Employees Tips For Working From Home

A few important guidelines to implement in order to protect the security of your organization's data, while your employees are working remotely.

It is important if an employee is using their own device (laptop, PC, etc.) to connect to the company's network that certain protocols are followed to ensure the hardware and sofware is secure and safe. Unknowingly their personal hardware could contain a virus or malware, that could be spread to your company's network.

Additionally, it becomes more of a challenge to verify the legitimacy of emails, you may be unfamiliar with policies and procedures as they pertain to a work from home environment, and the list goes on.

Note, this list is intended for guidance and information purposes only. If you have any questions regarding these tips, please reach out to your IT provider for additional information.

Guidelines & Tips

- Secure workspace
    - Ensure you have the ability to lock your devices (laptop, PC, etc.) and any business relevant information when not in use.
    - Avoid using your personal devices for work-related business, unless your device is professionally monitored, secured and updated by a qualified IT support team.
    - Protect the data you are accessing by using a VPN to log into the company network. A general suggestion to ensure you are protecting data visible on your screen use a screen protector, which is especially critical for employees who are required to be HIPAA compliant, PCI compliant, etc.
    - Do not let family members, friends, or anyone but yourself use company-owned devices or personal devices used for business purposes
    - Use strong unique passwords on all your devices and accounts to prevent unauthorized access
- Wireless Security
    - Enable WPA-2 or higher encryption
    - Ensure your local router firmware is up to date
    - Limit the use of public Wi-Fi. Always use a VPN when connecting to public Wi-Fi. Never use public Wi-Fi to send sensitive information without a VPN
- Ensure all personal devices are secure with company-provided or personally owned antivirus and antimalware software company

AWARENESS

- Remote Work Employee Awareness
    - Be extremely cautious of email phishing scams
    - Limit social media use
        - Don't reveal business itineraries, corporate info, daily routines, etc.