Topic:

How to Deal with Ransomware (Part 2 of 2)

Definitions:

Ransomware – A type of malicious software that infiltrates and blocks access to a computer system until a sum of money is paid.

How to Protect Against Ransomware Attacks

1. **Perform regular backups** – Your business data should be backed up or archived at least once a day and more often if necessary. Backing up data can be as simple as copying your data files to an external hard drive that can be purchased at Best Buy, Office Depot or any major electronics retailer. Setting up and using an external drive is generally simple. Another option is to set your system to back up to an encrypted cloud-based service. An added benefit of using a cloud-based service is that you can access and retrieve that data from just about any connected device. If you use your phone to store your photos and contact information, use the phone's backup feature to store your data. If necessary, you can connect your phone to your computer and transfer photos and contact information to it.

2. **Update your device's operating system as recommended** – Keeping the operating system current on your device reduces the chance of virus attacks. System developers monitor the integrity of their operating systems against virus attacks and develop patches and updates that "plug the gap" in the software when viruses succeed in penetrating the software.

3. **Install anti-virus and anti-malware software** – Think of these programs as soldiers standing guard over your data 24/7, 365. These programs filter all data coming and going from your device and block out any harmful data. These programs must be updated continuously to guard against new and different strains of old viruses as they occur.

4. **Be cautious with your email** – Email providers such as Google and Microsoft filter your emails to block obvious junk email. You should be cautious when you see an email from someone you don't know. And, you should be careful when receiving an email from a business you have dealt with in the past, particularly if an email sender is asking for information they should already have. The best bet is to delete the email if you do not know the sender or if the request is suspicious.

5. **Don't open attachments or files unless you know the sender** – When you receive an email with a file attached, or has a link for you to click, think before you open the file or click the link. In most cases you should be expecting that email or file. If you do not know the sender, don't open the attachment or click the link. Delete the email.

For more information, contact: technology@allianceswla.org.