Ransomware –

How to avoid and what to do if you download it

What is ransomware?
A computer malware that encrypts your files so you cannot access them until you pay a specific amount of money (using bitcoins, money-grams or western union: all untraceable to the bad guy's account). Once the malware gets on your computer, it looks for any shared resources (think, network drives or connected usb backup drives). It then encrypts all files on the shared/attached drive as well as your computer. Finally, a screen is displayed declaring your files have been encrypted and you are required to pay to regain access.

How do I get ransomware?

1. The most common delivery of the payload is via an **email attachment**.

   Beware of certain attachment extensions and subjects.

2. Ransomware may be hiding on a **bad or fake website**. A search may land you on a site that performs a "driveby" download, infecting your computer.
3. Even trusted **websites that sell Ads** may be harboring ransomware. The bad guys will actually purchase a legit ad to get you to click on an offer, releasing the malware.

What can I do to protect my system?

1. Make sure your email is filtered. If you do not recognize the sender, delete the email. Block common malware attachments (see below).

2. Be mindful of any email attachments you open. If you do not recognize the sender, do not open the attachment. Common tricks used to unleash the malware:

   Hiding Malware in Files with Common attachments extensions:
   Attachments which should be scrutinized include: .js, .vbs, .docm, .hta, .exe, .cmd, .scr, .bat. and .zip.

   Use of double extensions. That means the attachment name may say something like "document.pdf.exe", "filename.jpg.scr" or "yourfile.docx.pif"

Ransomware –

How to avoid and what to do if you download it

Sample subject lines may be similar to one of these:

USPS – Missed package deliver
FW: Invoice<random numbers>
ADP Reference #<random numbers>
Important – attached form
FW: Last Month Remit
Scanned Image from a Xerox WorkCentre
Fwd: IMG01041_6706015_m.zip
My resume
Voice Message from Unknown Caller <phone number>
New contract agreement
Important Notice – Incoming Money Transfer
Payment Overdue – Please respond

This is certainly NOT a complete list, but is meant to provide some key elements of an infected attachment.

3. Be Alert about Links that are presented in your email or you are directed to via a website link (ads, etc.)

   If you are directed to an IP address (http://96.105.1.32) instead of a domain name (www.example.com) you may be redirecting to a bad site.

   Do NOT connect to Links contained in an email from a sender you do not know.

4. Backup Often & Offsite; Do NOT keep local drives attached to your computer.

   Implement and test an multi-tier backup routine for Servers as well as local drives which may contain important documents/data. Backup often; use offsite backup to another location or, at least, rotate backup devices and take them offsite.

   No NOT keep your backup drive(s) connected to your computer system. These files may also be seized/infected/encrypted.

5. Other Items:
   - ✓ On Network, do not map drives using letters; use UNC
   - ✓ Use Strong, Complex Passwords
   - ✓ Limit permissions (do not provide Administrator rights to users)
   - ✓ Keep Windows, Virus Protection and Firewalls updated
   - ✓ Keep Java, Flash, Adobe and Silverlight updated; Remove if you do not need.

Ransomware –

How to avoid and what to do if you download it

What do I do if I think I have been infected?

If you think you have opened a questionable file or visited a questionable site, IMMEDIATELY power off your computer and disconnect from network/external drives; contact AlphaLink (740.788.9000) for assistance.

If you have been infected with Ransomware, your computer will display a screen similar to the following:

Other virus symptoms:

- Slow Performance
- Pop Ups

Last words:

Ransomware types/variants continue to change and it is impossible to stop the infection without cautious end-users. Be constantly alert. Immediately power off your computer and disconnect from network/external drives if you have ANY suspicion you may have opened a bad attachment or visited a bad site. Invest in a good firewall, email filtering and a malware removal tool; And, most important, implement a multi-level backup plan.