Ransomware

Ransomware — the malware that encrypts all your data and makes you pay a ransom in order to (hopefully) get it back — is the big new threat. So you need to know everything you can about it.

Here are five things to start with:

1. Ransomware is getting big. Attacks were up 600% in 2016 and cost more than $1 billion. So this is not a small threat.

2. You need to keep your software up to date. Ransomware often takes advantage of older vulnerabilities that have been fixed in newer software. As in defending against all attacks, keep that software updated: all of it.

3. Watch out for the precursor. Other types of malware often get into a system to collect information. It's often used to assess how much ransom an organization can afford. If you stop this quiet malware, you may take yourself off the target list.

4. You're the vector. Granted, the malware itself does the encrypting, but phishing attacks that convince employees to download the malware in the first place are the most common attacks. Train your staff on how to avoid phishing scams.

5. Back up your data. If you have a good recent backup, you can skip right past the demands for ransom and get on with your day. Segmenting your network can also mitigate the damage Ransomware wreaks.

Those are just a few things to keep in mind when setting up your defences.

Source – Angie Pearson Crime Prevention Tactical Advisor for Colchester and Tendring Police Districts