CTSI
Serving Colorado's Counties

Technical Update

Volume 24 Number 46 September 8, 2020

Data Security for Telecommuters

The COVID-19 Pandemic forced many businesses and organizations to embrace telecommuting almost overnight. While telecommuting was a popular benefit with employees and employers alike before the pandemic, the rapid move to telework has led to some challenges. One of which is maintaining the security and integrity of company data and networks with so many workers logging in remotely.

Increased Risks

There are 3 ways telecommuting employees expose data and networks to risk.

1. Open Wi-Fi Networks – Employees who telecommute may think nothing of logging into an unsecured Wi-Fi network on their company-issued phone or laptop; however, hackers often target these networks with keylogging software and malware. Once compromised, the telecommuters' device can then infect your entire network.
2. Non-authorized users – Once a company device has left the office, the company has no control over who has access to it. Risks range from device theft to use by a family member who accidentally or unknowingly erases essential information.
3. Altering/Not Updating Security Settings – Security software (e.g., antivirus, antimalware) installed on company equipment needs to be up-to-date and frequently used to be effective. Remote devices may have outdated virus/malware definitions, or the user may have altered security settings to bypass company firewalls on restricted sites. Either of these things can create a hole in network security that can be easily exploited by hackers.

Protect Data

While telecommuting does pose security threats, there are steps you can take to mitigate them.

1. Acceptable use policies – Draft a policy that covers where company-issued equipment can be used and that restricts device access to only the employee. Make sure the terms of the policy are known and acknowledged before an employee begins telecommuting.
2. Encrypt data – Set up a virtual private network (VPN), which allows data and internet traffic to be encrypted. It also lets you limit which parts of the network remote employees can access. Also consider encrypting and routinely backing up all data on remote devices in case the device is lost or stolen. Commercial encryption software is available from numerous vendors.
3. Automate security – Whenever possible, make security automatic. For instance, set antivirus/antimalware software to update and scan automatically. Also, require all employees to have a strong alphanumeric password that expires at regular intervals. Limit the ability to change security and firewall settings on company-issued machines to administrative access only.

What this Means to Counties

As employees have exchanged the business office for the home office in record numbers this year, it is vital to beware of the security risks that come with telecommuting. Educating yourselves and your employees is the most important step in creating a secure network. For more information, please contact CTSI's at 303 861 0507. CTSI