Monthly Cybersecurity Message from Scott Goodhart

Can you imagine turning on your computer only to find that you are unable to access your computer and any of your important files? Ransomware is an increasingly popular type of malware that infects your computer and holds files ransom by encrypting them. Hackers will only decrypt the files and allow you to regain access once you have paid a ransom. Similar to most malware, ransomware is often delivered via links and attachments contained in phishing emails. When reading email, consider the following pieces of guidance to help protect yourself and AES from falling victim to a sophisticated ransomware attack:

- If you receive an email that uses threatening language that urges you to take immediate action, be wary and do not click on links or open attachments enclosed in the message.
- Hover over links contained in messages and make sure they direct you to the correct website.
- Pay attention to the email address of a sender to ensure it is legitimate.

If you have any questions about ransomware or if you believe you've experienced a ransomware attack, please contact your local cybersecurity team.

Regards,

Scott Goodhart