Quarterly Security Awareness Newsletter

Ransomware Awareness

Imagine for a moment that you receive an email from a shipping provider. The message states that they cannot deliver your package, but attached is a document you can print and take with you to a delivery substation to collect your package. Your curiosity is getting the better of you, and the attachment is opened, only to discover that nothing seemed to happen. Then your laptop begins behaving strangely with files not loading correctly. The laptop restarts and eventually displays the following image:

This unfortunate scenario is an all too real situation happening at colleges and universities today. **How could this have been prevented?**

Prevention Method #1 (Identifying and Reporting Malicious Emails) - It is impossible to predict what the attackers might say, or attach to an email. In any event, email remains the number 1 attack vehicle. Identifying and reporting malicious emails not only protects you and your machine but those individuals that have not viewed or received their message yet. Also, we have recently added the **External Email** notification to emails originating from outside the environment (to give you advance 'warning' on e-mails with a higher threat level).

Prevention Method #2 (Next Generation Technology Tools) – We have adopted Sophos Intercept X to protect individual devices. It is using anti-exploit technology which stops the delivery of ransomware. Also, it stops ransomware before it can run. When or if Ransomware makes its way onto your laptop, there are still defenses to stop it.

> Even with the newest technology available, this does not prevent the risk of ransomware. New infiltration methods and strategies are developed daily, along with new software tools specifically designed to bypass existing prevention.

This can start or end with you!

We have all heard the saying "the best defense is a good offense," this could not be truer in the efforts to protect yourself and the organization from a ransomware outbreak.

1. **Being wary of email messages**.

    - Any messages that require immediate action, or cause you to wonder why your receiving this, should automatically trigger suspicion.

    - Think before you click – One of the best defenses to malicious links is thwarted by simply hovering your mouse over the link for 5 seconds. This will display a quick-tip showing the full address of the destination. When this does not match the information or business within the email, you can bet this link is not real.

    - Report malicious messages – Reporting may take a moment longer than simply deleting the message, but this moment can save a coworker from being annoyed by yet another spam email, or inadvertently taking action to their message, infecting their machine or others.

2. **Assisting in software patching**

    - Software patches are being regularly rolled out to your device. These patches do require a restart to take effect. When prompted to restart your device, please make every effort to comply with this request as soon as possible.

    - Remote users on VPN connections - Your involvement is even more necessary as you may need to connect your device to the VPN a least once per week for a minimum of 2-hours each session. This allows the device to receive any software updates, and fully synchronize with the internal network.
