Cyber Security Awareness Foundation

RANSOMWARE ADVICE

RANSOMWARE IS A CYBER-EXTORTION TACTIC THAT USES MALICIOUS SOFTWARE TO HOLD A USER'S COMPUTER SYSTEM HOSTAGE UNTIL A RANSOM IS PAID.

BACK UP YOUR FILES REGULARLY AND KEEP A RECENT BACKUP OFF-SITE: The only backup you'll ever regret is one you left for "another day." Backups can protect your data against more than just ransomware: theft, fire, flood or accidental deletion all have the same effect.

DON'T ENABLE MACROS: A lot of ransomware is distributed in Office documents that trick users into enabling macros. Microsoft has just released a new tool in Office 2016 that can limit the functionality of macros by preventing you from enabling them on documents downloaded from the internet.

CONSIDER INSTALLING MICROSOFT OFFICE VIEWERS: They allow you to see what a Word or Excel document looks like without macros. The viewers don't support macros so you can't enable them by mistake, either.

BE VERY CAREFUL ABOUT OPENING UNSOLICITED ATTACHMENT: Most Windows ransomware in recent months has been embedded in documents distributed as email attachments.

DON'T GIVE YOURSELF MORE LOGIN POWER THAN NECESSARY: Don't stay logged in as an administrator any longer than necessary. Avoid browsing, opening documents or other regular work activities while logged in as administrator.

PATCH, PATCH, PATCH: Malware that doesn't come in via document macros often relies on bugs in software and applications. When you apply security patches, you give the cybercriminals fewer options for infecting you with ransomware.