Securing your Password

Your passwords grant access into your personal kingdom, so you are probably thinking, what are the best practices to create a strong password to protect your accounts.

Let's look at the various ways passwords can be hacked.

Cybercriminals have several methods to hack your password, but the easiest one is simply buying your password from the dark web. This is a big business, selling and buying your login credentials on the black-market, and if you've been using the same password for many years, chances are it's been compromised; but if you've been wise enough to keep your passwords off the aggregated market lists, cybercriminals have to crack them, and if that is the case, they're bound to use one of the methods I will explain below.

Brute Force Attack

This attack tries to guess every combination in the book until it hits on yours. The attacker uses a software program to try and use as many combinations possible in as quick a time as possible. Hackers have unveiled computer programs that can crack 8-character passwords in less than six hours. Attempting over 300 billion guesses per second. Generally, anything below 12 characters is vulnerable to being cracked; hence why it is important to have a longer password character.

Dictionary Attack

This hacker is essentially attacking you with a dictionary, whereas a brute force attack tries every combination of symbols, numbers and letters, a dictionary attack tries a prearranged list of words such as you find them in a dictionary. If your password is indeed a regular word, you'll only survive a dictionary attack if your word is wildly uncommon in multiple phrases.

Phishing

The most awful of tactics is when a cybercriminal tries to trick, intimidate, or pressure you through social engineering into doing what they want. A phishing email may tell you that there's something wrong with your credit card account, then direct you to the click a link, which takes you to a fake website built to resemble your credit card company. The scammers stand by, hoping the ploy is working and that you'll now enter your password. Once you do, they have it. Phishing scams can try to entrap you through phone calls too. Be leery of any robocall you get claiming to be about your credit card.

Now that we know how passwords are hacked, we can create strong passwords that can outsmart each attack. (Though the way to outsmart a phishing scam is simply not to fall for it). Some basic rules.

Never use sequential numbers or letters, come up with unique passwords that do not include any personal info such as your name or date of birth. Keeping in mind the nature of a brute force attack, you can take specific steps to keep them at bay:

- *Making the password long is the most critical factor.*
- *The more you mix up letters (upper-case and lower-case), numbers, and symbols, the more potent your password.*
- *Avoid using common substitutions as password crackers understand the usual substitutions. Whether you use DOORBELL or D00R8377, the brute force attacker will crack it with equal ease.*

Ensure your password is not just a single word, multiple words will confuse the attacker and more importantly, use multiple phrase methods with a twist. Choose bizarre and uncommon words. You can add random characters in the middle of your words or between the words.

Security-conscious websites will hash its users' passwords so that even if the data gets out, the actual passwords are encrypted. Other websites don't bother with that step. Before starting up accounts, creating passwords, and entrusting a website with sensitive info, take a moment to assess the site. Does it have *https* in the address bar, ensuring a secure connection? Do you get the sense it is up on the newest security standards of the day? If not, think twice about sharing any personal data.

I also have a separate blog on multi-factor authentication (MFA) which adds an extra layer of protection (which becomes your first layer of protection should your account details ever get leaked). These have become the new industry standard for effective security. The best MFA method is to use a specialized app for your smartphone.