyone knows they should do but many keep passwords similar so they can remember their logins.

It's common to see people use passwords for different websites like this:

Facebook Password: **MyDogsName#1**

LinkedIn Password: **MyDogsName#123**

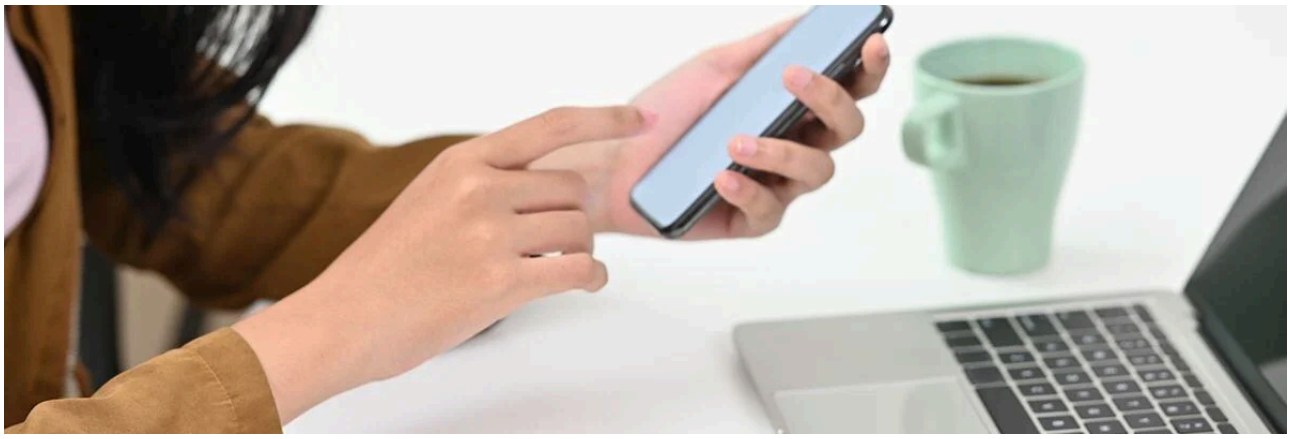
Bank Password: **ILoveMyDog123**

Sure those are three different passwords, **but they are essentially the same thing**. If a computer is able to guess one of those logins, you can **almost guarantee that it is going to guess the others as well.**

A password manager eliminates the need for you to remember each individual password. That means that you can **create extremely complex passwords** on your own, or **use a password generator to ensure that your passwords are unique and complicated.**

Now, if a brute force attack is able to guess one password **you are not totally compromised.** They will only be able to gain access to one part of your IT security network, instead of being able to access everything with a similar login.

Adding 2FA for Security



The common question we get from people is **why they need to use 2FA if they already use a password manager with unique and complicated logins.** Well, the answer is two-pronged.

1. **Your password manager has a master password that needs to be protected.**
   Whatever password manager you choose to use will need to have a master login. This will allow you to manage all of the passwords saved by that service. Protecting this password manager master password is incredibly important. If anyone is able to get your password manager master login then everything you have saved there will be stolen. Adding a second layer of the authorization will notify you if someone is trying to break in. If you do not confirm the login, then they will be unable to access your other passwords no matter what they do.

2. **Added security is always smart.**
   There is no complicated answer here other than adding steps to log in will only make you safer. Humans are notoriously lazy security managers and bad password creators. With that being said, it's always good to add an extra layer to make security even stronger.

Using a password generator does not ensure total security from every attack that comes your way. Using 2FA will alert you if anyone is ever successful and allow you to deny access before they are able to get in. This could save your personal information, or protect your business from a serious IT breach.

Why Use both 2FA and a Password Manager?

Cyber attacks are becoming more common every day. Phishing attacks rose as much as 600% following the nation's response to Covid-19, and cyber-attacks rose over 30% in the beginning months of 2020. There has never been a better time to reassess your password security.

Using a password manager and adding 2FA are both good ways to help secure your IT system, but individually they are just tools. Using both together is how you build a strong IT security infrastructure that can help protect your business from ruin. Contact us today for your cybersecurity needs.