**How should we stay updated to cope with cybercriminals?**

Each coin has two sides. While tossing a coin, we already know, it is going to be in someone’s favor and someone is losing for sure. The person who invented Nuclear power never wanted people to misuse it but eventually, it was the reason why WWII had such a harsh end and which resulted in a cold war. The same happened with the one who invented the internet. Nobody thought this network of interconnected devices that are at remote locations with no physical contact can harm somebody but alas, it eventually happened.

The Internet introduced the world to various terminologies such as Websites, Online Banking, Cashless Payments, Bitcoin, WIFI, and various others. While all these seem to be a blessing to us all, it did not take long to make it a curse.

People were less careful at the initial stages of the internet and they used to keep very predictable passwords which resulted in people stealing the online information of people. Then we came to know about how people brute force the passwords which meant the traditional password system needed an update. Another problem that was concerning was how people were not worried about openly posting their sensitive information, photos that were so easy to steal, and the integrity of the INTERNET was at risk. But we can be slightly cautious to be on the brighter side and can ensure we don’t fall prey to such jumla’s.

1. **Stronger Passwords -** Passwords should be such which cant be predicted and one should keep it as long and complex as possible. Also, one should use a different combination of words, numbers, special characters so that there is no chance someone can even guess what the password is. A strength of the password is dependent upon its unpredictability, length, and complexity.
2. **Two-step Verification -** Single passwords were being brute forced so easily that it Was essential to introduce a new type of password verification which included more than one layers of security which were later called two-step verification where the only password is enough to enter the system you have to confirm your integrity by a secondary source this insurance that only authorized person is entering the system and not can unauthorized personnel.
3. **Limited use of public Wi-Fi -**  Big companies used Wi-Fi for marketing where they ask people their phone numbers to enter the system. There is a very strong chance people can break through and access your phone information which is harmful so we should avoid using such public Wi-Fi is to ensure our security.
4. **Optimal use of the resources we have -** We are lucky enough to experience this digitalization and globalization but we should be careful while using these resources which are provided to us and use them optimally for only what is needed**.**

**Content Writer,  
Hardik Yewale**