Cyber Security Awareness Alert

Security through Vigilance

MICHIGAN CYBER COMMAND CENTER (MC3)

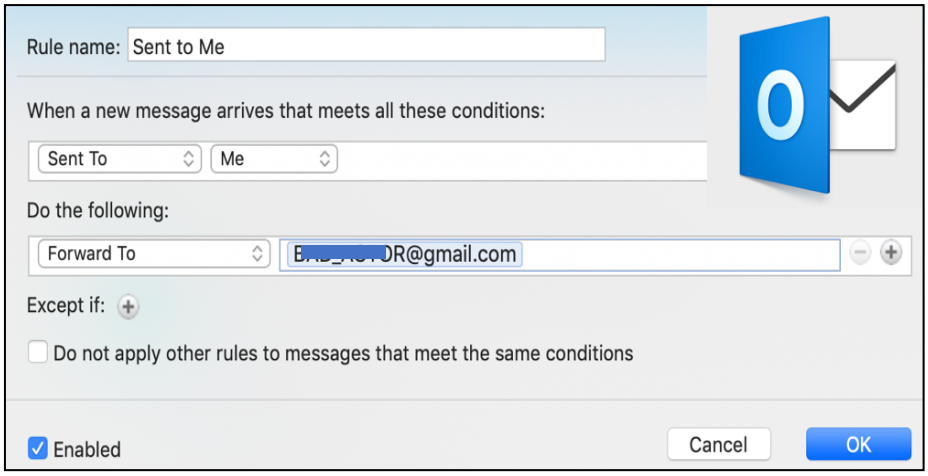
November 2, 2018
CA-02-2018

EMAIL FORWARDING RULES

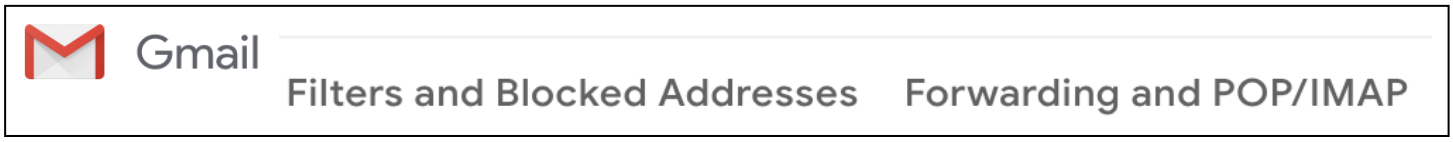
SUMMARY

The Michigan Cyber Command Center (MC3) has seen an increase in the use of email forwarding rules by malicious actors for illegal purposes. To do this, malicious actors often gain access to the victim's email account through a successful phishing attack. Once access is gained, malicious actors set up rules so that all emails received to the compromised account are forwarded to another account the malicious actor controls.

Recent investigations have shown that not only are malicious actors creating forwarding rules, but they are also creating filters to delete emails from specific contacts after being forwarded. Deletion filters have been observed in cases where fraud is being attempted via wire transfer or ACH transactions. Malicious actors appear to be monitoring accounts for a period of time where they learn how parties communicate, copy forms and digital signatures, and then use this information to attempt fraud once they learn a payment is upcoming.



Microsoft Outlook forwarding rule (above) and Gmail settings menu bar (below)



ANALYSIS

Users and system administrators are urged to review account settings and ensure no unauthorized email forwarding rules or filters are in place. If possible, create rules to alert account administrators to the creation of new rules. If any unauthorized email forwarding rules or filters are found, please report them to the MC3.

Continually updating and using strong passwords are important and highly recommended steps to help keep accounts secure. To help improve password strength, security experts recommend utilizing passphrases. If possible, users should utilize two-factor authentication (2FA), or multi-factor authentication (MFA).

When account changes for financial transactions are updated, controls should be in place to verify authenticity. It is a good practice to physically or verbally contact known parties prior to allowing the update or transfer of any funds to new accounts.

Any additional questions or concerns can be sent to the Michigan Cyber Command Center (MC3), mc3@michigan.gov or 1-877-MI-CYBER