your energy partner®
OPPD
Omaha Public Power District

SHIELD
Information Protection Newsletter

SECURE
HANDLE
INVOLVE
ELIMINATE
LEARN
DEFEND

# Improving Your Password Security

The majority of people use very weak passwords and re-use them on different websites. How are you supposed to use strong, unique passwords on all the websites you use without writing them down? The solution is a good password manager.

Password managers store your login information for all the websites you use and help you log into them automatically. They encrypt your password database with a master password – the master password is the only one you have to remember.

**Don't Reuse Passwords!**

Password reuse is a serious problem because of the many password leaks that occur each year, even on large websites. When your password gets leaked, malicious individuals now have your email address, username, and password combination that they can try on other websites. If you use the same login information everywhere, a leak at one website could give them access to all your accounts. If someone gains access to your email account in this way, they could use password-reset links to access other websites, like your online banking or PayPal account.

To prevent password leaks from being so damaging, you need to use unique passwords on every website. They should be strong passwords – long, unpredictable, and complex passwords that contain numbers and symbols.

Web geeks have hundreds of accounts to keep track of, while the average person likely has only tens of different passwords. Either way, remembering strong complex passwords is nearly impossible without resorting to some sort of trick. The ideal trick is a password manager that generates secure, random passwords for you and remembers them so you don't have to.

**What Using a Password Manager is Like**

A password manager will take a load off your mind, and free up brain power for doing other productive things rather than remembering a long list of passwords.

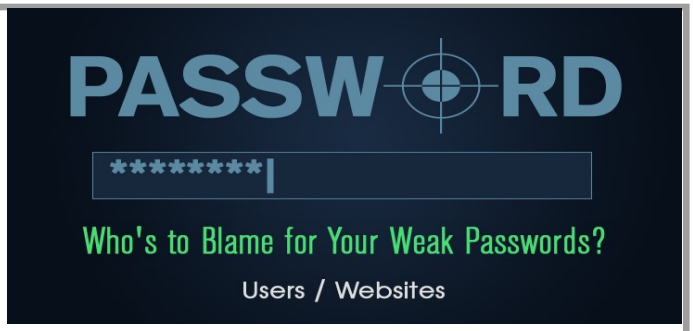

When you use a password manager and need to log into a website, you will first visit that website normally. Instead of typing your password into the website, you type your master password into the password manager, which automatically fills the appropriate login information into the website. (If you're already logged into your password manager, it will automatically fill the data for you). You don't have to think about what email address, username, and password you used for the website – your password manager does the dirty work for you.

If you're creating a new account, your password manager will offer to generate a secure random password for you, so you don't have to think about that. It can also be configured to automatically fill in information like your address, name, and email address into web forms.

Remember that web browser-based password managers aren't recommended. These don't offer the features of a dedicated password manager and many times store your password unencrypted. Avoid this risk by using a dedicated password manager and don't be an easy target.

*https://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/)*

# Methods to Create a Secure Password




Anyone who has had an ATM card, created an email address, opened an online bank account, or joined a social media website know how important passwords are. We know that passwords open the gates to our digital life, and we should never share them with other people, or anyone if we can help it. But even if we don't tell anyone our passwords, we are still vulnerable to cyber attacks if they somehow fall into the wrong hands.

Hackers have special skills and tools to infiltrate private accounts. But they typically target people who are easy prey, or individuals who have poor security practices. A weak password puts all of your accounts at risk. You can easily become a victim with a password that anybody can guess just by looking at your life. If you've used your child's birthday or your wedding anniversary as your password, chances are even your friends can guess it without a problem.

We all know how crucial it is for us to have a really strong password. The problem is, having a strong password means that we may not remember it ourselves. That's why most people never bother with including random numbers and characters and leads us down the path of using an easy word to remember.


If you're already using a password manager, you know that a good password manager takes care of all of those details for you. Use some of these basic tips to improve the passwords you may already be using that you 'think' are secure;

1.) Use longer passwords. 12 character passwords are good, but 17 character passwords are the best.

2.) Use CaPiTaLiZaTiOn and vary your choice of how and when your use it.

3.) Insert symbols in place of letters, use punctuation, and mix up where you insert numbers.

4.) Don't use pet or kids names. Avoid birthdates and family member names.

5.) Don't use a word that is found in the dictionary, use a variation of it.

6.) Use a different password for EVERY account that you have.

Remember, 90% of passwords generated by users are vulnerable to hacking so mix things up and don't be an easy target! For even more tips, tactics and recommendations visit the link below.

https://www.dhs.gov/sites/default/files/publications/Best%20Practices%20for%20Creating%20a%20Password.pdf


Using complex passwords often gets overlooked until you're involved in a compromise. By using a complex password, and changing it frequently, can be a great first line of defense. Remembering complex keystroke combinations and random symbols or characters can become challenging task for many, which is where a password manager comes in. Learn what it takes to improve your security posture and stay away from being an easy target.

**https://blog.envisionitsolutions.com/5-benefits-of-using-a-password-manager**