WHY CHOOSE A STRONG PASSWORD?

Strong passwords are key to protecting your personal information. Once a cybercriminal has your password, they will have unlimited access to unlock and steal your personal information, inflicting untold damage to your wallet and reputation. Criminals often employ sophisticated tools to help them decipher passwords – outsmart them by reading the tips below and create passwords that are challenging to crack.

HOW DO I CREATE A STRONG PASSWORD?

Strong passwords should be easy for you to remember, but difficult for others to guess. When choosing passwords, make sure they meet the standards below:

LENGTHY – Longer passwords are more difficult to crack.

MIX IT UP – Use mixed case letters, numbers, and special characters in each of your passwords. Note that common substitutions, like using $ for S, are so frequently used that they are easy for hackers to guess.

DON'T MAKE IT EASY – Try to be unpredictable. Common words or personal details are predictable. Choose words that are hard to guess.

AVOID REPETITION – Do not repeat the same password across your accounts. That way, if one password is stolen, it cannot be used elsewhere. If you must reuse passwords, do so only for accounts that have little importance.

USE A PASSPHRASE – Instead of a password, consider using a passphrase. Phrases are longer than words, and the added length will increase its complexity and make it more difficult to crack. You might use a phrase you were taught from your youth, your favorite movie quotation (Example: ETphonehome) or song lyric (Example: OhSayCanYouSee), or an original phrase you can easily remember (Example: "PitSteelersAreTheBestTeamInTheUS").

EXTRA STEPS TO PROTECT BANKING ACCOUNTS

ENABLE MULTI-FACTOR AUTHENTICATION – When available, take advantage of this additional level of security that authenticates you as the account owner using a one-time use code sent via a text/email, a code-generating fob or app, or biometrics (fingerprint scan, face/voice recognition, etc.).

SELECT A PASSWORD AND USER ID THAT ARE UNIQUE TO YOUR BANKING ACCOUNTS – Never use the same password and user ID to conduct your banking as you do for any other site. Reusing the same log-in credentials on different websites, such as social media sites or email, puts your credentials at risk, as well as any other account using those same credentials.

SET UP ALERTS – This is a security option to receive an email and/or text message notification of key activity on your bank accounts and credit cards. Check with your bank and card issuers if this security feature is available.

CHOOSE SECURITY QUESTIONS WHEN AVAILABLE/OFFERED – Select security questions with answers that cannot be found on public websites or guessed. For example, if you've ever noted your favorite color or favorite food on a social media website, this would not make for a good security question.

ADDITIONAL PASSWORD TIPS

NEVER GIVE OUT YOUR PASSWORD – Legitimate companies should not contact you by phone, text or email to ask for your password. If you are contacted and asked to provide sensitive financial information, such as passwords or PIN numbers, first call the company to check the legitimacy of the request, using a known, legitimate phone number.

KEEP YOUR PASSWORD SAFE – Keep passwords in a secure place and out of sight. If possible, memorize them rather than write them down.

PNC BANK