Cyber Security Awareness Alert

Security through Vigilance

MICHIGAN CYBER COMMAND CENTER (MC3)

January 14, 2019
CA-01-2019

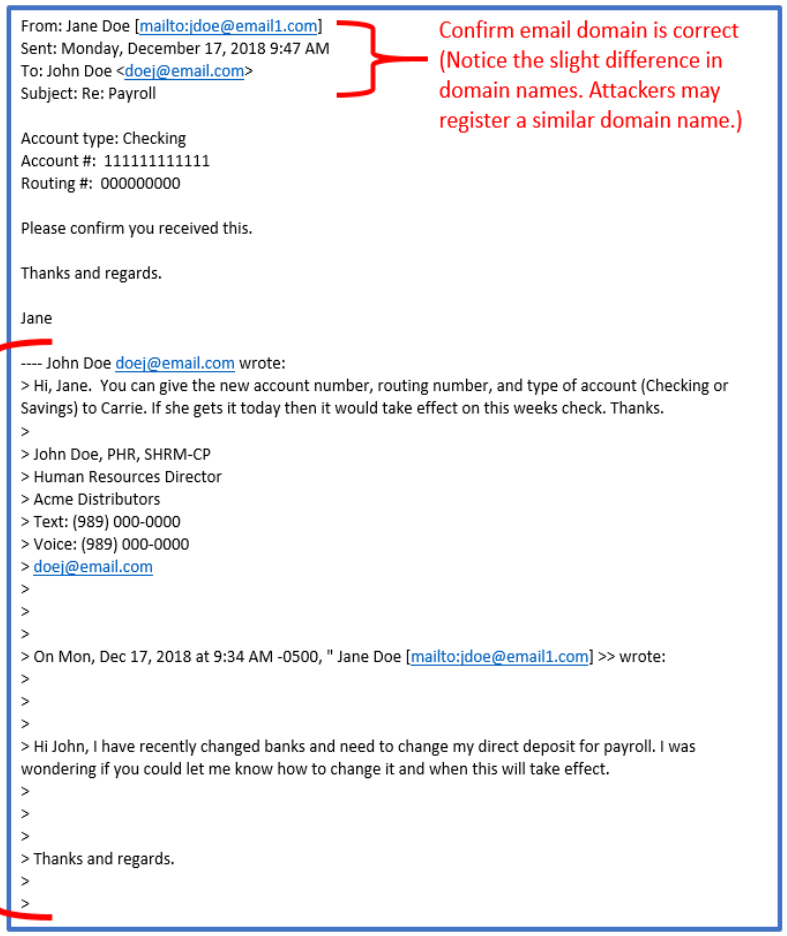
Payroll Phishing Attacks

Payroll and human resource departments are currently being targeted by malicious actors who send phishing emails, which appear to be coming from an employee of the organization. The graphics in this document show sanitized real-world examples. In these emails, the malicious actor requests for "their" payroll to be deposited into a different bank account which can be accessed by the malicious actor. The email accounts used to make the request can be external or come from an organization's domain as the result of an email account previously compromised.

It is not uncommon for malicious actors to set up forwarding rules and deletion filters in a compromised email account so that they may maintain persistence even after a password has been changed. Attackers have also been known to search email accounts for previously used ACH/direct deposit forms, so they appear legitimate. These emails may include sensitive information such as the "requestors" actual name, title, and social security number.

Example of a complex phishing attack.

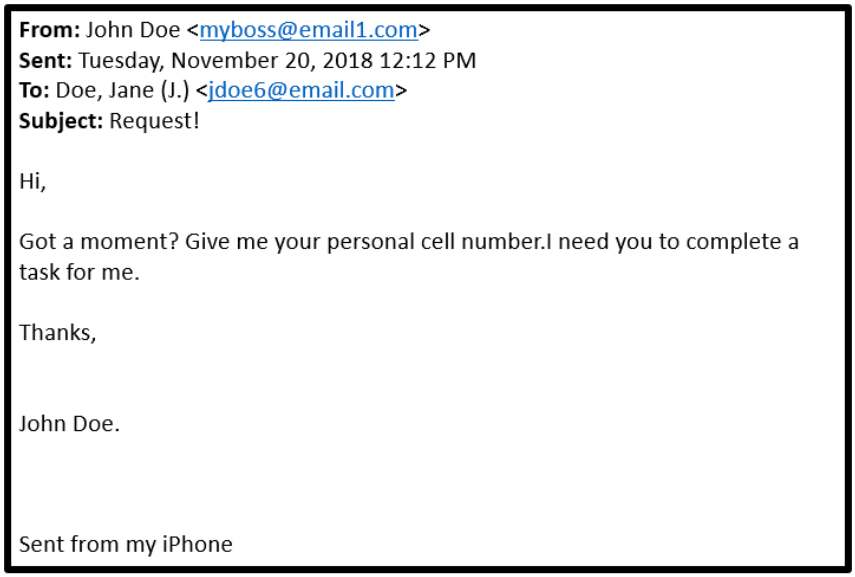
Crafted by the attacker to make it look like they were responding to an ongoing email thread.



The Michigan Cyber Command Center has seen numerous cases of this type of attack over the last few months. In some cases, the malicious actor has been successful at getting the payroll information changed which resulted in the funds being deposited into a fraudulent back account. Once this happens, the malicious actor usually withdraws the money immediately and the funds are lost. Other phishing attempts have been avoided by a human resources or payroll employee who recognized that something just wasn't right. In these cases, the payroll employee took additional steps to confirm the request prior to initiating it, or they were able to recognize it was a phishing attack. Recognizing these incidents as a phishing attack can be difficult due to some malicious actor's ability to make well-crafted attacks.

To avoid falling victim to these types of attacks, it is highly recommended that payroll and human resources employees use more than one verification process to confirm a payroll change request prior to it being implemented. For example, if a request comes in via email, additional contact should be made with the employee "requesting" the change via some other method, such as a phone number on record for the employee. Additionally, notification and mandatory waiting policies should be considered as well.

It is also recommended that organizations consider providing all employees with security awareness training. This training can help employees identify phishing emails and hopefully prevent attacks from being successful. If possible, this type of training should occur on a regular basis.



From: John Doe <myboss@email1.com>
Sent: Tuesday, November 20, 2018 12:12 PM
To: Doe, Jane (J.) <jdoe6@email.com>
Subject: Request!

Hi,

Got a moment? Give me your personal cell number.I need you to complete a task for me.

Thanks,

John Doe.

Sent from my iPhone

Example of a simple phishing attack requesting assistance.

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