



# 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.*

From: Jane Doe [mailto:jdoe@email1.com]  
 Sent: Monday, December 17, 2018 9:47 AM  
 To: John Doe <doej@email.com>  
 Subject: Re: Payroll

Account type: Checking  
 Account #: 11111111111  
 Routing #: 000000000

Please confirm you received this.

Thanks and regards.

Jane

----- John Doe doej@email.com wrote:  
 > Hi, Jane. You can give the new account number, routing number, and type of account (Checking or Savings) to Carrie. If she gets it today then it would take effect on this weeks check. Thanks.  
 >  
 > John Doe, PHR, SHRM-CP  
 > Human Resources Director  
 > Acme Distributors  
 > Text: (989) 000-0000  
 > Voice: (989) 000-0000  
 > doej@email.com  
 >  
 >  
 >  
 > On Mon, Dec 17, 2018 at 9:34 AM -0500, "Jane Doe [mailto:jdoe@email1.com]" >> wrote:  
 >  
 >  
 >  
 > Hi John, I have recently changed banks and need to change my direct deposit for payroll. I was wondering if you could let me know how to change it and when this will take effect.  
 >  
 >  
 >  
 > Thanks and regards.  
 >  
 >

} Confirm email domain is correct (Notice the slight difference in domain names. Attackers may register a similar domain name.)

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.

**TLP: WHITE**

This document is the property of the Michigan Cyber Command Center (MC3). This information is distributed as **TLP: WHITE**. Recipients may share this information with any parties. For more information on the Traffic Light Protocol, see <https://www.us-cert.gov/tlp>.



# Cyber Security Awareness Alert



Security through Vigilance

MICHIGAN CYBER COMMAND CENTER (MC3)

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.

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

**From:** John Doe <[myboss@email1.com](mailto:myboss@email1.com)>  
**Sent:** Tuesday, November 20, 2018 12:12 PM  
**To:** Doe, Jane (J.) <[jdoe6@email.com](mailto: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.*

**TLP: WHITE**

This document is the property of the Michigan Cyber Command Center (MC3). This information is distributed as **TLP: WHITE**. Recipients may share this information with any parties. For more information on the Traffic Light Protocol, see <https://www.us-cert.gov/tlp>.