D.L. Evans | BANK

Protecting Your Password

OVERVIEW

It is important to remember that if someone steals your password; you could be liable for anything they do! To better protect yourself, the following information will assist you with creating a strong password and provide you with information on how to use it safely.

STRONG PASSWORDS

Cyber criminals have developed programs that automate the ability to guess, or brute force your passwords. To protect yourself, your passwords must be difficult for others to guess but at the same time easy for you to remember.

Here is some guidance:

- You must have at least one number in your password.
- You must have at least one CAPITAL letter in your password.
- You must have at least one symbol in your password.
- We recommend your passwords be a minimum of 12 characters in length, however, the longer the better.

It is strongly recommended that you use a passphrase or something similar to the example below:

My 1st child was born at St. Lukes Hospital at 7:00pm

However, we can use that sentence to create the password you see here:

M1cwb@SL@7:00pm

A passphrase, for example:

I love vanilla ice cream!

Can become:

ILoveVanillaIceCream1!

PROTECTING YOUR PASSWORDS

Keep in mind that just having strong passwords is not enough. It does not matter if you have the most complex passwords in the world; failing to take the following steps can result in your passwords being compromised:

1. Do not make yourself vulnerable. One of the most common ways for cyber criminals to steal your password is to infect your computer. Once your machine is compromised, criminals will install specialized malware on it that captures all of your keystrokes, including any usernames and passwords to online bank accounts. When you log in to your bank, your information is automatically stolen and forwarded to the cyber criminals. These individuals can then access your bank account pretending to be you and literally steal all of your money. To protect yourself, make sure your computer is actively protected. This means making sure automatic updating is enabled and you have the latest anti-virus software running on your computer.
2. Be sure to use different passwords for different accounts. For example, never use the same passwords for your work or bank accounts as your personal accounts, such as Facebook, Instagram, or Twitter. This way if one of your passwords is hacked, the other accounts are still safe.
3. Never share your password with anyone else. Remember, your password is a secret. If anyone else knows your password, it is no longer secure.
4. Never use a public computer to log into an account containing sensitive information such as your credentials, account numbers, account balances, etc. Since anyone can use these computers or access the internet, they may be infected with a malicious code that is capturing all your keystrokes. Only log into your work or personal accounts on trusted computers you control. The same goes for free wifi. Anyone can access your device and the data it stores while you are using free internet service.
5. At times you may have so many passwords that you cannot remember them all, and storing them may be your only option. If you write them down, be sure to store them in locked location that only you have access to; never store them in public view. Another option is to store them in encrypted applications designed to store passwords on your computer or smartphone.
6. Exercise caution when websites require you to answer personal questions. These questions are often used if you forget your account password and need to reset it. The problem is the answers to these questions can often be found on the Internet, such as your personal Facebook page. So make sure that if you answer personal questions, you use only information that is not publicly known. If the website provides other password reset options, such as SMS messages to your smartphone, you may want to consider these alternatives.
7. If you believe your Online Banking password has been compromised or if you have reason to believe it is no longer a secret, contact a D.L. Evans Bank representative at 1-866-661-5463 and change your password immediately from a computer you control and trust.

D.L. Evans Bank
Member FDIC