**Cybersecurity Checklist for Remote Working**

If the Covid-19 pandemic has forced your organization to adopt remote working for employees, it is very likely that you were required to roll out new IT applications and services to maintain your employee efficiency, business continuity and production capacity. But as companies are implementing the new system to cater to the needs of remote workforces, this transformation may not have been very smooth for some of them due to limited technology capability. It is quite understandable that the speed with which the pandemic has spread, organizations understandably did not put cybersecurity in the forefront while implementing a remote workspace system.

While organizational IT infrastructures may be overloaded with increased demand, it has given cyber criminals an opportunity to exploit vulnerabilities in temporary and newly implemented IT systems. Now that the initial pandemic panic has considerably died down and people have started to adapt to remote working, it’s time for organizations to evaluate their changed IT infrastructure and its impact on security. The last thing you would want after being already financially strained during this time is to become a target of cybercriminals and face further reputational and financial constraints.

To ensure the robustness of your company’s security setup and protect your organization from cyber threats during this critical time, below is a security checklist of recommended considerations and steps to keep in mind while your employees work remotely.

|  |
| --- |
| **IT Infrastructure** |
| * Enable security protection on all endpoints |
| * Enforce software updates on remote employees |
| * Ensure secure remote access to IT assets with the capacity of being access by increased number of users |
| * Increase the time and capacity of IT helpdesk service to ensure that all employees get uninterrupted service and help while working remotely |
| * Ensure that helpdesk staff confirms identity before granting password resets or other unusual requests |
| * Provide software solution to employees for backing up their critical data |
| * If staff is using cloud storage service, ensure that they only use an approved service |
| **Governance and Risk** |
| * Update your policies and procedures for using devices at home and communicate accordingly to employees |
| * Remind the employees to ensure the confidentiality of their work and not to share their devices with others |
| * Ask all employees to regularly update their software programs and operating systems |
| * Communicate information security awareness messages regularly to employees to strengthen their security concepts |
| * Give reminders to staff to stay vigilant for phishing emails and all other attempts of stealing account details and report any malicious activity |
| **Password Management** |
| * Instruct the staff to never share their password via SMS or Emails |
| * Make two-factor authentication compulsory for all remote employees whenever they have to access any critical application or system |
| * Keep backup codes for times when two-factor authentication doesn’t work and ensure that backup codes can be restored safely |
| * To avoid scamming, communicate to all employees that you will not call them for resetting passwords |
| **Mobile Devices** |
| * Ensure hardware encryption for all mobile devices wherever possible, otherwise ensure software encryption |
| * Ensure full disk encryption in all mobile devices |
| * If an employee is using personal device, remind them to never download an untrusted application |
| * Communicate to all staff to update their device software and create backups |
| **Operations** |
| * Update firewall rules and VPN profiles to confirm that all employees have been assigned the right privileges according to their job roles |
| * Disable split tunneling for all VPN profiles so that remote staff is unable to have direct access to internet from their devices while they use VPN to access organization’s corporate information system |
| * Create a group where employees can share malicious activity with everyone, such as phishing emails |
| **Online Calls and Meetings** |
| * Teach your staff to not sit close to any smart devices such as Google Home or Alexa while discussing confidential information during calls |
| * All employees must mute their mics when they are not speaking |
| * Remind the employees to always keep their machines locked while they are taking a phone call, especially in a public place |
| * Communicate and remind employees to only use approved video and audio-conferencing apps that are password protected |
| * Cameras and mics should be switched off by default, and turned on when required |
| * A participant that is kicked out must not be able to join back in |
| * Before starting a conference, confirm and check the identity of all attendees |
| * Remind all employees to close the application after the conference call ends |
| **Employee Reminders** |
| Create security awareness training tailored to remote working situations which prompt and remind the employees to: |
| * Detect and avoid potential phishing threats, such as coronavirus scam emails |
| * Use secure WiFi in public and at homes |
| * Remind employees to never save their [credit card](http://www.cardzgroup.com/ContactLessSmartCard.html) details when making personal or official online transactions |
| * Not use official devices for personal emails, social media and file sharing apps without prior approval |
| * Save and secure all necessary printouts and discard unneeded documents by shredding |
| * Not copy any work-related files to their personal devices such as laptops or external hard disks |
| * Store all Personally Identifiable Information (PII) or Protected Health Information (PHI) of customers at data center storage or approved cloud storage service instead of storing them locally |
| * Avoid using removable storage such as flash drives |

The above checklist of security recommendations for a remote workforce can ensure that companies work securely and productively during this challenging time. Luckily, it’s not a very complicated process and with a little practice and vigilance, organizations can ensure that their employees maintain a good online hygiene to protect the privacy of their information assets while working remotely.