## **Password Best Practices**

It's important to keep up with your "cyber hygiene" to ensure you don't become a victim of digital fraud. The best strategy you can use to avoid becoming a victim is to use different passwords and usernames.

Try thinking of a sentence or a saying and then choose a password that takes certain characters from that:

 Will the Chicago Bears ever win another Super Bowl? This can be changed to ?WtCBewaSprBwl20

Think of a line from a song or book that you know by heart and select characters from that (*did you know you can use spaces as characters?*):

• Do you believe in love (Huey Lewis) can be changed to **D** u b i luv 2?

Avoid choosing a password that spells a "dictionary" word. But, if you must, then:

- Introduce "silent" characters into the word. Example: va7ni9llaisc3am
- Deliberately misspell the word or phrase. Example: **chokluttmilc**
- Choose a word that is not composed of smaller words.



## **Password Hints**

- Never send a password by email, instant message, or any other means of communication that is not reliably secure.
- If you don't want to memorize multiple passwords, consider using a password manager. The best password managers will automatically update stored passwords, keep them encrypted, and require multi-factor authentication for access.
- Don't store a password on the device it is designed to protect.
- Passwords should be at least 12 characters long but 14 or more is better.
- It's ok to write your passwords down, as long as you keep them secure. Don't write them on sticky notes or cards that you keep near the device the password protects, even if you think they're well-hidden; they could be discovered.

Do you have your passwords in your cell phone, maybe in the memo section? What if you lose your phone? Make sure your phone is protected too by using a secure PIN, or fingerprint or

facial recognition if your phone offers it. Consider removing any passwords you have stored on your phone.

## More on Passwords: Sometimes the Longer the Better

This chart proves that longer passwords are more effective:

## TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years



-Data sourced from HowSecureismyPassword.net