Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

May 4, 2020
CS-05-2020

LIMITING EMPLOYEE INFORMATION PUBLISHED ON WEBSITES

SPEAR-PHISHING:

Organizations and businesses in Michigan are constantly falling victim to spear-phishing attacks. Spear-phishing, like phishing, involves electronic communications sent by malicious actors who are attempting to steal sensitive information or trick people into sending money. However, unlike general phishing where mass emails are sent out to random individuals, spear-phishing is a targeted attack which targets a specific individual or company and appears to come from a trusted source. There are several preventative measures that an organization or business can take to avoid falling victim to these attacks. For example, endpoint security software can be installed on devices and phishing awareness training for employees can be conducted. Another simple preventative measure that a company can take is to limit the amount of employee information and other sensitive information published on organization websites.

Image Source: hackernoon.com

HOW MALICIOUS ACTORS FIND AND USE EMPLOYEE INFORMATION:

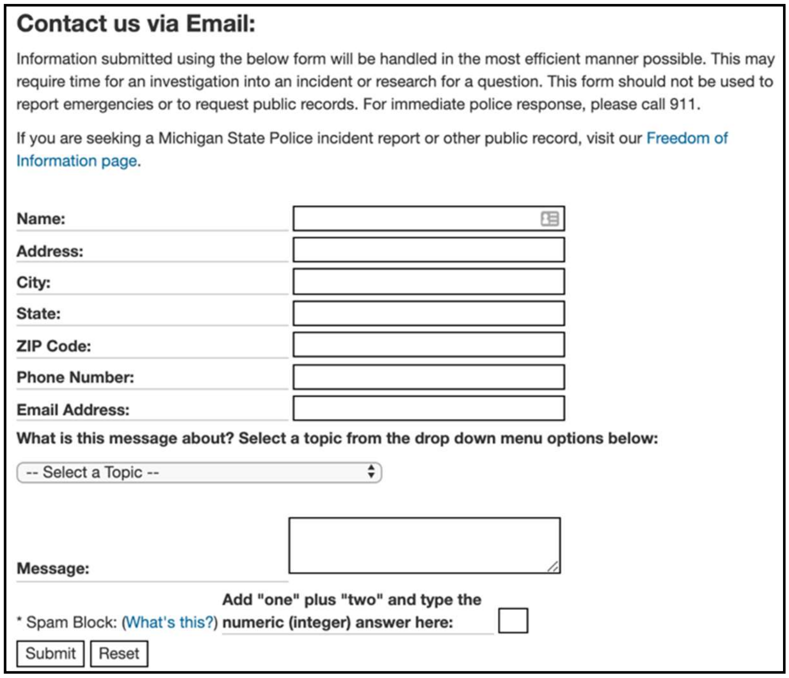
Prior to conducting a spear-phishing attack, suspects will conduct open source intelligence gathering and research on their targets. Many times, this includes visiting an organization’s website and searching for employee information. For example, many businesses and organizations have a “Meet Our Team” or “Staff Directory” page on their website. On these pages, many companies include information valuable to malicious actors, such as employee names, titles/positions, email addresses, phone numbers, and pictures. This makes it very simple for a malicious actor to identify which employees hold important positions within the company, such as CEO, human resources manager, accounts payable manager, finance director, school principal, county/township clerk, etc. Some companies also publish other sensitive information, such as which clients the company does business with or the schedule/travel plans of an important employee.

Once this information is obtained, it can be used for social engineering attacks or to craft emails targeted toward employees within the company. The malicious actor would know which email address to spoof, which email address to send the spoofed email to, names of parties involved, and the information needed to make the signature block look more legitimate. The MC3 is aware of malicious actors using this information in various ways. Below are some examples:

- A malicious actor discovers from a company website that the CEO is away from the office at a charity event. The malicious actor impersonates the CEO and sends a spoofed email to an administrative assistant asking them to purchase gift cards for a charity event and then scratch off the back of those cards and send the codes back.

- A malicious actor impersonates a company employee and sends a spoofed email to the human resources manager asking to have their direct deposit bank account changed to a new fraudulent bank account.
- A malicious actor impersonates the accounts payable manager of a company and sends a spoofed email to a client of the company advising them to wire money due for any new/outstanding invoices to a new fraudulent bank account.
- A malicious actor impersonates the head of an organization and sends a spoofed email to the human resources manager asking for all employee tax information for the past tax year.

UTILIZE A “CONTACT US” PAGE:



Contact us via Email:

Information submitted using the below form will be handled in the most efficient manner possible. This may require time for an investigation into an incident or research for a question. This form should not be used to report emergencies or to request public records. For immediate police response, please call 911.

If you are seeking a Michigan State Police incident report or other public record, visit our Freedom of Information page.

Name:

Address:

City:

State:

ZIP Code:

Phone Number:

Email Address:

What is this message about? Select a topic from the drop down menu options below:

Message:

* Spam Block: (What's this?) **Add "one" plus "two" and type the numeric (integer) answer here:**

Image Source: michigan.gov/msp

Instead of publishing employee information such as names, direct numbers, and email addresses on a company website, it is recommended that organizations publish a general phone number and have a “Contact Us” page which allows an individual to specify who/which department they would like to speak to and allows them to leave their contact information. Once submitted, this information then gets reviewed internally and sent to the appropriate employee who can recontact this individual. This provides people with an opportunity to contact the company while at the same time protecting sensitive employee information. Consideration should also be taken to protect employee information on social media pages, such as Facebook and LinkedIn. It is recommended that privacy settings are utilized on each platform to minimize the amount of sensitive data exposed to somebody who is not a friend/connection.

USE AN EMAIL WARNING BANNER FOR EXTERNAL EMAILS:

Organizations are encouraged to use a warning banner in their email system to alert employees the email came from outside the organization. As malicious actors often spoof email addresses, warning banners alert the recipient the email is not from their own organization.

Any additional questions or concerns can be sent to mc3@michigan.gov or 1-877-MI-CYBER.