5 ACTION ITEMS TO IMPROVE YOUR NETWORK SECURITY

Here are 5 easy things you can do today to better protect your network.

BACK UP YOUR FILES REGULARLY

Work files should be backed up to the cloud and a physical hard drive. In the event of hardware failure or human error, you can quickly access those files in an emergency. Proper backup procedures can stop ransomware in its tracks. With on-site, up-to-date backups, you can reinstall those files from your backup drive. Backup and Disaster Recovery services can be outsourced to a vendor with the IT resources to quickly recover and restore lost files and data. BDR solutions can even protect against cyber threats including ransomware.

RESTRICT USER RIGHTS ON OFFICE DEVICES

If a user doesn't need administrator privileges or access to enterprise-level administration, create a regular user account instead of an administrator account. Ask your IT team to handle non-admin work from a regular user account and only log into an admin account when necessary. Switching users takes seconds, but can save hours of heartache from an unintentional mishap.

USE VLANS TO SEPARATE TRAFFIC ON YOUR NETWORK

A VLAN, or Virtual Local Area Network, is a networking technology that groups together devices on separate local area networks. VLANs can improve office security because they offer greater control over which devices have access to each other. Users should be on one VLAN; servers should be on a separate one. Your public-facing servers can be accessed by people from outside your network. You want to keep your private, trusted, internal network completely separate from any potential outside attack.

ENABLE WPA2 FOR YOUR WIRELESS NETWORK

You should be using WPA2-AES (Advanced Encryption Standard), as well as enabling separate SSIDs for company employees and guests who might visit your offices. WPA2 protects both your company devices and your corporate WiFi network by encrypting the data.

WHEN YOUR WORK IS DONE, LOG OUT

Make it an office policy to have employees log out of their computers when not in use. Set up a screensaver that is password-protected. Use a strong password that no one can guess for your account login. This is a simple step, but it can prevent unwanted access to the network and user devices.

Some of the most effective measures to secure your business IT network and devices are free or low-cost. Businesses can't afford to take chances at a time when cyber attacks happen daily around the world. Hardware and software is expensive, your time is valuable and your sensitive corporate data is always a target. **WHY RISK IT?**

Arvig® can help your business implement a comprehensive IT management strategy to protect your network against hardware failure, natural disasters and cyber threats.

Find information and resources at arvigbusiness.com.

888.992.7844 | **arvigbusiness.com**

arvig®
Do Business