Best Security Practices for Remote Workforce

In today's highly competitive economy, organizations rely on remote workforce more than ever. From pandemic prevention to hyper urbanization relief, the news seems to be buzzing with the tones of remote work lately. Amid Covid-19 outbreak, most of the companies across the world are telling their employees to telecommute to contain the spread of the virus. Governments across the world are taking preventive measures, including closing schools and asking people to work from home. Thanks to the internet era in which we live in, today we enjoy the luxury of working from the comfort of our couch. In many cases, people already work from the comfort of their homes. However, this luxury of working from home has its own pitfalls and the biggest one being online security threats. Remote work poses serious security challenges for companies. Since remote workers are not physically present in the office, they often access company networks using wifi from popular locations such as coffee shops etc. which are prime spots for hackers to spy on internet traffic.

Security Concerns for Remote Workforce

Following are the online threats of which remote workers should be aware of:

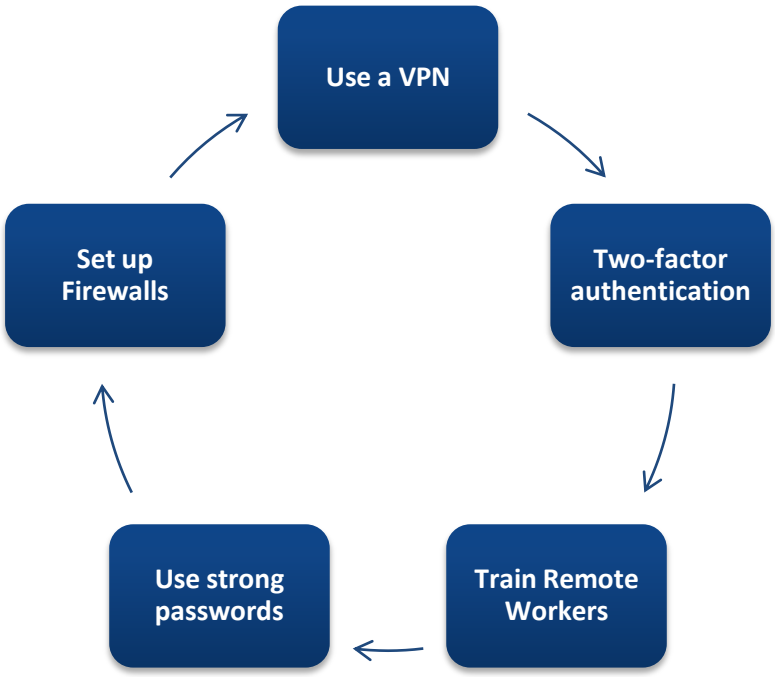
Public wifi Networks: While working remotely, workers might sometimes use unsecured public wifi networks which are prime spots for hackers to spy on internet traffic and collect confidential information. Public wifi is the worst security offender and one of the most popular cybersecurity attack vectors. Other challenges that public wifi poses include phishing attacks where targets are contacted by email, telephone by someone posing as a legitimate institution to lure individuals.

Use of Personal Devices and Networks: Remote workers often use their personal devices and networks for their work-related tasks. Generally, personal devices and networks lack tools built into business networks such as strong antivirus software, automatic online backup tools etc. This poses a serious threat of both personal and work-related information being leaked.

Spam and Phishing E-mails: Remote workers receive spam and phishing emails on a daily basis, which poses a serious threat to the security of the remote workforce. This becomes more important if your remote workforce includes the likes of customer service employees those who handle the information of your company as well as of your customers. Hackers can easily trick them with a spam email that looks like a standard customer inquiry.

Cyber security Practices for Remote Workforce

As technology has evolved over the past decade, we have observed a gradual shift from the traditional model of the nine-to-five office experience to companies having employees working remotely. Now, as working practices become more casual and collaborative, it becomes important for organizations to ensure the security of confidential information from online threats. Following are some of the ways of ensuring the security of the remote workforce:



Use a VPN: Companies can resort to remote-access VPN to establish secure connections between their networks and the devices used by remote employees. A VPN encrypts data in transfer, allowing personal and confidential data to tunnel from one device to the next, away from prying eyes. Moreover, VPNs offer companies an affordable way of securing data sent by offsite employees.

Better Remote Access Policies: Remote access control policy basically contains an overview of the company's network and outlines how the business would react when unacceptable or unauthorized use occurs. Unfortunately, many business owners tend to ignore the importance of having a good remote policy even though a compelling remote access policy can help companies mitigate many remote access dangers.

Set up Firewalls: A Firewall is a software or a hardware device which examines data from several networks and filters out malicious programs. Firewall guards the network against hackers and prohibits their actions at predefined boundary levels. The firewall ensures 24*7 protection of network from hackers. For Companies, it is a one-time investment and only needs timely updates to function properly.

Two-Factor Authentication: It is a two-step verification process where you have to provide your account details (username and password) followed by a randomly generated security code that's automatically sent to an email associated with your account. Basically, two-factor authentication reduces the threat of online identity theft and fraud by providing an extra layer of security to guard your account information and all communication processes.

Protect devices with Antivirus software: Generally, companies install powerful security solutions, prohibit employees from installing applications, and restrict online access from unauthorized devices and so on. However, it gets trickier for companies to provide the same level of security to its remote workforce, which puts companies' data at risk. To safeguard computers from malware, organizations should install good antivirus software. Norton, McAfee, Bitdefender are some of the best-known options.

Keep work data on work computers: Naturally, it is tempting for remote workers to use their personal computer if their work computer is in a different room or because of any other reason. Such unintentional mistakes pose a serious threat to you and your company. Therefore it is advised to keep work data on work computers and avoid using unsecured networks to access office information.

Use Strong Passwords: Strong passwords on any accounts with access to Remote Desktop should be considered an essentially required step before enabling Remote Desktop. Unfortunately, many people mostly use the same passwords across multiple accounts. Hackers take leaked usernames and passwords and attempt to log into other online accounts, a tactic called credential stuffing. Therefore, it is advised to use a unique password for every account comprising of a long string of upper and lower case letters, numbers and special characters.

Encrypt Sensitive Data on your device: Any remote communication with employees or customers should be encrypted at every possible point. What encryption does is that it puts all your data into unreadable code. Even if a hacker steals your data, he won't be able to use anything encrypted because he doesn't have the encryption key. Encrypted data can't be read, so it is advised to at least encrypt your business emails.

Training of Remote Workers: It's not enough to have the right policies and expect your employees to abide by them without educating and training them about policies. In order to ensure the security of data and employees of the company, a solid foundation needs to be laid. This foundation should include a remote working policy and good training to ensure that remote workers understand their responsibilities.

Avoid the use of unvetted USBs: USB devices should be treated as if they may contain malware. You should avoid plugging any USB device into a computer that is used to access work-related data.

Take Away

Over the years, the use of the internet has evolved vastly in almost all sectors. The growth and usage of the internet have brought in several benefits and has given rise to 'work from home' culture. Currently, as the whole world remains at a standstill because of coronavirus pandemic, the remote workforce trend shows no sign of slowing down. Remote workforce offers loads of benefits to organizations, but at the same time, there are challenges that come with organizing a remote workforce. Remote workers present a unique challenge for information security because remote work environments don't usually have the same protection measures as in the office. By following the tips mentioned above, workers and companies can prevent confidential data leakage.