Best Practices for Ransomware Protection

FOR YOUR EMPLOYEES

To keep your employees safe, they should personally do the following 6 things.

- Use a Password Management System
- Ensure Multi-factor authentication (MFA) is enabled
- Change All The Passwords
- Keep The Software Up-to-date
- Use Multiple Email Addresses
- Protect Files with a Cloud Storage System

Password Management System

- Each Computer System, Each App, and Each Website should have its own password, however remembering many different passwords is difficult.
- Password Management Systems like KeePass, and LastPass are Free and are very secure. They use a Master password that you can easily remember. When using the mobile app they use technology like Facial Recognition or Biometrics to keep it safe.
- Don't store passwords in a document on a phone or a basic document on the computer. Using the save password feature in web browsers is not recommended.

Multi-factor authentication (MFA)

- MFA makes sure that only YOU are logging into an account. Even if your password is compromised a Hacker still needs an additional type of authentication.
- Authentication is broken down into 3 categories. Something You Know, (your password) Something You Have, (text message or App with a number to enter on the website) and Something You Are (fingerprint, facial recognition).
- Most applications offer free MFA solutions. They might use one of the following: Authenticator App, Text Message, Biometrics, Passcode, or Face ID.

Cloud Storage

- Cloud storage systems are a great place to store your important files, photos, and videos.
- Many companies offer Free storage. If you pay a small monthly fee you can have file level history. If the file gets deleted or encrypted by ransomware you can easily restore from the online backup.
- Cloud Storage Systems like, Dropbox, OneDrive, Google Drive, Box, iCloud, have mobile apps so you can have your data everywhere. They also use MFA to keep data safe!

Change Passwords

- Personal passwords may have been stored on the computer. Change ALL your passwords.
- Use passwords that are phrases. For example, the password SunnyDaysInMayAreTheBest! will take 4 Octillion years to crack.
- Record the new password in your Password Management System.

Multiple Email Addresses

- Ransomware attacks generally start with an email that has malware in it. Identifying a safe incoming email is not easy to do.
- Consider having multiple email addresses for separate uses. Category examples could be: Confidential, Social Networks, and Advertising.
- Always use secure passwords and MFA when setting up new email accounts.

Keep Software Up-To-Date

- Keeping Software up-to-date, helps keep the hackers out.
- All apps should be updated as well as Computer Operating System and Phone Operating Systems. When updates are available, you should install as soon as possible.
- Doing updates lowers your risk to have vulnerabilities on devices.

Need Help with these 6 Steps? Text: 630-940-6883 or Email: Judah@hawkeyet.com