NEWS RELEASE
MICHIGAN STATE POLICE

STATE POLICE WARNS OF MALICIOUS EMAIL CAMPAIGN

FOR IMMEDIATE RELEASE: **February 8, 2019**

LANSING, MICH. The Michigan State Police (MSP), Michigan Cyber Command Center (MC3) is noticing an increase in fraudulent emails containing malicious links or attachments that are being sent to businesses and individuals across Michigan.

Recent emails have had subject lines that include terms such as “Invoice” or “Receipt.” The email contains an attachment or link to download a PDF, MS Word or Excel document that contains malware.

Recent infections have been a result of the Emotet virus. Once infected, the virus has been known to steal contact information from any email address book that the user maintains, which allows the scammer to send spoofed emails to the user’s contacts. Other side effects of the malware include the stealing of passwords or banking information, encryption of user files and spreading of the virus to other computers that may be connected to the user’s network.

The MC3 recommends carefully screening all emails prior to clicking links or opening any attachments. Any email with attachments or embedded web links should be handled with care until the recipient can verify the authenticity of the email. Users should consider if they are expecting an email or document from the “sender” prior to opening any attachments or clicking on any links.

Additional information about this virus can be found at https://www.us-cert.gov/ncas/alerts/TA18-201A.

###

MEDIA CONTACT:
D/Sgt. Jeff Hoffman, MC3, mc3@michigan.gov or 1-877-MI-CYBER