arcserve®

Ransomware Prevention Checklist

Immediate Steps to Take After a Ransomware Attack

- ☑ **Disconnect infected machine from the network & Internet** so ransomware doesn't spread to other machines
- ☑ **Run a virus scanner from a bootable disc or USB drive** (aka an offline virus scan) to try to remove the virus from the machine
- ☑ **Do a System Restore** to take your machine back to a previous state (this option is in earlier versions of Windows (pre Win 8))
- ☑ **Reformat the hard drive and reinstall your last backup**

How to Prevent Future Ransomware Attacks

Review and Update Network Security

- ☑ **Have Windows Firewall on at all times if you run Windows**
- ☑ **Install an anti-virus program that has a real-time virus scanner and automatically updates**
- ☑ **Keep your browser and plug-ins up-to-date, including Adobe Flash Player, Java, etc.**
- ☑ **Maintain up-to-date inventory of all of your digital assets, so hackers don't attack systems you've forgotten or don't closely monitor**
- ☑ **Segment your file access so only authorized users have permission to make changes**
- ☑ **Install pop-up blockers, as pop ups are another way for ransomware viruses to enter your system**

Ensure Data and Hardware are Adequately Protected

- ☑ **Keep your OS and applications up-to-date**
- ☑ **Back up critical data on a regular basis so if you're a victim of ransomware, you can recover important data without being forced to pay up**
- ☑ **Always have a copy of your data offsite whether on an external hard drive, secure cloud, or best case scenario: both**

Change Online Behaviors and Practices

- ☑ **Never download attachments from unknown senders or sources you don't know**
- ☑ **Don't download and execute unauthorized applications from the Internet unless they are from a trusted source and have been scanned for malware**

For more information, please visit **arcserve.com**