Protect yourself from fraud and phishing by verifying – and verifying again

Municipalities and governmental entities are prime targets for phishing scams and fraud. According to the Merriam-Webster Dictionary: Phishing is “to try to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.”

Especially now in this crazy time of global pandemics and volatility, scam artists hope you will be distracted and either not follow protocols or believe that policies have changed. Recently, we at MMA Risk Management Services have been advised of similar attacks and have been threatened by hackers ourselves. We wish to share these stories as a lesson learned for you.

On recent occasions, municipalities here in Maine have received typical business phone calls from local businesses asking to update their bank account information. The person on the other end of the phone provides a name and title, which are accurate to the account. This is a common practice with what is called *a Spear Phishing Attack*, which is the fraudulent act of using electronic communication that is being sent from a presumably trusted source.

These criminal enterprises do research on the group that they are impersonating and use the names, titles and other contact information details to gain trust. As a result, the municipal employee may trust the information provided and view the person making the request as legitimate.

The person conducting the phishing attack then follows up with an email requesting a copy of their Automatic Clearing House/Electronic Funds Transfer (ACH/EFT) form. The municipal employee sends the ACH/EFT form to the person who they incorrectly think is the authentic vendor, allowing the criminal to complete and return the electronic form. The completed form is returned and the banking information for the “vendor” is updated in the municipal computer system. Following this change, legitimate-looking invoices are submitted to the municipality – but when they are paid, the payment is actually sent to a fraudulent bank account.

This can and does go unnoticed until the *actual* vendor calls to check on the status of payment. Unfortunately, this occurs after the payment has been made and several thousands of dollars were sent to the fraudulent bank account.

You might read this and find yourself asking: What more could have been done? With the implementation of a few minor verification procedures, this event may have been averted.

We strongly recommend that you establish the following minimum verification tools:

1. Set up key contacts for your accounts and only provide information to those designated individual.
2. Use multi-factor authentication for account access and changes. Multi-factor authentication is confirmation from two points of contact prior to the release of information or the altering of accounts.
3. Never use an email as your primary form of verification.
4. Call the account holder utilizing your original contact information, not that in the email communication and verify.
5. Increase awareness. Educate your entire staff and keep diligent to always follow the established rules.
6. Look out for fake emails:
    a. **Don't trust display names** as these can be anything a scammer wants them to be.
    b. **Check for fake email domains**; they'll often be slightly different versions of the real thing.
    c. **Look at the logo** and other images; low resolution images can be a giveaway.
    d. **Review links carefully** by hovering over the link text (without clicking). A link that is different from the one in the link text is a sign of a malicious link.
    e. **Look out for bad spelling and grammar**, as this can be a tell-tale sign that it's not a legitimate message.

Remember that the best defense against phishing attacks is employee training and education. A good security awareness program is most effective when you communicate through multiple formats. Consider awareness posters in common areas, helpful hints distributed to employees via email, and classroom training sessions.

MMA Risk Management Services Online University offers the course, "Preventing Phishing," which raises employee awareness and offers practical advice on avoiding phishing attempts.

Training your employees to detect phishing and other fraudulent activity is one of the most important safeguards against cybercrimes. If you need assistance with employee training, contact the MMA Risk Management Services at 800-590-5583, or find online training at www.memun.org.