How to Add Mobile Devices to Your Network Without Compromising Security

The future of business information technology is a mobile future. The rising popularity of laptops, smartphones, and tablets has created a new workforce that wants – and needs – to be able to take their data on the road. No longer content to be shackled to desktop computers, workers now need to flexibility and freedom to take their data and applications to where the customers are.

This can reap enormous benefits for your business. Unfortunately, it can also expose you to an entirely new range of threats, from data theft and security breaches to viruses and malware.

And this problem is only made worse if you allow employees to connect their own devices to your network. While employees love the freedom BYOD (bring your own device), this also means that you are giving access to your network, and potentially to every device, to any number of unknown, third-party devices that are out of your control.

Fortunately, there are a few common-sense practices you can put into place to minimize potential problems caused by mobile devices.

A comprehensive firewall and virtual private networking (VPN) solution: Allow access to your network, data, and servers from outside of your network requires a strong, manageable firewall solution to keep unauthorized users from accessing your network. A firewall acts as an impenetrable barrier that allows only the data traffic you authorize from entering or leaving your network from the outside. A VPN is a secure conduit or tunnel that allows authorized client devices to connect through the firewall into your network. This is a critical must-have if you plan on allowing outside access to your network.

Strong antivirus software: Antivirus software is your first line of defense against computer viruses and malware that can compromise your network and steal or destroy your valuable data. Although traditionally a problem for computer users, viruses can now strike a number of mobile devices and use these devices to spread on your network. To be effective, antivirus software must be installed on every device that touches your network and must be frequently updated. Most will automatically update, but need occasional monitoring to make sure they are performing as expected. Also, many business antivirus packages also offer the option of allowing you to distribute your antivirus solution to personal devices owned by your employees, which would give you considerable piece of mind for BYOD as well as a nice benefit for your workers.

Continued on Page 2

CST
Combined Systems Technology
800-944-2966 515-270-5300
www.cstoncall.com info@cstoncall.com

How to Add Mobile Devices to Your Network Without Compromising Security [Continued]

Encryption: What would happen if a laptop or mobile device owned by your company was to fall into the wrong hands? Could you withstand the loss of proprietary client data, or data such as social security numbers or medical information, both of which carry regulatory fines if handled carelessly? Data encryption can prevent this from happening, and should be a requirement for any portable devices your company owns or any BYOD device that contains company data. Many new laptops and USB memory devices have easy-to-use encryption built-in, or it can be easily added with any number of software packages ranging from free, such as Truecrypt to robust commercial packages such as Safeguard.

Wi-Fi security: Open, unsecured Wi-Fi is an invitation for unauthorized access, use, and potential abuse of your network. If you have wireless networking in your facility, and devices that need to connect wirelessly, make sure you use password-protected, encrypted connections. This means no one can connect to your wireless without the correct password, which should keep unauthorized access at bay. For greater security, you may want to set up a secondary or 'guest' Wi-Fi for employees, clients, or visitors to use that access just the internet, and not your internal network. This network should be set up in a separate IP address range or subnet outside of your dedicated work network. After all, if all they really want is internet access, why give them access to your network?

Network security is serious business.

At Combined Systems Technology, we speak the language of business.

Contact us for more information on how you can accommodate the future of business without compromising your security.

CST
Combined Systems Technology
800-944-2966 515-270-5300
www.cstoncall.com info@cstoncall.com