With advancement in technology, it is now easier than ever before for cyber criminals to access your private information. When it comes to cybercrime, there are multiple ways in which cyber criminals can attack your network. Some of the most common ones include malware and ransomware, phishing, social engineering scams, Denial of Service (DoS) attacks, Man-in-the-middle, and Zero-day exploits. It is important for organizations to have awareness of these and all other threats faced by their networks and to ensure **secure devices** within the network.

Here are 5 essential measures that can prevent cyber criminals from launching successful cyber attacks on your network.

1. **Use Password Best Practices**

Weak passwords are one of the most common reasons of a data breach. However, using password best practices to [**secure devices**](http://www.cardzgroup.com/ContactSmartCard.html) is a simple yet often overlooked practice. To protect a business from cybercrime, it is important to ensure the use of strong passwords across your workplace and to change them every six months. Using common passwords and not changing them regularly can make your organization an easy target for cyber criminals.

Here are some tips on how you can follow password best practices.

1. Never use same password for more than one accounts.
2. Use a combination of numbers, letters and symbols when keeping a password.
3. Avoid using personal information in your password that can be guessed such as, name initials, date of birth, organization name, your pet’s name, etc.
4. Do not keep weak passwords such as ‘12345’, ‘password’, or ‘qwerty’.
5. **Install Anti-Malware Software**

Malware includes multiple threats including viruses, worms, ransomware, spyware, trojans, bots, and adware. Anti-malware software helps detect and remove malware from infected devices. It is important that all devices are installed with updated anti-malware with latest patches to help prevent your data from being stolen.

The use of antimalware software is far beyond merely scanning a file for malware. It can also prevent a malware attack from happening by scanning incoming data and preventing malware from getting installed and subsequently infecting a computer. Advanced antimalware programs can also protect against ransomware attacks.

Antimalware software applications can help users in the following ways:

* Preventing to visit malicious websites by warning them that the websites may contain malware.
* Preventing malware from spreading within a network from one computer system to another.
* Providing insight into the infected programs and the time that is required to remove them.
* Providing details of how the malware compromised the network or the computer system.

1. **Regularly Back Up Your Data**

Regularly backing up data is important to protect it against being stolen or lost. A recent data backup can be restored if it is ever compromised by cyber criminals. It can also protect you from paying huge amounts of ransom to hackers in case of a ransomware attack. Data can be backed up using a number of ways, such as local backup or online backup.

Online backup is stored in the cloud and is a preferred option. The data can be backed up on a remote server and accessed from any location. An online backup is also usually automated, which means that the data is regularly backed up at regular intervals without requiring manual updates.

1. **Monitor Network for Suspicious Activity**

As a proactive measure to keep your business protected from cyber-crime, it is important to keep monitoring your network for any suspicious activity. If any unusual or strange activity comes under observation, take steps to prevent cyber criminals from gaining access to your system.

To monitor your network for suspicious activity, take the following essential steps:

* Use firewall to keep network intruders away.
* Install security software and patches to prevent and detect potential attacks.
* Review server data and logs at regular intervals to look for any unauthorized activity.
* Put up automatic alerts and Advanced Threat Detection to get immediately notified in case of any suspicious activity in the network.

1. **Train Employees to be Vigilant about Sharing Personal Information**

Employees need to get regular security awareness trainings on how they can recognize and avoid threats from cyber criminals. The most important measure in this regard is to be careful about what personal information they share online, since it can be misused for accessing the business network. Never give personal details such as date of birth, family details, or the model of your cell phone. Keeping your personal information as private as possible can help prevent hackers from accessing your sensitive data to a great extent. It is also important to never make your personal information visible for public on your social media accounts.

**Conclusion**

As technology advances, hackers also come up with new ways to infiltrate into organizational networks and gain access to sensitive data. Hence, it is important to stay updated with emerging security threats and protect your data from being compromised.