Commercial Bank

Creating Strong Passwords

Passwords have become an integral part of our lives, whether logging into work stations, online banking, personal email, or even our phones. Password strength is an important component in protecting against fraud, but a frightening number of online users are still using predictable passwords.

Common Passwords

Data breaches are now a regular news story, which prompted SplashData to analyze over 5 million passwords that were leaked online during 2018. Their research showed that the following 25 passwords were the most commonly used; each of which could be cracked by a fraudster in a matter of seconds:

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou
11. princess
12. admin
13. welcome
14. 666666
15. abc123
16. football
17. 123123
18. monkey
19. 654321
20. !@#$%^&*
21. charlie
22. aa123456
23. donald
24. password1
25. qwerty123

How Fraudsters Attack

It's far easier to create a strong password if you understand how a cyber-criminal might try to hack your account. The hacking process has been industrialized and the majority of compromises are now completed by automated software.

The hacking programs start by trying the most frequently used passwords, before progressing into common words and phrases, such as people's names, places and sports teams. The program then proceeds to work through all of the words in the dictionary, before finally attempting millions of combinations of random characters, until the password is cracked or the hacker moves on to an easier target.

The below examples illustrate how long it would take a hacker with a common home computer to crack each password:

password	1 second	My P4ssw0rd	19 minutes
Password	1 second	Str0ngp@ssW0rd	13 days
password1	2 seconds	Th15izmyP4ssWord	8 years
password17	3 minutes	A_Str0ng p@ssW0rd	33 years
Password2017	3 minutes	Cr34teAStr0ngp@ssW0rd	400 years

Tips for Creating a Strong Password

- Passwords should be at least eight characters long and include a combination of letters, numbers and symbols. As a general rule, the longer the password, the stronger it becomes.
- Alternating between upper case and lower case letters helps to strengthen the password. For example, the word 'transfer' could be typed as 'tRAnsFeR'.
- Use "hacker speak" by substituting letters for similar looking numbers or special characters. For example, the word 'banking' could be typed as 'b@Nk1nG'.
- Basing your password on a phrase can help you remember more complex combinations. For example 'HumPty dUmpty S@T'.
- Another good way of remembering a more complex password is to think of a sentence and then use the first letter of each word. For example, 'Boston is 4 hours from New York City by car' could be typed as 'Bi4hfNYCbc'.

Common Mistakes to Avoid

- Do not use personal information, common words, names, sports teams or places in your passwords.
- Adding a single digit number to the end of a well-known word (for example 'computer1') does not make it any more secure.
- Do not reuse the same password for different online accounts, as a single breach could result in multiple compromises.
- Never write down your passwords; they can easily be stolen from your computer or desk.
- Do not share your passwords with friends, colleagues, or anyone who requests this information over the telephone.