# Cybersecurity Tips For A Remote Workforce

## Cybersecurity for a  Remote Workforce.

**Home and Public WIFI Networks:** These networks typically lack sophisticated cybersecurity protection and have multiple users who are not trained in or are monitored for basic cyber security behaviors. Lack of adequate cyber security coupled with user limitations exposes remote worker's devices to infiltration by spyware, ransomware, or a trojan virus which then attempts to propagate through any network the user connects to.

**Use of Personal Devices and Hot Spot Networks:** Accessing the company network through personal devices and hot spots is a major risk. These devices frequently lack security protection and work outside the anti virus protection and firewalls of a company network. Personal devices may be be shared with multiple potentially high risk users thus enabling an entry point for cyber criminals.

## Planning Remote Access Cybersecurity

The attached checklist will help identify cyber security gaps and how you can be better protected.

If you would like a customized review, please contact us for a free cybersecurity consultation.

Review our
**Remote Workforce**
**CYBERSECURITY CHECKLIST**

# Reducing Risk for The Remote Workforce

□ **Confirm antivirus and endpoint software solutions are up-to-date**

Are your anti-virus and end point solutions running the latest software versions? Have they been disabled anywhere in your network?

□ **Run vulnerability scans update/patch systems as needed**

Are you performing network security assessments routinely and what is your schedule? Weekly, monthly or quarterly? Are you scanning Internally and Externally? Are you really sure what is currently connected to your network?

□ **Are security alerts reviewed proactively 24/7**

Who is reviewing your network alarms? Is it the same team supporting the new challenge for remote IT connectivity? Are you throwing too much at them? Often the same team checking alerts is supporting the transition of the entire work force to remote working. Are you monitoring this team for Alert Fatigue? Who is doing that and how? Evidence confirms that Advanced Persistent Threats (APTs) sit in networks for months transmitting your critical data to cyber criminals before discovery. The Target data breach confirms how a threat can lie hidden in a protected network for months before discovery. Network security needs to be monitored and threats promptly responded to 24/7 - is that happening with your network? This is an area with zero tolerance for failure.

□ **Security Awareness Training including Phishing Simulation**

Are you providing employees with routine cyber security awareness training? If not, why not? Employees are the weakest link in your cyber defenses - are you protecting your network from employee lapses and failures? An ongoing internal security awareness program which includes phishing simulations is critical in reducing your company's risk vulnerability.

□ **Monitor Dark Web for stolen credentials**

Digital credentials, such as usernames and passwords, connect you and your employees to every aspect of your digital business applications. By using our Dark Web Monitoring tool, you will be alerted if your company's credentials or PII appear on the Dark Web. Credentials appearing on the Dark Web are an indicator your network is compromised.

□ **Ensure back ups are configured properly, segmented and actually working**

Are your backups properly configured and running? Backups can be tested via automation to ensure they are working. Best practice is to keep backups offsite and off the network. Segmentation of your network will also help prevent or slow down the spread of infection. Ensure your administrators use unique domain admin credentials for their server access and backups.

□ **Enable multi-factor authentication (MFA) where possible**

Enable MFA on all hardware, software and cloudware. MFA is an authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism. MFA is an additional layer of system security helping prevent cybercriminals gaining access to systems.

□ **Use encrypted communications**

For organizations which operate under regulatory oversight, encrypting sensitive data is critical. Provide encrypted systems and solutions since non compliance will potentially result in major fines.

□ **Enable Virtual Private Networks (VPNs) for remote workers**

Ensure remote workers connect to company's network resources via a Virtual Private Network (VPN) which encrypts all of your internet traffic. Ensure firewalls are up-to-date and use the most recent rulesets.

□ **Implement SIEM and ensure proper logging**

A Security Information and Event Management (SIEM) solution centralizes data by collecting logs and events generated by host systems, security devices and applications. Ensure all authentication related solutions are logging to your SIEM. Make sure to be able to record successful and failed login attempts along with remote access solutions.

## Closing Advice for Leadership

**Update Policies:** Review technology policies and procedures and ensure that employees understand workplace regulations for working remote. Remind staff to lock computers and do not share corporate machines with other members of the family.

**Maintain Communication:** Use tools that will maintain communication while not introducing new vulnerabilities. Employees will appreciate updates from leadership and avoid speculation.

**Create/Update Preparedness Plan:** Make preparations in case a cyber incident occurs so you can respond to and recover and access critical data. Ensure internal IT or outsourced Security Operations Center have incident escalation procedures. Identify who in the organization will send urgent information so users can identify legitimate information.

**Consult with Security Experts:** If preparing adequately for remote working cybersecurity challenges is beyond your resources, SECNAP has the capability to manage, detect and respond to threats on behalf of your organization. This checklist is a great start, but our SECNAP experts are available for consultations that can go over your team's readiness and security in depth.