‘Cybercrime’ also known as computer crime involves a wide range of criminal activities that are carried out by using and/or targeting a computer or related system especially illegally to access, transmit or manipulate data.

Some cybercriminals conduct cybercrime through the dark web but it is not the case all the time. Some of them use public platforms such as social media to gain access to your system. Some of the examples are ransomware attacks, malware attacks, identity theft, crypto mining, crypto-jacking, manipulating or leaking data, privacy violation, human and sex trafficking, selling drugs or weapons online, etc. For example, if you have ASIC miners from Australia for your cryptocurrency mining, you would need to have the dedicated software to protect your mining rig from it. It must be noted that the victims of cybercrime include individuals, organizations and businesses – almost everyone from all corners of life. Just like how other kinds of crime can impact your life (and are usually the kinds you’d need to view website details to learn more about), becoming a victim of these things can be very serious.

The best thing to protect from cybercrime is to take some precautions. If you are using the internet, then definitely you should be aware of the following tips to protect yourself from cybercrime.

1. Use a Total Anti-Virus Protection

Use good anti-virus security to protect against malware including ransomware and viruses.

2. Passwords

Always use a strong password and ensure you don’t repeat your password on multiple websites.

3. Keep Your Software Updated

Updated software is highly important for the operating system and internet security software. Cybercriminals always try to exploit defects in the software to get access to your system.

4. Social Media Settings

All personal information on social media platforms should be kept locked. Apart from this, the less information is shared publicly, the better it would be.

5. Protect Your Identity

Identify theft occurs in situations where you will be prompted to give your personal information over the internet. A VPN can also help you to protect the data you send and receive online.

6. Keep up to Date on Major Security Breaches

If you are doing business through a website that has been impacted by a security breach, find out what information hackers accessed and accordingly change your password immediately.

7. Educate & Monitor Kids

Teach your kids about the acceptable use of the internet without blocking them from using the internet. They should be aware of any kind of illegal activity happens like online harassment, stalking or bullying. Similarly, be careful while sharing your child's personal information as identity thieves often target children.

8. Understand What to Do If You Become a Victim

If in any circumstance, you believe that you have become a victim of cybercrime, then the first thing to do is to inform the local police. Similarly, if you believe that criminals have stolen your identity, then alert the companies and banks where the fraud occurred and place fraud alerts and get your credit reports.

9. side note

In a way, fighting cybercrime is everyone's job. So, consider it as an obligation and be a part of the fight against cybercrime.