If it's easy to remember, is it also easy to steal? Not necessarily, says Brunswick's **SARAH RALL**

Hey!uNeedaNewP@s$word

Passwords are the first and perhaps most important line of cyber defense, and faulty passwords have caused major headaches and big financial losses for individuals, companies and governments. An industry report from 2017 found that 81 percent of breaches were "leveraged by a weak, default or stolen password."

What makes a good password? The better question to ask might be: What makes a bad one? The top three entries on SplashData's list of 2017's worst passwords: "123456"; "password"; and "12345678." It takes cyber-criminals seconds to hack these.

If you are a chronic password re-user, your Netflix account could grant access to your bank account, email or healthcare records. Conventional wisdom is that a strong password is just a string of random characters. But it's not exactly easy to remember "T8#ks&4hd" – making that password trick somewhat impractical.

Thankfully, there are other solutions:

Passphrase is the new password. A passphrase is a long string of words or characters much easier to remember and much harder to hack. A sentence, for instance, "1ShouldUseAStrongPassword!" is significantly more difficult for a computer or hacker to crack than a random grouping of numbers, capital letters and obscure characters.

SARAH RALL is an Associate at Brunswick Group specializing in privacy and data security. She is based in the firm's San Francisco office.

Complex doesn't have to be confusing. Complexity in passwords has more to do with length than anything else. Using arbitrary characters might make your password look hard to break – but it can also make it incredibly difficult to recall. There's no need to devote brain space to an obscure string of characters that you forget every time you try to log in to your account – and you can spare yourself the needless time and effort it takes to endlessly reset forgotten passwords.

Mix it up. While it might be more convenient to use the same password for all accounts, it puts your personal information at serious risk. Passwords should be changed frequently to stay cyber safe and should be unique to each site.

(Memory) tricks of the trade. Song lyrics and movie quotes always seem to stay in the brain longer than necessary – use this to your advantage. Pairing your favorite movie quote or song lyric with the year it came out is a simple technique to create a strong passphrase: "MayTheForceBeWithYou!1977."

Another trick is positive association. If you're going on a trip to Thailand with your best friends in October, you might use something like: "CountdowntoThailand<3BFF10!"

If you're having trouble remembering a pin number, you can use a silly association to help jog your memory; if your bank pin is 4101, for instance, you might picture four elephants running wild on the 101 freeway.

Lock it up. A post-it note on your desk listing your password isn't keeping your data secure. Password managers such as Dashlane allow you to securely store your passwords and only remember one master password. Most password vaults also offer tools to generate strong passwords that will then be stored and secured and allow you seamless access to your many accounts. With Dashlane, the master password isn't stored on your computer or the company's servers, so it's harder to steal. The service also requires you to log on from an approved device. If you try to log in from a new one, it will ask for two-factor authentication.

There's no simple answer to securing your identity across all of your professional and personal accounts. But complexity is your friend, and the best passwords require a layered approach. Computer processers can run billions of combinations per seconds to try and crack your password, but a little extra effort from you can go a long way in protecting your information.

ILLUSTRATION: PABLO AMARGO