List of ways to prevent security breaches and other malicious intent to ensure a better network security

* **Change default passwords.** Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily available to obtain online, and so provide only marginal protection. Changing default passwords makes it harder for attackers to access a device. Use and periodic changing of complex passwords is your first line of defense in protecting your device.
* **Restrict access.** Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses. Consult your user documentation for specific information about enabling these features. You can also utilize the “guest” account, which is a widely used feature on many wireless routers. This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.
* **Encrypt the data on your network.** Encrypting your wireless data prevents anyone who might be able to access your network from viewing it. There are several encryption protocols available to provide this protection. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices. WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.
* **Protect your Service Set Identifier (SSID).** To prevent outsiders from easily accessing your network, avoid publicizing your SSID. All Wi-Fi routers allow users to protect their device’s SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer’s default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.
* **Install a firewall.** Consider installing a firewall directly on your wireless devices (a host-based firewall), as well as on your home network (a router- or modem-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall—a host-based firewall will add a layer of protection to the data on your computer.
* **Maintain antivirus software.**Install antivirus software and keep your virus definitions up to date. Many antivirus programs also have additional features that detect or protect against spyware and adware.
* **Use file sharing with caution.**File sharing between devices should be disabled when not needed. You should always choose to only allow file sharing over home or work networks, never on public networks. You may want to consider creating a dedicated directory for file sharing and restrict access to all other directories. In addition, you should password protect anything you share. Never open an entire hard drive for file sharing.
* **Keep your access point software patched and up to date.**The manufacturer of your wireless access point will periodically release updates to and patches for a device’s software and firmware. Be sure to check the manufacturer’s website regularly for any updates or patches for your device.
* **Check your internet provider’s or router manufacturer’s wireless security options.** Your internet service provider and router manufacturer may provide information or resources to assist in securing your wireless network. Check the customer support area of their websites for specific suggestions or instructions.
* **Connect using a Virtual Private Network (VPN).**Many companies and organizations have a VPN. VPNs allow employees to connect securely to their network when away from the office. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted. If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

And there other ways of prevent any sort of cyberattacks as well these are:

**1. Firewall**

[Firewalls](https://www.fortinet.com/resources/cyberglossary/firewall) filter the traffic on your network. They work to prevent and block unauthorized internet traffic and manage authorized access within your network.

**2. Network Segmentation**

[Network segmentation](https://www.fortinet.com/resources/cyberglossary/network-segmentation) divides a network into multiple sections, and each section then acts as their own individual networks. The administrator is able to control the access to each smaller network while improving performance, localizing issues, and boosting security.

**3. Access Control**

[Access control](https://www.fortinet.com/resources/cyberglossary/access-control) gives you the ability to grant or deny access to individual users based on their responsibilities within your network. This will define a person or group's access to a specific application and system on the network and prevent any unauthorized use.

**4. Remote Access VPN**

A remote access virtual private network (VPN) provides integrity and privacy of information by utilizing endpoint compliance scanning, [multi-factor authentication (MFA)](https://www.fortinet.com/resources/cyberglossary/multi-factor-authentication), and transmitted [data encryption](https://www.fortinet.com/resources/cyberglossary/encryption). The remote access VPN is typically provided for telecommuters, extranet consumers, or mobile users.

**5. Zero-Trust Network Access (ZTNA)**

The [Zero Trust Network](https://www.fortinet.com/solutions/enterprise-midsize-business/network-access) grants specific access to an individual user based on the exact role they play within the network. Each individual is only granted access to certain processes or applications they need to complete their job successfully.

**6. Email Security**

[Email security](https://www.fortinet.com/resources/cyberglossary/email-security) is set up to prevent users from unknowingly providing sensitive information or allowing access to the network via a malware-infected email. This security feature will warn or block emails containing potentially dangerous threats.

**7. Data Loss Prevention (DLP)**

[DLP](https://www.fortinet.com/resources/cyberglossary/dlp) is a network security technology that aids in preventing sensitive information from accidentally being leaked outside of the network by users. It works to prevent the misuse or compromise of data to protect the network from exposure to outside entities.

There are things that the company needed to put into and these included:

1. **Ensure endpoint security is enabled for all of your endpoints.** Every device attached to your network is a potential entry point for a hacker. Therefore, the first step in improving your business security is to make sure your endpoint security, whether on the device or part of a secure SD-WAN solution, is up-to-date and functioning optimally.
2. **Keep all software updated**. After ensuring your endpoints are protected, double-check that the software they run is the most recent version. This includes both the firmware that runs each endpoint and the apps they operate.
3. **Update your router’s name and password**. Don’t use your routers’ default network names and passwords. Using default authentication info is like rolling out a red carpet for hackers.
4. **Use a network firewall**. A firewall prevents multiple kinds of attacks, such as attempts at unauthorized network access, malware, and distributed denial-of-service (DDoS) assaults.
5. **Ensure you train all employees**. By arming your employees with the knowledge they need to recognize and prevent cyberattacks, you empower them as proactive auxiliary "members" of your security team.
6. **Get rid of software you don’t use**. Similar to endpoints, each piece of software, especially if it connects to the internet, gives a hacker an opportunity to penetrate your system. By discarding old or unused apps, you shrink your attack surface.
7. **Use frequent backups**. You should frequently back up and encrypt your data. In the event of a ransomware attack, theft, or loss due to a disaster, you can use the most recent backup to maintain business continuity.

**These are the procedures that the company can implemented into their network security system for a better and safer network**.