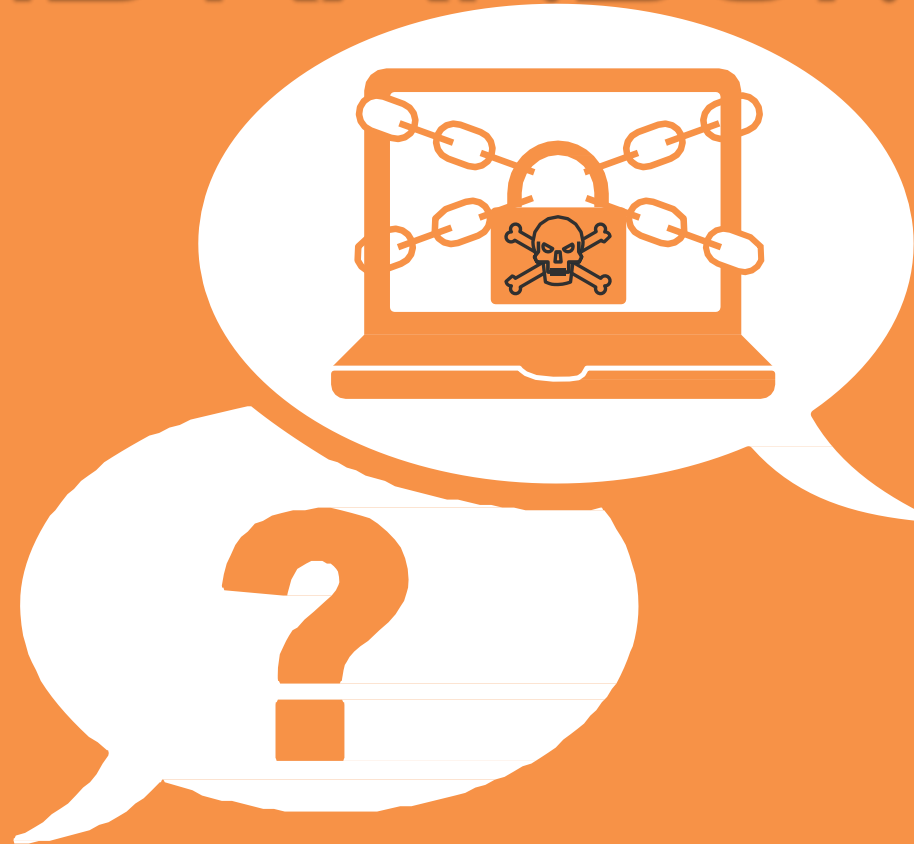


WHAT IS RANSOMWARE?



A quick guide to help you understand Ransomware
and its dangers

RANSOMWARE IS:

A type of malicious software that blocks access to data or threatens to publish it until a ransom is paid. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse.



RANSOMWARE IS NOT LOSING ANY MOMENTUM

Attacks on various industries are becoming daily occurrences. There are companies paying huge sums to retrieve their data from the malicious software. Often, the companies affected aren't familiar with ransomware until it's too late. So, allow us to introduce you to the infamous ransomware.



While ransomware is a form of malware, it's definitely unique in what it does.

Sprinkle in some 'ransom' and you've got a malicious virus that keeps your data encrypted until ransom is paid.

SO WHY SHOULD YOU CARE? THE NUMBERS TELL A DARK TALE!



INBOX SCAMS

This image is a prime example of a phishing email used to spread “Locky,” a common strain of ransomware. To the recipient, the email appears to come from a business partner asking the reader to “see the attached invoice” by clicking on the attached Word doc. Note how harmless this email appears and how easy it would be for a user to absentmindedly open and click, an action that would result in an instant ransomware infection. It happens every single day.

