ARIZONA Auditor General
Making a Positive Difference

FRAUD PREVENTION ALERT
Phishing Scam Emails
July 2016

Why are we issuing this alert?

Our Office received information that some entities have received phishing scam emails that appear to have been sent by upper management and request business office officials to divulge private information or process a wire transfer. Although these emails may appear to be legitimate, they are not. This alert outlines how public officials and other employees can recognize a phishing scam and reduce the risk of loss due to unapproved and erroneously processed transactions, specifically by familiarizing themselves with the general characteristics of phishing scam emails and ensuring that they take the appropriate actions should they receive a suspicious email.

What are phishing scam emails?

Phishing scams typically involve email communications where the email appears to come from a legitimate and often trusted sender and requests the receiver to divulge private information or perform certain actions that could potentially lead to data or financial loss. The email often requests the receiver to divulge information by either clicking on a link to a fraudulent website and entering in account numbers, user credentials and passwords, or other private information, or by requesting the receiver to take some other action like making a wire transfer. The fraudsters often "spoof" an email address, such as a high-level executive or administrator's email, to appear more credible when making the request. These scams are varied depending on the fraudster's expertise and objectives, and they often target high-profile individuals like a county manager, school superintendent, chief financial officer, or business office personnel. Suspicious emails often:

- Are unsolicited.
- Sound like they come from someone or some company you know.
- Request entity or personal financial or confidential information.
- Contain spelling or grammatical errors.
- Try to create a sense of urgency, asking or demanding that you take action right away.
- Include links to websites that look real but have a discrepancy in the actual underlying link address.
- Request that you deal directly with the email sender either by calling a phone number or emailing them.

In fact, our Office recently received information about a phishing scam email that appeared to have been sent by a school superintendent to the school's chief financial officer. The email requested the chief financial officer to process a $14,500 wire transfer to another bank account. The fraudster ended each email exchange with "email me." This was a tactic used to prevent the chief financial officer from calling the superintendent directly and discovering the scam. In this case, through the various email exchanges and by asking additional questions, the chief financial officer became suspicious, stopped communicating with the scammer, and contacted our Office. If your entity has received one of these emails, do not send payment. If your entity has made a payment for one of these requests, you should immediately attempt to stop the payment.

Additionally, we received information that another entity received a phishing email requesting certain employee payroll and tax information. In response, the Internal Revenue Service (IRS) issued an alert[1] in part stating, "The Internal Revenue Service today issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees. The IRS has learned this scheme – part of the surge in phishing emails seen this year – already has claimed several victims as payroll and human resources offices mistakenly email payroll data including Forms W-2 that contain Social Security numbers and other personally identifiable information to cybercriminals posing as company executives."

[1] See Internal Revenue Service Alert: *IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s*, March 1, 2016, Alert No. IR-2016-34.

Finally, as another example of the types of phishing emails you might encounter, several members from our own Office received an email message claiming that their email accounts were near their email quota, and provided a link to log in to their account to resolve the issue. The email came from an unknown individual and contained inaccurate information about mailbox size and limits. It also contained a link to an unknown site. Our IT Department sent an email the same day to all employees notifying them of the scheme, and requesting they delete the email and refrain from clicking on any links.

As identified in these three examples, phishing scam emails are diverse, have varying strategies and unique objectives, and try to appear like legitimate requests so that unsuspecting individuals will click on links, provide private information, or send the fraudster money.

How public officials can protect their entities from divulging information to a phishing scam email

In addition to the characteristics of suspicious email messages listed earlier, phishing scam emails often contain suspicious language and request private information, which should alert the receiver to be cautious and make them skeptical about clicking on links or providing any information to the email sender. Public officials should instruct their employees on what actions to take if they receive a phishing scam or other suspicious email, which could include:

- Checking the sender's entire email address, not just the sender name, by hovering over it to verify it is a reasonable email address. In the first example discussed earlier, the email listed the superintendent's name, but when looking at the actual email address it read: "officialdetailsemail@sent.as."
- Considering whether the email looks like other emails from the indicated sender. How does that sender normally address you? Is it unusual for them to use your full name or their own full name and title in an email?
- Verifying the email is genuine by contacting the actual business or person directly. Do not reply to the suspicious email, or use a phone number or website link provided in the email.
- Following standard procedures for notifying your IT personnel so that appropriate action, such as updating email filters to block messages with specific characteristics, can be taken entity-wide, if needed.
- Ensuring security and computer software is up to date.
- Avoid clicking links. One of the most common phishing techniques is the use of obfuscated links. There are many tricks used to mask the true destination of a link contained in an email message or presented on a web page, including using misspelled versions of the real organization's Uniform Resource Locator (URL) address or including the real company's name in a URL that belongs to another organization. Instead of clicking on the link, users should visit the websites manually by typing their addresses in the web browser or using a search engine like Google to search for an entity you are being directed to. Even if you think the email source is valid, you can hover over links before clicking on them to make sure they will take you where they say they will. Also, many messages give you an opportunity to unsubscribe, or be removed, from receiving future messages. Do not attempt to disenroll from a suspicious or unsolicited email's mailing list by clicking on links named "Unsubscribe"—just delete the email.
- Avoid filling out forms in email messages or opening attachments you were not expecting.
- Always follow your entity's proper expenditure processing policies and procedures, including requiring adequate documentation to support the public purpose for which the expenditure is being requested. Do not make a wire transfer, charge a credit card, or send a payment based on an unsupported request.
- Do not send sensitive or confidential information through email. Use secure methods or channels instead. If it cannot be avoided, secure the information in some other way, such as using software to encrypt it and requiring an agreed-upon password or other secure mechanism be used before the data can be opened or accessed.