Topic:

How to Deal with Ransomware (Part 1 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.

What to Know about Ransomware:

Ransomware attacks have grown exponentially across the globe. Ransomware typically encrypts a victim's computer network or files, making it inaccessible. When this happens, the hacker demands a payment to decrypt the data – effectively holding a business hostage until money is paid. Efforts to trace the hacker are usually difficult and unsuccessful. While a tech-savvy person can sometimes reverse ransomware, it is almost impossible to recover encrypted files without the decryption key.

Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. In a rare instance, the "WannaCry worm" virus traveled automatically between computers without user interaction.

Everyone using a computing device (computer, smart phone, tablet, or any device connected to the Internet) is at risk to ransomware. Whatever kind of business you own, whether it's a hair salon, plumbing business, or medical office, the information on your devices is of interest to a hacker. Think about losing access to all the information, such as emails, phone numbers, schedules, or photos, that your business uses daily to operate. A hacker is trying to figure out, "How much can I get for that data?"

What to Do If You Get Hit by Ransomware

If you got the dreaded message on your screen that says you must pay X amount of dollars to access your data, what should you do? **Do not pay the ransom** – it is not worth it. If you pay the ransom, there is no guarantee you will be given access to your data. The hacker may just ask for more money. It's best to recover your data from backups and start from there.

However, you still must get past the screen on your computer/device to use it – so how do you do that? If possible, disconnect your device from the Internet. This could be unplugging the network cable or going to your device settings and turning off the Wi-Fi setting. If you are able to do this, then power the device off. Otherwise, do not turn the device off.

If your device is part of a business network, get in touch with your company's Information Technology (IT) department to inform them of what happened. They will work with you to get your computer up and running. Co-workers should be notified of the attack and what steps to take to prevent their computer/device from being hacked. If your device is for personal use, you should contact a local IT support company who will work with you to get your device working again or to advise what step to take next.

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