ALERT : WannaCry Ransomware

As many of you are aware, a new ransomware attack was discovered on May 12, 2017, that has impacted over 10,000 organizations in over 150 countries. This new variant of ransomware has a much more destructive characteristic due to its ability to spread across networks by exploiting a critical vulnerability in Windows computers.

The primary method of ransomware infection is through the use of deceptive emails or malicious websites that imitate legitimate organizations or communications. Ransomware typically encrypts the data on the target machine, making data inaccessible. The victim is then prompted to make a payment in order to release or unlock the files. In some cases where a payment has been made, there have been reports the files have not been decrypted after payment, or their computer has been infected with the ransomware again shortly after being decrypted.

What can I do to mitigate my risk?

At minimum ensure you have a 3-pronged defense for your systems:

- Anti-virus software – active and up to date.
- Patching – ensure that your Windows systems have all the latest critical patches installed
- Backups – Ensure you have a backup solution in place and more importantly perform regular test restores of data.

Continued Vigilance

The single most effective tool today is constant vigilance.

- PHISHING EMAILS: MOST infections come from users clicking on links in emails. Attackers are very sophisticated and know how to bypass standard SPAM filters. Here is how to identify a phishing email:
    - RECIPIENT ADDRESS: The recipient shows a reputable name like a banking institution or another corporate employee. If you hover over the

recipients email address with your cursor you can verify if it is coming from their valid address.

- GRAMMATICAL ERRORS OR TONE: Is the tone of the content unprofessional or unusual? Are there odd grammatical mistakes?

- LINKS: BE VERY WARY OF ANY LINK IN AN EMAIL. If you think the email is from a reputable source, first hover over the link with your cursor and verify that the full address is from a recognizable domain. Oftentimes these addresses are spoofed and either the domain name (typically the company name) or top level domain (.com, .org) is from a foreign country.

- WEB SITES: Many websites are now being corrupted through content on web pages or through banner ads. Do not click on pop-ups or suggested links in news articles or familiar sites that is not directly related to the reason you have visited the site.