How Can Hackers Gain Access to Passwords?

Dictionary (wordlist) Attack - This involves hackers using a program that tests lists of popular words and passwords against your password until one is successful or the list is exhausted. Hackers can also alter these phrases using rules to target typical behaviors, such as changing a "E" to a "3" or attaching a character that is frequently used, such as "1" or "!"

Brute Force Attack - Unlike a dictionary attack, which works word by word, a brute force attack works letter by letter, trying every possible combination of characters to guess the password. Common or readily guessed passwords are frequently the starting point of brute force attacks, which then move on from there. This is one of the most common attacks, and generally the easiest to perform.

Rainbow Table Attack - Password data can be protected by a method called hashing. Hash algorithms are used almost like a digital fingerprint of a file's contents and used to ensure that the file has not been hacked. With a rainbow table attack, hackers use a collection of pre-hashed, frequently used passwords to breach confidential data.

Credential Stuffing - When a hacker uses lists of stolen credentials from other online services to find a match, this is known as credential stuffing. This method depends on reusing passwords. Online databases of stolen credentials are widely offered for purchase and sale by hackers.