

ONLY **YOU** CAN PREVENT RANSOMWARE!



# CHECKLIST FOR PREVENTING RANSOMWARE



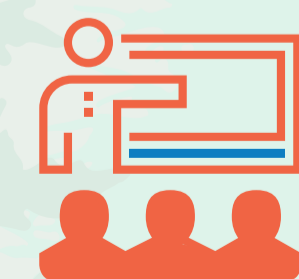
## STAY UPDATED

*This seems pretty simple, but ensuring internet browsers, computer operating systems and applications are on their most current release, and all security patches have been applied takes a lot of work. The time and effort are worth it if you can prevent ransomware attacks!*



## STRONG PASSWORD POLICY

*Set standards for passwords that are complex. This should include length requirements, special characters, capital and lowercase letters, and numbers. Encourage your employees to use strong, hard-to-guess combinations. Do not allow them to use any personal information.*



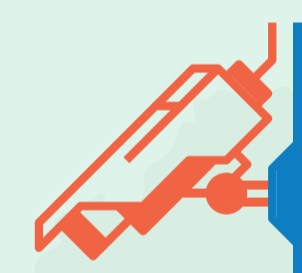
## TRAINING

*You need to thoroughly train your employees not open links or attachments that seem suspicious or come from unfamiliar or unexpected sources. This is the most common way that a hacker places ransomware in your network.*



## BACKUP

*It is extremely important to fully back up critical and important data on a set and routine basis. This would allow you to recover from an attack as quickly as possible or not be held hostage to the ransomware at all.*



## STAY VIGILANT

*Educate yourself and your workforce on what the current trends are in cyber-attacks, what to look for and recognize them, and report any suspicious activity to your designated Security Official.*



Better Solutions. Better Patient Care.