UPPER PENINSULA
STATE BANK
You're Going To Like It Here!

Using Strong Passwords

We live in a password-driven world, where between 4 and 20 characters are the difference makers in whether you are able to access your data, communicate with friends, or your online purchases. Passwords protect every part of your life "*online*". If you don't treat them properly, you could be exposing yourself to unwanted risks.

Passwords keep strangers off our computers and smartphones. They keep criminals from reading (and writing) our email, updating our Facebook status, and cleaning out our bank accounts. The longer the password, the more combinations of letters, numbers, or symbols you use, and more frequency at which you change them, the better off you will be.

Why should you do this when it's so easy and more convenient to just use the same simple password for everything? Well - Imagine that you had one key that unlocked your house, your garage, your office and your car. Then, to make sure you always had the key handy, you made about 80 copies. And engraved your address on every one before leaving them in convenient locations. That's about the level of security you have if you use the same easy-to-guess passwords for multiple purposes. Far too many people do just that.

To help you create strong passwords, we put together some helpful hints that can assist you in this process.

Avoid Common Passwords
Don't use words that can be found in a dictionary, words or letters that appear on a keyboard ("1234" or "qwerty"), names of relatives, kids, birth dates, graduation dates, car license plates, etc. – these are all things hackers would try first.

Strong Password Suggestions

- You should use a string of text that mixes numbers, letters (both upper and lower case) and special characters.
- Password length should be at least 8 characters or more (the longer it is the harder it will be to hack).
- Spell a word backwards (i.e. New York becomes kroywen), substitute some numbers for letters, add some capital letters and special characters – "kroywen" becomes "Kr0yw3^")
- Use substitution characters (i.e. @ for a, 3 for E, 8 for B) or anything that makes sense to you.
- Use a phrase – "Don't worry, be happy!" becomes "D0^tw0rRyB3h@pPy!"
- Use acronyms from a phrase of your choice. "We didn't start the fire, it was always burning" becomes "wdstfiwab" based on the first letters of each word.

Once you have a strong password you like and can remember, it can be very tempting to re-use it everywhere – ***DON'T***! Use a different password for all of your accounts. This way if one of your passwords is compromised, the bad guys won't have access to all of your other passwords. A simple trick would be to individualize it for each place you go. Simply take the first three letters of the site or service you're entering and at them to the beginning or end of your password. For example, for access to Amazon use "Kr0yw3^AMA"; for email use "Kr0yw3^EMA", for Facebook use "Kr0yw3^FAC", etc.

Make sure you change your password every few months. Even if your password is strong, if you have shared it with anyone (a co-worker, boyfriend/girlfriend, or spouse) and they suddenly become ex-coworkers, or ex-BF/GF, or ex-spouse – you can probably guess what may happen next. When an old password expires, ***DO NOT*** increment a number at the end. It may be one of the easiest ways to remember your password, but hackers know this trick and are counting on you to use it.

Other Helpful Tips

- Always be careful when answering personal questions. These questions are often used to help you reset your password if it is forgotten. Try not to use any information that is publicly available when answering these questions. If the bad guys can find it, they don't need to guess your password, they can just reset it.

- Enable Two-Factor Authentication if possible. Two Factor Authentication relies on something you know (your password) and something you have (typically your cell phone). When you sign into a system with Two Factor Authentication enabled, you will often receive a text message containing a one-time use key. Only after correctly entering the one time use key will obtain access to the service.

- Don't write your password down. If someone has physical access to your computer, often the first place to look is under the keyboard and in your drawers. While it may make it easier to remember your password, it provides others an opportunity to easily gain access to your valuable information.

- Utilize a password manager to help keep track of passwords. There are many services and applications available to help keep track of all of your different accounts securely. These applications securely store your passwords and grant access through a "Master Password". It is important that this master password is strong and uses the above practices where available. Some of the more popular password managers are *PasswordManager*, *1Password*, *LastPass*, and *KeePass*.   Before utilizing a password manager for business purposes make sure you check with your supervisor to use an officially approved product.

Make strong passwords your new habit and your online life will take a step in a more secure direction.

References:
- Spector, Lincoln. "Learn to Use Strong Passwords." *PCWorld*. PCWorld, Oct. 2012. Web 22 Oct. 2012.
- Griffin, Eric. "Password Protection: How to Create Strong Passwords". *PCMag*. PCMagazine, Nov 2011. Web 29 Nov. 2011.