Remote working may have its benefits and convenience, but it also puts a company’s networks and data at risk due to unintentional careless behavior of employees. Data breaches, unattended computers, and unsecured Wi-Fi connections are only some of the potential concerns an organization may face due to remote working. Moreover, employees with little or no knowledge of keeping data secure can leave your company particularly vulnerable to cyber security challenges.

Let’s have a look at some major security challenges of working remotely that companies should know about. This is important so companies can incorporate secure remote working tips into their remote working policies and keep their corporate information secure.

1. **Phishing Emails**

Phishing emails are one of the most common causes of data breaches. Most of the malware is delivered through phishing email attacks. According to a [2021 survey on Phishing attacks](https://www.proofpoint.com/us/resources/threat-reports/state-of-phish) by Proofpoint Research, around 66% or surveyed organizations were victims of successful phishing attacks in 2020, with 30% of them experiencing malware infection.

It is not only remote employees that receive phishing emails. However, employees that work from office can be constantly reminded of identifying and handling phishing emails at workplace. Remote employees tend to forget basic security practices and often get tricked into handing over their login details or downloading malicious software that ultimately provides criminals the access to their systems.

Training remote employees to detect and avoid phishing email can significantly reduce data breach threats posed by the email. These regular reminders are very important for remote employees as they use their personal devices or software to access corporate networks.

1. **Unsecured Home Devices**

Remote employees usually use their personal devices while connecting to corporate networks. Most of them are not provided with corporate laptops and can lead to security problems. Organizations with good cybersecurity practices use Virtual Private Networks to provide more security with devices that access organizational network. However, employees usually do not use VPN to access internet at home or encrypt their smartphones while checking their work mails or conducting regular online [transactions](http://www.cardzgroup.com/PvcCard.html).

Moreover, personal laptops are generally not as secure as corporate systems. Hence, security features such as firewalls, encryption, email filtering may not be available on their personal systems with no oversight for corporate teams to find out what’s happening.

1. **Weak Passwords**

Even with firewalls, VPNs, trainings and remote work security policy, employees are the biggest risk to corporate networks. Particularly when it comes to passwords, humans are the weakest link. Employees often repeat their passwords or write them down in their smartphones to remember multiple passwords. Cybercriminals also know that employees who work from home are less careful when it comes to security practices.

Organizations that assign corporate systems to remote employees should add a login app or a lock screen that is triggered after a certain time of inactivity. This can make it harder for third parties and cyber criminals to access these computers. It is also advisable to use a password management solution that helps employees store passwords in a secure manner.

1. **Unencrypted File Sharing**

Organizations may have policies to encrypt data stored on their devices and networks, but many don’t take into consideration the encryption of data that is in transit between different systems. This includes email solutions and third-party cloud file-sharing. Everyday, employees share a lot of critical data, from product information to client data. Hence, these companies cannot afford to put this data at risk by using unencrypted file sharing services or solutions. If unencrypted, it can lead to information theft, ransomware and malware attacks, and reputational damage.

This may be easier to control in official premises. However, for remote employees, it gets hard for companies to ensure that that their information stays encrypted at all times. To ensure this, employees need to use file sharing services that have inbuilt security such as OneDrive, Dropbox, or WeTransfer. For email encryption, remote employees should use services such as ProtonMail to send and receive corporate emails via VPN.

1. **Open Home WiFi Networks**

This is of particular importance for organizations where employees are allowed to access a work network via their personal devices. When thinking of personal devices, we often forget about employee home WiFi networks. Just like any other hardware, it needs to be updated and password-protected. Routers that have not been updated can have security vulnerabilities which hackers can exploit. Moreover, remote employees should never connect to an open public WiFi while carrying out official activities.

To keep home WiFi networks protected, it is important to change default passwords and also keep changing them from time to time. It is also important to anonymize the Service Set Identifier (SSID) or WiFi network name and avoid using any information that can help hackers recognize your identity.

Also advise all remote employees to encrypt their WiFi devices with WPA or WPA2. Also ensure that all employees check their router settings regularly and run latest version of its firmware to address security vulnerabilities before they can become an issue.

**Wrapping it Up**

Remote working is not going anywhere anytime soon, and if proper measures are taken, it can be as secure as on-premise working where employees have up-to-date security procedures. Companies can identify and mitigate the security concerns of their remote employees to ensure that their information and systems remain protected. Moreover, it is important to keep the employees aware and educated about all these challenges and keep them equipped with the knowledge to overcome these threats by protecting their devices and home networks while they work remotely.