mbc
MANAGED IT SERVICES

RANSOMWARE

WHAT IS IT?

Ransomware is malware that gets installed on a PC user's workstation using social engineering attacks where the user gets tricked into clicking on a link or opening an attachment. Once the malware in on the machine, it starts to encrypt all data files it can find on the PC itself and on any network shares the PC has access to.

HOW CAN IT AFFECT YOUR BUSINESS?

When a user wants to access one of these files they are blocked and unable to use the file - this can be a severe problem for business' critical data. The system admin who investigates this problem typically finds two files in the directory that indicate the files are taken ransom, and how to pay the ransom to decrypt the files.

Once encrypted the only way to way to get them back is to restore a recent backup or pay the ransom. These ransoms are about $500 within the first deadline and can double if the deadline expires.

WHAT DO YOU NEED TO LOOK FOR?

Ransomware uses social engineering techniques to trick the user into running it. Commonly, the victim receives an email with a password-protected ZIP file purported to be from a company.

The Ransomware gets run when the user opens the attached files, which are often ZIP files, DOC or PDFs. So when in doubt, delete the email and the attachment.

WORK SAFE:

1. **BE CAUTIUS** of emails from senders you don't know, especially those with attached files or with passwords
2. **EVEN IF YOU KNOW THE SENDER,** Its best to confirm verbally
3. **WHEN DOUBT,** delete the email
4. **NEVER** open odd attachments
5. **AVOIND** storing your files on your local PC
6. **ENSURE** you have reliable data backups