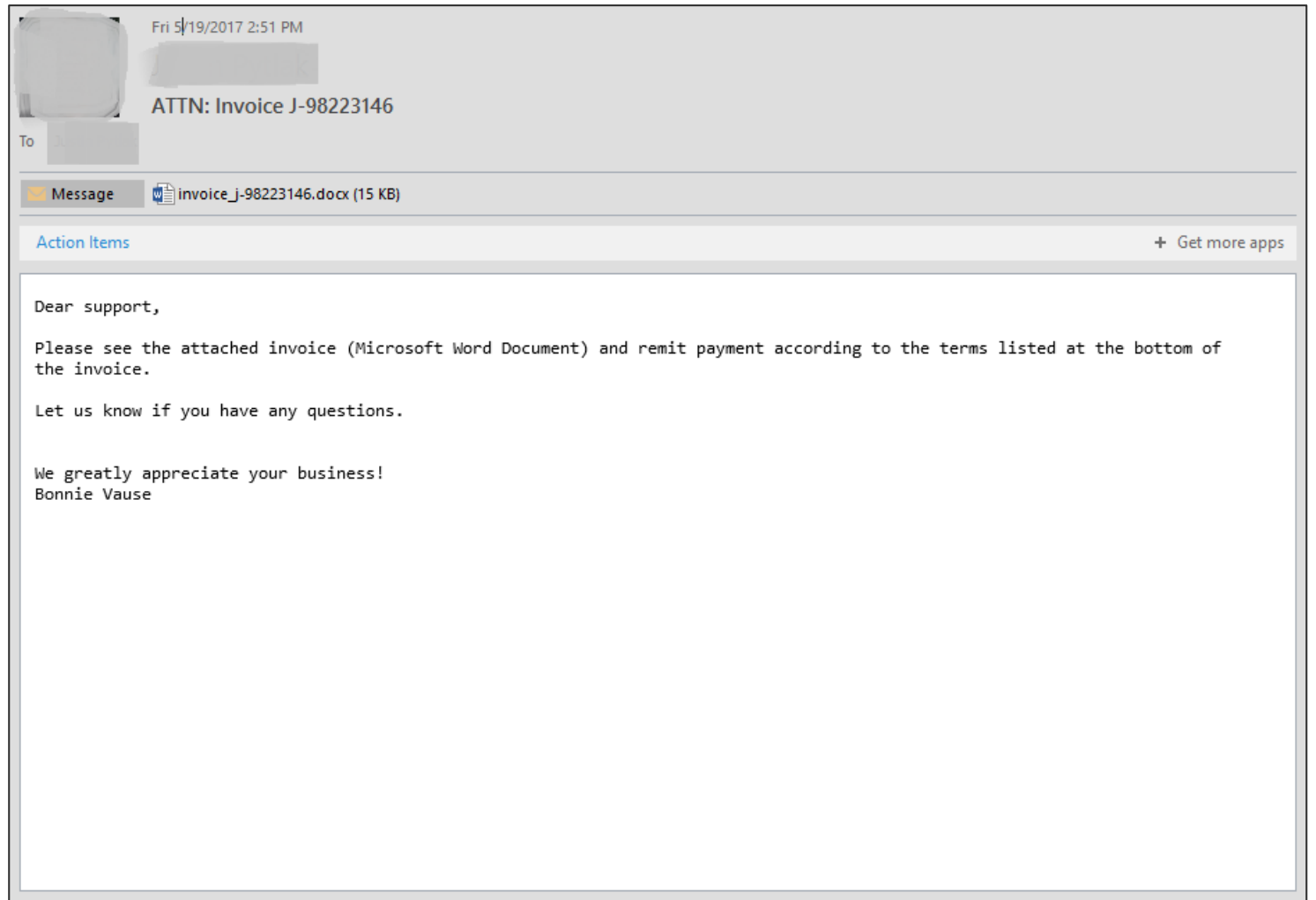
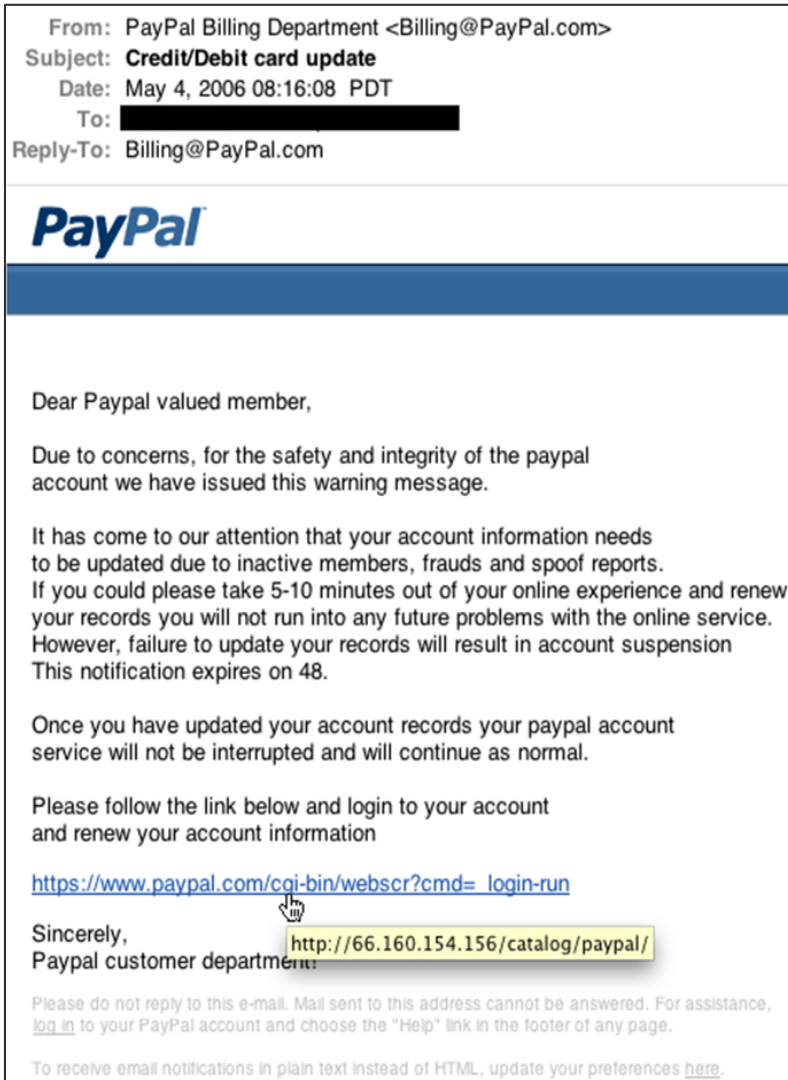


Image 1



In image 2, note the link appears to direct the reader to a legitimate PayPal web page and yet, when the mouse is hovered over the link, you see that it actually directs to a different site designed to inject malware or illegally collect personal information.

RED FLAGS: Missing sender or recipient information, generic greetings, misspelled email addresses, (e.g. billing@amzaon.com), and email addresses that don't match the company name. Any emails that ask the recipient to download a form or macro in order to complete a task are highly suspicious and an employee should NOT click on anything. Instead, report the email to IT immediately.

Image 2

POP UPS

Another common lure is a pop-up that claims that a user's computer has been locked by the FBI because it was used to access illegal material such as child pornography (Image 3). The lure instructs users to click a link in order to pay a fine, which is bogus.

RED FLAGS: Links that redirect to a different domain, pop-ups that require you to enter personal information, or misspelled URLs. This type of attack can be very hard to detect, even if employs are highly vigilant.



Image 3

**MOST IMPORTANTLY, IF
YOU SEE SOMETHING,
SAY SOMETHING!**

For more information, please contact:

Nex Level Networks

315.426.8800

helpdesk@nlnit.com