Martha C. Yoder

TRUMBULL COUNTY AUDITOR
160 High Street, N.W., Warren, Ohio 44481
Phone: 330-675-2420 Fax: 330-675-2419
auditor@co.trumbull.oh.us

PRESS RELEASE
RE: BAZETTA TOWNSHIP HACKING INCIDENT

For Immediate Release

October 21, 2024-Warren, Ohio On September 3, 2024, my office became aware of irregularities regarding emails sent from Bazetta Township and of changes made to the Township's banking information resulting from our office's reasonable reliance on those emails. Upon examination of those emails by both myself and Deputy Auditor and Information Technology Director (Tim Haniford), we realized that these emails were the result of active hacking in which third parties took control of the Microsoft Office 365 account of the Fiscal Officer of Bazetta Township.

***Regarding this matter, it is vital to understand the difference between Phishing and Hacking. Phishing and Hacking are both internet crimes that aim to defraud people and organizations, but they differ in how they obtain information:*

- ***Phishing -*** *A type of social engineering attack that uses fake emails, websites, or phone calls to trick people into giving away vital information. The goal is to get people to voluntarily provide vital information, such as passwords or bank account details.*
- ***Hacking -*** *Involves forcefully gaining access to information by taking over a computer system, program, or account. Hackers can use brute force or more sophisticated methods to disable security measures and access sensitive data.*

The County's bank, Huntington, was immediately notified of the situation in order to try to recover the funds. I also informed the Prosecutor's office of the situation that day. We also notified, and later made a report with the Sheriff's Office.
Trustee Michael Hovis came to my office on the morning of September 3, 2024 shortly after the issue was discovered. I told him of both mine and Mr. Haniford's concerns that they had been hacked; and Mr. Haniford specifically noted that with Microsoft Office 365, it is very important to maintain and ensure that proper security measures were in place. It was specified that turning off those measures could put an entity at great risk for hacking. Mr. Haniford advised him to work with the township's IT staff/service to be sure that they were not at continued risk. It appeared that the emails from the hacked account had begun about a month prior to my office being notified. I also suggested that he call OTARMA (Ohio Township Association Risk Management Authority), the township's insurance company. As a former trustee, I know it is important to notify them of any loss quickly. My focus at that time was to work with the bank to attempt to recover the funds. Both Mr. Haniford and I were also concerned that Trustee Hovis was not taking the security issue of the Township's computer system seriously. I felt he was

more concerned about fault; however, at no time did I state who was responsible for the missing funds.
Over the next few days, my office cooperated with authorities on the investigation. I also spoke with Trustee Hovis several times.
While Trustee Hovis and the Township continue to broadcast their narrative publicly, they conveniently have left out the most important facts.

Here are the rest of the facts about this situation:

- Bazetta's computer system was compromised, specifically the Microsoft Office 365 account of the Fiscal Officer associated with email fiscalofficer@bazettatwp.org. This hack included all facets of the Microsoft Suite of products (Word, Excel, Outlook, OneDrive, etc...). Any stored or recently opened documents that contained financial information or information relating to how the processes work were in the hands of the hacker to use as he or she pleased to make documentation look legitimate.
- The emails received by my office were sent from the actual Microsoft Office 365 email account of the Bazetta Fiscal Officer, which was taken over by the hackers. This was not a phishing or fake email scam. The County investigated and determined that the Fiscal Officer's account had been compromised since August 9th, 2024, possibly earlier. The hacker had full access to the Bazetta's Fiscal Officer's account until, at least, September 3rd, 2024.
- ***The Fiscal Officer has admitted to asking for multifactor authentication (MFA) turned off for her Microsoft Office 365 email account.*** MFA is an electronic authentication security method that allows access to an application only after a user successfully presents two or more pieces of evidence (or factors) to authenticate his or her identity. MFA protects personal data-which may include personal identification or financial assets-from being accessed by an unauthorized third party who may may been able to discover, for example, a single password. ***Township IT did this either with or without the Trustees' permission or knowledge.***
- Turning off the multifactor authentication removed a vital barrier and opened the door for a hacker to take over the Fiscal Officer's account and control it, which the hacker did for at least three weeks.
- In its summer 2024 newsletter published just a few months ago, OTARMA directly addressed this threat and recommended using MFA as best practice along with other security measures. The Fiscal Officer ***intentionally*** had this measure disabled for her account, against OTARMA's specific guidance.

If the Township is looking for methods to recover its funds, this situation is covered by Ohio Revised Code 507.14 which states that a township fiscal officer *"shall be liable…when the loss of public funds results from the township fiscal officer's or deputy fiscal officer's negligence or other wrongful act"*. ***Disabling the township's MFA for the one person overseeing the township's funds was negligent.***

While much has been said about my office, ***the reality is that were it not for the disabling by the Township of its basic cybersecurity protections, this fraud would not have occurred.*** Until the Township owns this responsibility, determining liability for this loss cannot even begin.