By Jeffrey Guy
Commissioner, Burnet County ESD No. 1

Emergency Service District treasurers are being targeted with wire transfer "phishing" email scams. Treasurers across the state are receiving carefully-crafted emails that appear to come from their ESD Board president, vice president or county commissioner.

These differ from normal phishing emails in that they are sent only to board treasurers and contain locally-specific names of other board members, increasing the credibility of the scam. Treasurers should remain vigilant and not act on any unsolicited financial requests received via email or over the phone from unknown or unverified personnel.

If you have received a targeted phishing email, delete the email and ignore it. If your ESD fell victim to an email scam and transferred funds to an unauthorized party, contact your local FBI Field Office.

In addition to following good cybersecurity practices, ESDs are encouraged to carry cyber liability insurance that includes phishing and cyber fraud protections to guard against financial losses from those that fall victim. Computer systems are complex and cyber criminals are exceedingly clever. Even cybersecurity experts can fall victim to a targeted and well-crafted phishing email.

Answers to the most common questions are below.

**What is a phishing email?**

A phishing email is a type of spam email that encourages the recipient to take an action on behalf of an attacker. The digital equivalent of a con artist, the pretext can vary widely. The most common email scam is the "Nigerian prince" scam, in which a so-called Nigerian prince is seeking a trusted partner to get funds out of Nigeria and only needs a partner with a U.S. bank account.

Most email scams are sent blindly to tens of thousands of email addresses at a time. If the success rate is just 0.001%, an attacker only has to send 100,000 emails for each success. Since the cost of sending email is effectively zero and success rates are non-zero, it remains a viable criminal enterprise.

**What is the difference between these emails and the typical email scam?**

The recent ESD phishing emails are not sent blindly, but one at a time only to board treasurers. The "from" name is spoofed to come from people the treasurer knows and who may be involved with the ESD board, such as the board president, vice president or local county commissioner.

The email contents are brief, but are typically requesting transfer of funds, an urgent situation and immediate deadline. This technique is frequently used by attackers targeting the commercial sector, sending similar emails, spoofed to come from the CEO, late on a Friday afternoon to the CFO or finance director. They are surprisingly successful.

An example email is pasted below. In this ESD, Frank Thompson is the Board President and John Kissinger is the Treasurer. (names are fictitious)

> **From:** "Frank Thompson" <thompson.mycountyesd1@gmail.com>
> **Date:** March 29, 2018 at 9:32:03 AM CDT
> **To:** John Kissinger
> **Subject: TREAT AS URGENT**
>
> Hi John,
>
> I need you to make a payment to a vendor for services.
> Confirm if you can get this done today, so I can forward you the beneficiary details.
>
> Regards,
> Frank Thompson
>
> Sent from my iPad

The details included in the emails received by ESD treasurers means there is a group (or groups) of criminals that have researched the Texas ESD system, how an ESD functions and the individuals responsible for the targeted ESD. That group is specifically targeting our treasurers with the same attacks previously directed at commercial CFOs or finance directors.

**How did attackers get our names and email addresses?**

ESD board member names, roles and email addresses are a matter of public record and can be retrieved from the safe-d.org website, amongst other places.

**What should I do if I have received an email like this?**

There are too many phishing emails for law enforcement to act on each one. Delete the email, congratulate yourself on recognizing a fraudulent email and continue with your day.

**What should I do if my ESD has fallen victim to a phishing email and transferred funds to an unauthorized account?**

Contact your local FBI Field Office as soon as possible.

**What should ESDs be doing to mitigate the risk of these and other cyber risks?**

*Be vigilant.* Email phishing attacks are a scam – recognize when an emailed request is unusual and unprompted. Verify it with a phone call to the alleged email sender. Be equally skeptical of unsolicited phone calls received from unknown persons.

*Use Two Factor Authentication for online banking*. Most websites authenticate users with just a username and password. However, usernames and passwords are too easily stolen to protect assets as critical as your ESD's bank account. Use two-factor authentication with your bank's online portal that requires a special code from your cell phone in addition to the typical username and password.

*Carry Cyber Liability Insurance.* No matter what protections are in place, it is impossible to eliminate the risk of a loss event in a system as complex as the Internet. Work with your insurance provider to add cyber liability insurance to your policy portfolio.