Problems with password

I don't need to explain what password really is. Hence, I will be summarizing the problems that password have/has.

1. Users won't choose long passwords as it's hard to remember
2. Users won't choose passwords that have been rarely used by public
3. Users will reuse any passwords that they have been used

Majority of the users use password to login/sign up for an online service. It's uncertain whether the services use cryptography hashing (standard and safest way) to produce and store the fingerprint.

4. Let's say they don't use cryptography hashing or use improper cryptography hashing to generate and store the fingerprint and the service provider servers get hacked. What you can expect is that all passwords that were chosen by the users get stolen and possibly was auctioned through dark web by using cryptocurrency. This whole incident can be summarized as "data leakage/data breaches", this does not only limit to passwords, it can also apply to many of the private information that users willingly submit to the service provider.

If someone buys that list of passwords and it happens to be your password is in that list. You use that password into logging into any online services. You may start to get the idea. Users will not bother with choosing passwords that are not in any of the data leakage/breaches incident.

5. If the services that users use did indeed uses proper cryptography hashing to produce and store the fingerprint. Let's say the server gets hacked, it may take considerable amount of time and energy to keep on feeding potential password then get its output and compare with the fingerprint stored.

Users might start to think, "Oh goodness, I appreciate the service provider uses proper cryptography hashing to protect my passwords". Hang on a minute.., this case is also similar to problem number 4. Even if attacker/hacker is trying to guess what your password could be, it's not recommended to use the password that has been leaked in properly protected format.

The truth is.., users won't care.

6. Due to the presence of PIN or numbers that bank uses to request verification from users, many users will stick to their old good fashioned bad password mindset and practices. If your passwords are good and strong, you wouldn’t need to even rely on PIN or numbers.

You may or may not want to see if your passwords are in that big list. Here’s a link. (https://haveibeenpwned.com/Passwords)

If you happen to play with cryptography hashing through the website I provide, excluding the algorithm that starts from ripemd128 to the lowest algorithm, all the algorithm starting from md2 to SHA256 should not be used by developer anymore. If the developer happens to use any of the algorithms, the chances are it will be in that big list of stolen passwords.

The first problem which is good password requires a long numbers of characters. However, the minimum length of good password has been changed since 2016. For more information, you can refer to passwords topic on ComputerPhile YouTube channel.

What is passphrase?

Passphrase was a better replacement for passwords. It intends to solve the good and strong passwords user experience aspect by making it friendlier to users.

A strong password generally appears like this.
MEP\6+;=jgqxZMzh^)-2&y/:h{y@"k

A passphrase generally appears like this.
gogh scab all avail myself menu worth fairy cathy glow jade qua place

This is the old words list. (https://theworld.com/~reinhold/diceware.wordlist.asc)

This is the new words list.
(https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt)

The idea of passphrase was to roll a dice six times to randomly choose a single word that is available in the list. The list mostly contains English words and occasionally some symbols and numbers. It’s friendlier to users as they need to memorize only the English words but not some nonsensible mixture of characters, symbols and numbers.

In 2018, Computerphile makes a video about Diceware & Passwords. In that video, Dr Mike Pound stated 4-5 words chosen by rolling dices was consider a good and strong enough replacement to password. (More details refer to this link https://www.youtube.com/watch?v=Pe_3cFuSw1E)

If there’s a need to add more words, the security of the passphrase will only increase. In cryptocurrency wallet and in some cases, users will realized that the developer chooses 12-15 words that exist in the passphrase list.

Passphrase is better than password in all aspects but not many websites or services support the use of passphrase as we know some of the services force users to include symbols like “!@#$%^&*()” and in some cases include numbers as well.

I am not a good explainer in explaining the difference between passphrase and passwords. Hopefully, someone can explain better than I do.

Most of the problems that exist in passwords generally do not exist in passphrase except problem number 4th that exist in password. Users can only blame developers/companies/corporate at this point and there’s nothing they can do.

Common drawbacks of password and phrases

1. When users type in their password/passphrase, it’s a risk as their keyboard might record the buttons that they pushed on the keyboard which will reveal the potential password/passphrase.

2. When users feel that remembering them is a disaster, you can expect them to post a list of their passwords that has been written into a text file and upload it into free storage such as Google Drive or other applicable storage.