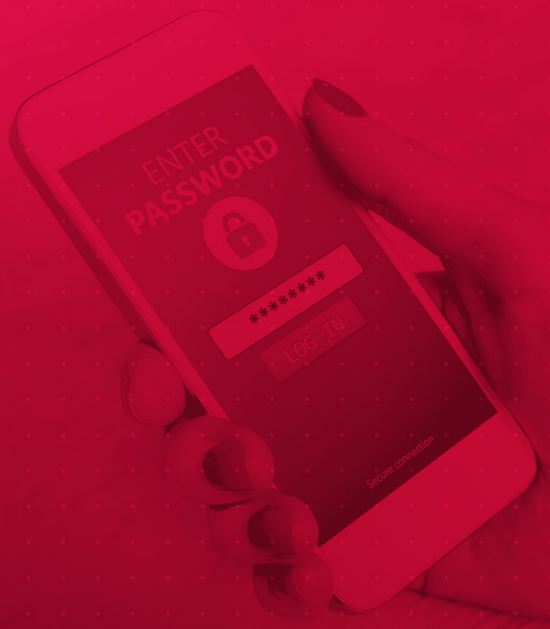
Step Up to **Stronger** Passwords



CYBER SECURITY MAY 2017

A password is often all that stands between you and sensitive data. It's also often all that stands between a cybercriminal and your account. Below are tips to help you create stronger passwords, manage them more easily, and take one further step to protect against account theft.

ALWAYS ▸ Use a unique password for each account so one compromised password does not put all of your accounts at risk of takeover.

GOOD ▸ A good password is 10 or more characters in length, with a combination of uppercase and lowercase letters, plus numbers and/or symbols — such as pAMPh$3let. Complex passwords can be challenging to remember for even one site, let alone using multiple passwords for multiple sites; strong passwords are also difficult to type on a smartphone keyboard (for an easy password management option, see "best" below).

BETTER ▸ A passphrase uses a combination of words to achieve a length of 20 or more characters. That additional length makes its exponentially harder for hackers to crack, yet a passphrase is easier for you to remember and more natural to type. To create a passphrase, generate four or more random words from a dictionary, mix in uppercase letters, and add a number or symbol to make it even stronger — such as rubbishconsiderGREENSwim$3. You will still find it challenging to remember multiple passphrases, though, so read on.

BEST ▸ The strongest passwords are created by password managers — software that generates and keeps track of complex and unique passwords for all of your accounts. All you need to remember is one complex password or passphrase to access your password manager. With a password manager, you can look up passwords when you need them, copy and paste from the vault, or use functionality within the software to log you in automatically. Best practice is to add two-step verification to your password manager account. Keep reading!

STEP IT UP! ▸ When you use two-step verification (a.k.a., two-factor authentication or login approval), a stolen password doesn't result in a stolen account. Anytime your account is logged into from a new device, you receive an authorization check on your smartphone or other registered device. Without that second piece, a password thief can't get into your account. It's the single best way to protect your account from cybercriminals.