April 24, 2019

Email Malware

We received reports this week from many staff members stating that they are receiving emails which appear to have familiar content or names but upon closer inspection, realize that the sender is not anyone we know or are affiliated with.

This concern has been reported to our IT tech support, Maxis360. They advised that we should not click on any links or respond to these emails under no circumstances. Also, they are blocking the reported senders from our email servers.

Additionally, there is a text message circulating around which was also reported to us by staff. Please do not respond to text messages you do not recognize the origin or sender and do not open any links. You may need to contact your cell phone carrier for assistance with such text messages

Tips for Recognizing a Malware Email

1. **Sender's email address**. If the sender's address is unfamiliar or doesn't match an expected address for a company, then it is probably a malware email. Most malware emails appear to be package delivery notices, invoices, fax/scans, or court notices. These emails rarely appear to come from an appropriate address, for example emails claiming to be from Fedex or UPS are likely to be malware if their From address does not match fedex.com or ups.com.
2. **Email subject or attachment contains username.** A malware email may contain your username in the subject or the attachment filename, or the Subject field may be blank. Contrast this to normal emails which almost always have a Subject and rarely mention your email username.
3. **Enticement to open an attachment.** Many emails containing malware will encourage you to open an attachment. Many attachments can still be harmful even if you are running antivirus. Emails about package delivery problems have no good reason to require you to open an attachment; if they were emailing you about a legitimate delivery problem, they could just inform you in the body of the email.
4. **Enticement to follow a link.** Some malware emails are like phishing emails where they encourage you to follow a web link. This web link could lead to malware, so please consider all the tips first.
5. **Information verification.** If an email is asking for you to confirm, check, review or provide information using an attachment, it may be a malware attachment. Reconsider if this seems safe and contact support if in doubt. It may not be safe to open the attachment.
6. **Problem warning, threat, or urgency**. Malware emails often attempt to incite your fear, worry, or a sense of urgency. If an email encourages you to solve a problem by opening an attachment, then you should be very wary. Some emails appear to be a second response asking you for a follow-up. Examples include dealing with package delivery problems, information about fake court appearances, or fake invoices from entities you may not be doing business with.
7. **Undisclosed-recipients/unlisted-recipients.** If the email recipient list shows undisclosed-recipients/unlisted-recipients or an email address other than yours, then it may be malware.
8. **Suspicious attachment.** If the email has an unexpected attachment such as a file with the extensions .doc, .zip, .xls, .js, .pdf, .ace, .arj, .wsh, .scr, .exe, .com, .bat, or other Microsoft Office file types then it may be malware. Consider that sometimes the file extension is hidden, or the contents are different than indicated.
9. **Plain text/absence of logos.** Most legitimate email messages tend to be written with HTML and they may have a mix of text and images. Malware emails rarely have images and tend to have plain formatting.
10. **Generic greeting**. If the email is addressed with a generic phrase like "*Dear Customer*" then it may be malware or a phishing attempt.
11. **Unexpected attachment contents.** If you do ultimately open an attachment and the contents are empty or are very different from what you expected, it may be malware. Please contact support for help immediately! Support may be able to limit damage or help you recover.

Below are a couple of additional links for additional review about viruses and various spam and malware.

https://www.us-cert.gov/publications/virus-basics

https://www.malwarebytes.com/spam/#recent-news-on-spam